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**"

ℕ INET	
	Please log in!
	A user
	B passeord
	D #

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:

🕅 INET platform	🗑 Dashboard 🗞 Change 🕀 Analyze 🗒 Search 🎕 Co	nfig		🖉 💿 T 🛞 admin
Platform				3 🔳
A User R User Group	I Basic information Authorization type : Formal	Serial number ×	lssuer: 深圳天元云和技有限公司	
Mail sso SSO Setting	Project name : Net Effective start time : 2023-02-01 0000001	Smit (6853/80(6919/867508/988004/6018/65005104/34A). 0 4 COPY number	Deployment mode : Single node mode	

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:

🚺 INET platform	뛓 Dashboard 🗞 Change 🛛 Analyze 🗇 Search	😫 Config					r (0)	Т ⊗ас
Platform								
Co License								
& User	Basic information							
R User Group								
Q _e Role	Authorization type : Formal	Authorized customer: 172.21.1.	36	Issuer : 1	和此方元云科技有限公司			
Mail	Project name : iNet		Issue date : 2023-02-	01 00:00:01	Deployment mode : 5	ingle node mode		
sse SSO Setting	Effective start time: 2023-02-01 00:00:01		Effective deadline : 2123-04-	30 11:22:00				
	Feature support Totagy source Tot	Sontgy optimization Topology management Wookflow Device sattings		Capacity support Winese I will Muncher of formation Muncher of SDN controllers- Muncher of study exchanges	10	20	30	

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

🚫 INET platform	뛓 Dashboard 🗞 Change 🛛 Ar	alyze 🖾 Search 🞕 Config			0 T	le admin
 Platform License 	New			Please input Role Name	۹٥	
A User	Role Name	Type ☑ Users	Description	Op	eration	
K User Group	ROLE_ADMIN	System default 2				A
Mail	default_role	Customize 1		Aut	horize Edit Delete	v
sso SSO Setting				1-2 of 2	items < 1 > 20/j	page 🗸

Click on Settings \rightarrow 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.

🚫 INET platform	Dashboard 🗞 Change 😪 Analyze	🔯 Search 🎕 Config					🖓 💿 T 🛞 admin
 Platform License User 	Role / default_role Select All Save Reset						
R User Group	Module name	Submodule name	Function authorization				
Q, Role	 Dashboard 	Dashboard	Read-only	🛃 Add/Change	🖌 Delete		<u>^</u>
Mail SSO Setting		Firewall Policy	Read-only	Add/Change	Delete	Audit	
		Internet Policy	Read-only	Add/Change	Delete	Audit	
		 SDN policy 	Read-only	Add/Change	Delete	Audit	
		Policy inheritance	Read-only	Add/Change			
		Cibject management	Read-only	Add/Change	🛃 Delete		
		Load balancing	Read-only	Add/Change			
	Change	Emergency blocking	Read-only	Add/Change	🛃 Delete	🛃 Audit	
		Review	Read-only	Add/Change	Delete	Audit	
		Batch job	Read-only				
		Configuration rollback	Read-only	Add/Change	Delete	Audit	
		Pipeline	Read-only	Add/Change	Delete	Audit	

3. 2. 2. Create a new role group

		y adm	n
		٢	1
			1
		-	
Edit Delete			
1 > 20,	/ page		1
	Q C as Deine da Delete	O Define Define Define Define O	O

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

🕅 INET platform	뛓 Dashboard 원 Change 😡 Analyze 🔞 Search	Config			🕼 💿 T 🛞 admin
Platform					
🐻 License	New Delete				Q D @
A User				Creation time	
R User Group	developer				Edit Delete
Mail	default_group				Edit Delete
sso SSO Setting	admin				Edit Delete
	operator				Edit Delete
		New	×	1-4 of 4 it	ems < 1 > 20/page >
		• Name:			
		Description :			
			Cancel		

Click on Settings \rightarrow 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

🕅 INET platform	Dashboard 🛛 🗞 Char	ige 🎯 Analyze	🐼 Search 🎕 Config						Ф 🗇 Т	le admin
Platform Dicense	New						Username V Please in			
A User	Username		Group		⊽ Role	♥ Email	Creation time			
R User Group	admin			Available	ROLE_ADMIN	admin@sky-cloud.r	et 2019-08-05 21:37:29	- Disable	d Reset Password	
Mail SSO Setting	inet-ngparser	inet-ngparser		Available		support@sky-cloud	.net 2023-07-31 18:25:11	admin Edit	d Reset Password	
	🗌 test		admin; default_group; develope	r; operator • Available	default_role; ROLE_ADMIN	123@qq.com	2024-05-24 18:00:52	admin Disable Edit	d Reset Password	
	4		New User			×	_	1-3 of 3 item	s < 1 > 20/p	age ∨
			• Username: Rease input		English Name: Please input					
			* Group: Please select		Role: Please select					
			Password: Please input	ø	Confirm Password: Please input	90				
			• Email: Please input		* Status:					
			Description :							
						Cancel				

Click on Settings \rightarrow 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 \rightarrow Device \rightarrow credential (indicated by the red arrow). You can see the corresponding connection credentials. Vouchers can be edited or deleted.

🕥 INET platform	행 Dashboard 원 Change 원 Ar	nalyze 😨 Search 🔒 Config			Q © T ®
Device ^					
Catalogue	New Delete				Please enter keyword Q C I \$
Credential	Name	Туре	Username	Remarks	Operation
HA Group	testa	Username/Password	admin		Edit Delete
Template	52	Username/Password	admin		Edit Delete
ask Setting	itest	Username/Password	inet		Edit Delete
opology	□ AF	Username/Password	admin		Edit Delete
PAM	ра	Username/Password	admin		Edit Delete
Nodel Details	admin-admin	Username/Password	admin		Edit Delete
fodel	panorama	Username/Password	admin		Edit Delete
elation	hilstone	Username/Password	hillstone		Edit Delete
lssociation	wpq-cisco	Username/Password	admin		Edit Delete
ibrary ^	labla	Username/Password	admin		Edit Delete
pplication(Huawei)					50 - D

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

🚫 INET platfori	Dashboard 🖓 Change 4	la Analyze 🗊 Search 🚳 Config			φ Θ T Θ.	admin
IE Device						
Catalogue	New Dente	New		×	Presse setter beyonder C I C	Þ
Credential	Name	Туре			Operation	
HA Group	testa	Username/Password	e: Please input Name	0	Edit Delete	
Template	62	Username/Password * TyP	e: Usemame/Password	~	Edit Delate	
Task Setting	itest	Username/Password • Usernam	et Please input Username		Edit Delete	
Y Topology	AF .	Username/Password Password	d: Please input Password		Edit Delete	
IPAM	(pa)	Usemanie/Fassword			Edit Deleto	
Model Details	admin-admin	Usemame/Fassword	 Prease input Hermania 		Edit Delete	
Model	🔲 panorama	Usemame/Password			Edit Delete	
Relation	Hilatone	Username/Password			Edit Delete	
Association	wpq-cisco)	Username/Password		Cancel OK	Edit Delete	
Library ·	Table :	Usemanie/Password	aderin		Edit Delete	

- 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.

-								
=	Device •	创 Device catalog C	Domain Operation 4					
	Catalogue	Search	Overview Firewall Route	Switch SDN Controller Virtual gatewa	y Load Balancer Authority			
	Credential HA Group	• 🚔 frame	✓ Basic info					
	Template	* Domain	default					
ų	Task Setting Topology	 172.21.1.84 internet-172.21.1.80 	name : Di	main 24-07-31 14:47:26	created_at : 2023-07-21	1 11:55:13		
品	IPAM	F5-192.168.60.132	opusieu_ar zr	De 07 51 MAR 26				
	Model Details	172.21.1.94	Load Balancer		SDN Controller		Virtual gateway	
	Model Relation	Manage-Huawei-Firewall- 172.21.1.84	1		0	0	0	
	Association	172.21.1.93						
ê	Library 0	• 💼 test	Firewall		Router Switch			
	Application(Huawei)	High 172.21.1.110-url	4		1			
	Antivirus(PA)	* Balance					-	
	Object Management2.0	192.168.60.132						
		* susiness						
		FortiGat_172.21.1.162						
		testcisco						
		E panorama 192, 168, 60, 100						
		gw-020000-1						
		172.21.1.162-1						
		Pa-192.168.60.99						
		Cisco-172.21.1.160-2						

4.4.1. New Firewall

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

Crea	te firewall			Х
1	Basic properties	* Vendor: * Model:	FortiGate V	
2	Configuratic	* Version:	FortiOS 6.0 V	
3	Initial settings	* Device name:	Please input Device name	
4	About to	Description :	Please input Description	
	complete			

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".

Crea	te firewall			×
\bigcirc	Basic properties	* How to get configu	Pull automatically Upload manually	
		* Management IP:	Please input Management IP	
2	Configuratic	* Portocol:	SSH V	
		* Port:	22	
3	Initial settings	* Credentials:	admin V Test connection New credential	I
		* Management mod	Collect only 🗸	
4	About to complete	Advanced: S	Show	
			Previous	Next

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, \bigotimes 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".

Creat	e firewall			×
\odot	Basic	* Working mode:	Routing	
	properties	* Coding:	UTF-8 V	
	Configuratic	HA group:	Please select HA group	
		Logical system:	Enter the logic system	
3	Initial	* Time zone:	Asia/Shanghai	
	settings	* Object group refer	Object group reference object \lor	
4	About to	* object reference:	referencing object name	
<u> </u>	complete	Set the new config a	True V	
			Previous	Next

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

=	Device	^	Device catalog C		₩ 172.21.1.184 <mark>⊘</mark>	」		
	Catalogue		Search Q	0	verview Configutation	n Setting Authority		
	Credential		+ 🖶 frama	-				
	HA Group		 Anne DATA 	Y	Basic info			
	Template		🝷 🚘 Domain		Basic properties			
	Task Setting		172.21.1.184		Vendor	: Huawei	Model	: USG6000
×	Topology		(5 F5-192.168.60.132		Version	: V100R001C30SPCa00 View Template	Device	: Domain
딦	IPAM		Route-172.21.1.94					
2	Model Details	^	😤 Manage-Huawei-		Device Name	: 1/2.21.1.184	Description	: -

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.

Image: Contract of the contract of	Device catalog C	Analyze-Huawei-1	72.21.1.93 🧿 📋 👫 🍄 🎯 🏦 🗎 🤉	peration \downarrow				
Image: Normal Partial Partia Partial Partial Partial Partial Partial P	Search	Overview Configutation	Setting Authority					
• Tormain • Memoin Under time	▼ 🚔 frame ▼ 🗞 DATA	Configuration Repo Route Repo	Upload Compare Active Rollback					CI®
1722.1.184 Nur poing 202-04-23 144481 202-04-23 144481 922 Nur pite Main Weing Take Weing	👻 🚞 Domain	Security policy	Version	Update time	The length of config	Update source	Operation	/0
• Orgin	172.21.1.84	NAT policy	2025-03-20 16:46:51 Active	2025-03-20 16:46:51	58722	Pulling Task	View	Delete Download
16 16 <td< td=""><td>Internet-172.21.1.80</td><td>Object</td><td>2025-02-22 19:46:51</td><td>2025-02-22 19:46:51</td><td>58528</td><td>Pulling Task</td><td>Vew</td><td>Delete Download</td></td<>	Internet-172.21.1.80	Object	2025-02-22 19:46:51	2025-02-22 19:46:51	58528	Pulling Task	Vew	Delete Download
Immung-jung-super	F5-192.168.60.132	Service Object						
1722.1.194 ULC Chepy 2026.02.11 20481 2203.02.11 20481 9120 Auing fack Wein (% or owned) 1722.1.164 2026.02.11 20481 2203.02.11 20481 2203.02.11 20481 9120 Auing fack Wein (% owned) Wein (% owned) 1722.1.164 2026.02.11 20481 2203.02.11 20481 9203 Auing fack Wein (% owned) Wein (% owned) 102.11.1041 2026.02.11 20481 2203.02.11 20481 9203 Auing fack Wein (% owned) Wein (% owned) 102.11.1041 2026.02.11 20481 2203.02.11 20481 9203 Auing fack Wein (% owned) Wein (% owned) 102.11.0401 2026.02.01 20481 2203.02.01 20481 9203 Auing fack Wein (% owned) Wein (% owned) 102.02.02.01 20481 2203.02.01 20481 2203.02.01 20481 9203 Auing fack Wein (% owned) Wein (% owned) 102.02.02.01 20481 2203.02.01 20481 2203.02.01 20481 9203 Auing fack Wein (% owned)	manage-juniper-Route-	Time Schedule Object	2025-02-22 18/4651	2025-02-22 18/46/51	93	Pulling lask	view	Derete Download
Mundge Haumer Personers 2824-22.1124451 2826-22.1124451 9824 Aulog Tak Verv Der Dorrsdot 1722.1130 Aulog Tak 2826-22.1124451 2826-22.1124451 9824 Aulog Tak Verv Der Dorrsdot 1202.1130 Aulog Tak 2826-22.1124451 2826-22.1124451 9824 Aulog Tak Verv Der Dorrsdot 1212.1130 1122.1130 2826-22.1124451 2826-22.1124451 9826 Der Dorrsdot Verv Der Dorrsdot 1212.1130 1122.1130 2826-22.1124451 2826-20.0124451 9807 Aulog Tak Verv Der Dorrsdot 1202-02.0129.4481 2826-20.0129.4481 2826-20.0129.4481 9807 Aulog Tak Verv Der Dorrsdot 1202-02.0129.4481 2826-20.0129.4481 2826-20.0129.4481 9807 Aulog Tak Verv Der Dorrsdot 1202-02.0129.4481 2826-20.0129.4481 2826-20.0129.4481 9807 Aulog Tak Verv Der Dorrsdot 1202-02.0129.4481 2826-02.0129.4481 2826-02.0129.4481 9807 Aulog Tak Verv Der Dorrsdot 1202-02.0129.44841 2826-02.0129.44841	172.21.1.94	URL Category	2025-02-21 13:46:51	2025-02-21 13:46:51	58528	Pulling Task	View	Delete Download
A conjunctionarii A conjuncto conjunctionarii A conjunctionarii<	Manage-Huawei-Firewall- 172.21.1.84	Network Interface	2025-02-21 12:46:51	2025-02-21 12:46:51	58624	Pulling Task	View	Delete Download
1722-19.93 Porty based multiply 2025-02.11 01:44:51 2025-02.11 01:44:51 2025-02.11 01:44:51 2025-02.11 01:44:51 2025-02.11 01:44:51 2025-02.11 01:44:51 2025-02.01 01:44:54 2025-01 01:44:54<td>🔝 Analyze-Huawei-</td><td>Zone</td><td>2025-02-13 15:46:51</td><td>2025-02-13 15:46:51</td><td>58528</td><td>Pulling Task</td><td>View</td><td>Delete Download</td>	🔝 Analyze-Huawei-	Zone	2025-02-13 15:46:51	2025-02-13 15:46:51	58528	Pulling Task	View	Delete Download
• TST 0 203-0.01 1004690 203 0.01 1004690 80 Aling Tak View Deret Deretad • 10 702.11.100 0 203-0.01 004691 203 0.04 1004691 5001 Aling Tak View Deret Deretad • 203-0.01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-0.01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-0.01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-0.01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-0.01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-01 004691 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-01 004691 203 0.04 00461 203 0.04 00461 2007 Aling Tak View Deret Deretad • 203-01 004691 203 0.04 004691 203 0.04 004691 2007 Aling Tak View Deret Deretad • 203-01 004691 203 0.04 004691 203 0.04 004691 2030 Aling Tak View Deretad • 203-01 004691 203 0.04 004691 203 0.01 004691 203 0.01 004691	172.21.1.93	Policy based routing	2025-02-11 01:46:51	2025-02-11 01:46:51	58001	Pulling Task	View	Delete Download
1722.1.1.10-ut - 202-0.01 204401 2020-0.01 204401 9007 Autor State Ver	🕶 🚔 TEST			2015 02 11 02 (CE)		Realizer Reals		and a second
 2026-020 874481 2026-0148 8448 2026-0148 8484	172.21.1.110-url		2023-02-11 0094630	2023-02-11 0094650	89	Pulling lask	view	Delete Download
• Market 2054-20.0044451 2020.0024455 5007 Auling Task Verr Deck Download • 2054-20.0044451 2020.00244451 5001 Auling Task Verr Deck Download • 2054-20.0044451 2020.00244451 5001 Auling Task Verr Deck Download • 2054-20.0044451 2020.0024454 80 Auling Task Verr Deck Download • 2054-20.0044452 2020.0024454 80 Auling Task Verr Deck Download • 2056-20.0044452 2020.0014 80 Auling Task Verr Deck Download • 2020.001 2020.01446465 2020.01404645 5001 Auling Task Verr Deck Download • 2020.01146465 2020.01146465 5001 Auling Task Verr Deck Download • 2020.01146464 2020.01146465 5001 Auling Task Verr Deck Download • 2020.01146464 2020.011464645 5001 Auling Task Verr Deck Download Download • 2020.011644645 2020.0116446	Clsco-172.21.1.160		2025-02-08 07:46:51	2025-02-08 07:46:51	58001	Pulling Task	View	Delete Download
10 102.108.00.122 10 202.02.02 08.46.51 2025.02.02 08.46.51 5001 Autrop Task Vere Derts Dortsmall 10 102.108.00.122 10 202.02.02 08.46.51 2025.02.02.02 08.46.51 2025.02.02 08.46.51	 Balance 		2025-02-08 06:46:51	2025-02-08 06:46:51	58097	Pulling Task	View	Delete Download
• Explorings • Enclosed within in and in and in a final within in a final within the set of	192.168.60.132		2025 02 03 08:46:51	2025 02 03 08-46-51	58001	Pulling Tark	View	Delete Download
1722.1.1.191 2025-0.019.0462 2023-0.019.0462 80 Aulor Tax Wei Device	 Business 			2023-02-03-02/0231	55501	runing last		John Dominana
Image:	172.21.1.191		2025-02-03 07:46:52	2025-02-03 07:46:52	89	Pulling Task	View	Delete Download
Image: Section Control 2025-01-34 484452 2025-01-34 284452 5807 Pulling Task Verm Denter Downstad Image: Section Control 2025-01-34 284452 2025-01-18 284455 5807 Pulling Task Verm Denter Downstad Image: Section Control 2025-01-18 284455 2025-01-18 284451 S807 Pulling Task Verm Denter Downstad Image: Section Control 2025-01-18 284451 2025-01-18 284451 S807 Pulling Task Verm Denter	FortiGat_172.21.1.162		2025-01-24 09:46:51	2025-01-24 09:46:51	58001	Pulling Task	View	Delete Download
Begin partorizanti \$2,164,0100 Display Constraint Status Auring Task Versil Device Device <thdevice< th=""> Device <thdevice< t<="" td=""><td>testcisco</td><td></td><td>2025-01-24 08:46:52</td><td>2025-01-24 08:46:52</td><td>58097</td><td>Pulling Task</td><td>View</td><td>Delete Download</td></thdevice<></thdevice<>	testcisco		2025-01-24 08:46:52	2025-01-24 08:46:52	58097	Pulling Task	View	Delete Download
gr v02000-1 2025-11:0.04465 2.025-11:0.04465 5001 Puling Task Verice Dented III 72.21.1.02-1 2025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented III 000000-1 2025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented III 000000-1 2.025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented III 000000-1 2.025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented III 00000-1 2.025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented III 00000-1 2.025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented IIII 0000-1 2.025-01:0.034651 2.025-01:0.034651 58171 Puling Task Verice Dented IIII 0000-1 2.025-01:0.034651 2.025-01:0.034651 2.025-01:0.034651 2.025-01:0.034651 2.025-01:0.034651 2.025-01:0.034651 2.025-01:0.034651 2.0	panorama192.168.60.100					-		
Image: T7221.1.162-1 2025-01-16.03.46631 2025-01-16.03.4651 Still 7 Pulling Task Vew Detete Dourised Image: T7221.1.162-1 Citico-17221.1.160-2 1.20 of 79 lems Image: Transmission of the temperature of t	gw-020000-1		2025-01-18 04:46:56	2025-01-18 04:46:56	58001	Pulling Task	View	Delete Download
1-30 of 79 terms 1 2 3 4 → 20/ page	172.21.1.162-1		2025-01-18 03:46:51	2025-01-18 03:46:51	58171	Pulling Task	View	Delete Download
1-20 of 79 items < 1 2 3 4 ≯ 20 / page ∨	pa-192.168.60.99							
	Cisco-172.21.1.160-2						1-20 of 79 items < 1	2 3 4 > 20/page ∨

- **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.

Device catalog C	Analyze-Huawei-1	72.21.1.93 📀 🔢 👭 🍄 🎯 🏪 🕴 Operation	Ŷ			
Search C	Configutation	Setting Authority				
frame & DATA * * Domain	Configuration Repo Route Repo Policy	Uphoad Compare Active Roliback	Update time	The length of config	Update source	C I 🕸
172.21.1.84	Security policy	2025-03-20 1646/51 Active	2025-03-20 16:46:51	58722	Bullion Tark	View Delete Drumland
internet-172.21.1.80	Object Address Object	2025-02-22 1946:51	2025-02-22 19:46:51	58528	Pulling Task	View Delete Download
manage-juniper-Route-	Service Object	2025-02-22 18:46:51	2025-02-22 18:46:51	89	Pulling Task	View Delete Download
172.21.1.94	URL Category	2025-02-21 13:46:51	2025-02-21 13:46:51	58528	Pulling Task	View Delete Download
Manage-Huawei-Firewall- 172.21.1.84	 Network Interface 	2025-02-21 12:46:51	2025-02-21 12:46:51	58624	Pulling Task	View Delete Download
🔝 Analyze-Huawei-	Zone Router	2025-02-13 15:46:51	2025-02-13 15:46:51	58528	Pulling Task	View Delete Download
172.21.1.93	Policy based routing	2025-02-11 01:46:51	2025-02-11 01:46:51	58001	Pulling Task	View Delete Download
 TEST 172.21.1.110-url 		2025-02-11 00:46:50	2025-02-11 00:46:50	89	Pulling Task	View Delete Download
Cisco-172.21.1.160		2025-02-08 07:46:51	2025-02-08 07:46:51	58001	Pulling Task	View Delete Download
👻 🚔 Balance		2025-02-08 06:46:51	2025-02-08 06:46:51	58097	Pulling Task	View Delete Download
192.168.60.132		2025-02-03 08:46:51	2025-02-03 08:46:51	58001	Pulling Task	View Delete Download
172.21.1.191		2025-02-03 07:46:52	2025-02-03 07:46:52	89	Pulling Task	View Delete Download
ErrtiGat_172.21.1.162		2025-01-24 09:46:51	2025-01-24 09:46:51	58001	Pulling Task	View Delete Download
testcisco		2025-01-24 08:46:52	2025-01-24 08:46:52	58097	Pulling Task	View Delete Download
gw-020000-1		2025-01-18 04:46:56	2025-01-18 04:46:56	58001	Pulling Task	View Delete Download
172.21.1.162-1		2025-01-18 03:46:51	2025-01-18 03:46:51	58171	Pulling Task	View Delete Download
pa-192.168.60.99					-	
Cisco-172.21.1.160-2						1-20 of 79 items < 1 2 3 4 > 20 / page ∨

• Manually triggering configuration updates

Click on the selected firewall, select "Configuration", click on "Configuration Repo", and then click on "Configuration Repo" 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

Device catalog	Analyze-Huawei-1	172.21.1.93 (Ø) 👬	Operation 4				
rch	Overview Configutation	Setting Authority					
frame	Basic properties	Configuation update					
Dala Domain	Policy anchor NAT policy anchor	Z Enable Repeat	× 1		Hour 兴	Save	
172,21.1.184	NAT settings	Execution history			Second		C T @
F5-192.168.60.132	 Task 	Execution history			Minute		0 1 4
manage-juniper-	Connection check	Context ID	Start at	End at	Hour	Execution result	Operation
Route-172.21.1.94	Configuation update	-10107-01-0-000-00-0-01-0-00-0	2024 02 05 10 45 10	2021 00 05 10 46 51	Dav	ADD UNICUALIZED	A 2 3 4
Manage-Huawei-	Route update	e 19301/ C-91C3-4109-508D-521CE350344E0	2024-00-00 10:40:49	2024-06-06 10:46:31		KYC UNCHANGED	EEC/G. VIEW configuration
Firewall-172.21.1.84	Hitcount update	5464e71d-77c9-4c3e-962a-15ddce669e6c	2024-08-06 09:46:49	2024-08-06 09:46:51	SUCCESS	RPC (UNCHANGED	会要日志 View configuration
Analyze-Huawei-							
172.21.1.93		65813911-e066-4ee3-a693-c0c8f00e7cee	2024-08-06 08:46:49	2024-08-06 08:46:51	SUCCESS	RPC :UNCHANGED	豊香日志 View configuration
🔹 🧰 TEST					Concessor 1	-	
172.21.1.110-url		azasc/sa-esar-este-9d2c-39d83c/e1cd5	2024-00-06 07:46:49	2024-00-06 07:46:51	SUCCESS	NHC IDIVCHARIOED	TELS New configuration
Cisco-172.21.1.160		459c0b53-a74c-45c6-87fd-4094335413ed	2024-08-06 06:46:49	2024-08-06 06:46:51	SUCCESS	RPC :UNCHANGED	● 日本 View configuration

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.

	Overview Configutation	Settin	ig Authority						
frame	Configuration Repo	Upio	ad Complete Active Rolback					C) I @
CO DATA	· Policy	Sele	cted 1 item						Cent
172 21 1 84	Security policy								
Internet-172.21.1.80	Object		Version	Update time	the length of config	Update source	Operation		
F5-192.168.60.132	Address Object		2025-03-20 1646:51 Active	2025-03-20 16:46:51	58722	Pulling Task	View Delete	e Download	d
manage-juniper-Route-	Time Schedule Object		2025-02-22 19:46:51	2025-02-22 19:46:51	58528	Pulling Task	View Delets	a Download	d
Manana-Huawai-Firawall-	URL Category Network	NO.	2025-02-22 18:46:51	2025-02-22 18:46:51	89	Pulling Task	View C Delete	Download	
172.21.1.84	Interface		2025-02-21 13:46:51	2025-02-21 13:46:51	58528	Pulling Task	View Delete	E I Download	
Analyze-Huawei-	Zone Router		2025-02-21 12:46:51	2025-02-21 12:46:51	58624	Pulling Task	View Delet	Download	d
172.21.1.93	Policy based routing		3035 03 13 12 42 51	2026 02 12 15 46 61	1917M	Duting Task	Mary Outer	-	
• 112 110 and			2023-02-13 124631	2023-02-13 1346(3)	30320	Pointy lask.	Vev Dees	i Downioad	
Cisco-172.21.1.160			2025-02-11 01:46:51	2025-02-11 01:4651	58001	Pulling Task	View Delets	Download	d
Balance			2025-02-11 00:46:50	2025-02-11 00:46:50	89	Pulling Task	View Delete	t Download	d .
192.168.60.132			2025-02-08 07:46:51	2025-02-08 07:46:51	58001	Pulling Task	View Delete	Download	0
• 💼 Business			2025-02-08 06:46:51	2025-02-08 06:46:51	58097	Pulling Task	View Deleti	Download	d
172.21.1.191			3035 03 03 08-46-51	2026 02 02 05 06-46-61	E8001	D dies Task	View Date	Deserves	
E FortiGat_172.21.1.162			2021-02-03 00/4031	2023-02-03 00:40.31	30001	Furing lask	Vev Leter	- Dominicati	-
testoisco			2025-02-03 07:46:52	2025-02-03 07:46:52	89	Pulling Task	View Deleti	/ Download	a.
panorama192.168.60.100			2025-01-24 09:46:51	2025-01-24 09:46:51	58001	Pulling Task	View Deleta	Download	0
gw-020000-1			2025-01-24 08/46/52	2025-01-24 08:46:52	58097	Putling Task	View Delet	e Download	a'
172.21.1.162-1			2025-01-18 04:46:56	2025-01-18 04:46:56	58001	Pulling Task	View Delete	Download	d
Circo. 172 21 1 160-2						10 17 18 1			
			2025-01-18 03:46:51	2025-01-18 03:46:51	58171	Putting Task	View / Delets	2 Download	ð.

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:

Device catalog 🜺 Analyze-Huawei-172.21.1.93 ② | 拼 🍄 🎯 싎 | Operation 🤟 erview Configutation Setting Authority 💼 frame 🔹 🗞 DATA Upload Compare CI® Selected 2 Item - 🚔 Domain 172.21.1.84 Version Internet-172.21.1.80 F5-192.168.60.132 Update time 2025-03-20 16:46:51 Active 2025-03-20 16:46:51 Pulling Task manage-juniper-Route-172.21.1.94 Manage-Huawei-Firewall 2025-02-22 19:46:51 2025-02-22 19:46:51 Pulling Task 2025-02-22 18:46:51 2025-02-22 18:46:51 Pulling Tasl 2025-02-21 13:46:51 172.21.1.84 2025-02-21 13:46:51 Pulling Task 58528 Analyze-Huaw 172.21.1.93 2025-02-21 12:46:51 2025-02-21 12:46:51 Pulling Tasl TEST 172.21.1.110-url Cisco-172.21.1.160 2025-02-13 15:46:51 2025-02-13 15:46:51 58528 Pulling Task 2025-02-11 01:46:51 2025-02-11 01:46:51 58001 Pulling Task 2025-02-11 00:46:50 2025-02-11 00:46:50 Pulling Task 🚔 Balance 2025-02-08 07:46:51 192,168,60,132 2025-02-08 07:46:51 58001 Pulling Task Business 172.21.1.191 2025-02-08 06:46:51 2025-02-08 06:46:51 58097 Pulling Task 2025-02-03 08:46:51 2025-02-03 08:46:51 Pulling Task FortiGat_172.21.1.162 2025-02-03 07:46:52 2025-02-03 07:46:52 Pulling Task testcisco panorama192.168.60.100 2025-01-24 09:46:51 2025-01-24 09:46:51 Pulling Task 2025-01-24 08:46:52 2025-01-24 08:46:52 58097 Pulling Task 2025-01-18 04:46:56 2025-01-18 04:46:56 58001 Pulling Task 2025-01-18 03:46:51 2025-01-18 03:46:51 58171 Pulling Task 172.21.1.80 -20 of 79 items < 1 2 3 4 > 20 / page or-172 21 1 00 Compare 2024-07-19 06:46:51 ← 2024-05-21 13:46:51 339 address 0 32.4.2.1 mask 255.255.255.255 address 0 32.4.2.1 mask 255.255.255.255 340 # 341 ip_address.set_172.20.1.60_32_type_object 342 __address_0_172.20.1.60_mask_255.255.255 343 # 344 ip_address-set_10.1.1.60_32_type_object 345 address_0_10.1.1.60_mask_255.255.255.255 347 ip_address.set 172.20.1.59 32_type_object 348 address_0 172.20.1.59 mask_255.255.255.255 350 ip address-set 10.1.1.59_32 type object address 0 10.1.1.59 mask 255.255.255.255 353 m 353 ip_address-set_10.1.1.34_32_type_object 354 address 0 10.1.1.34_mask_255.255.255.255 m ip address-set 172.20.1.34 32 type object address 0 172.20.1.34 mask 255.255.255.255 # ip_address-set 172.20.1.61_32_type_object address_0_172.20.1.61_mask_255.255.255.255 362 ip address-set 10.1.1.61 32 type object

iNet Intelligent Platform Operation Manual 2024

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

٩	Overview Configutation	Setting	Authority						
ame	Configuration Repo	Upload	Compare Active					С	J
Domain	Policy Security policy		Version	Update time	the length of config	Update source	Operation		
172.21.1.84	NAT policy		2025-03-29 23:58:42 Active	2025-03-29 23:58:42	4183	Pulling Task	View De	ete Download	
El Internet-172.21.1.80	Object		2025-03-29 23:28:44	2025-03-29 23:26:44	2822	Pulling Task	View De	ete : Download	
F5-192.168.60.132	Address Object Service Object		500 0 30 30 80 10	2010 02 26 22 20 20 21	4162	Pulling Task	Mars 1 Per	a l Barriero	
manage-juniper-Route-	Time Schedule Object		2023-03-28 22138/42	2063-03-20 2230942	4103	Formy lask	view De	Ine Dominoso	
Managa-Munusi-Eiroupli-	URL Category • Network		2025-03-26 22:28:45	2025-03-26 22:28:45	2822	Pulling Task	View De	ete Download	
172.21.1.84	Interface		2025-03-26 14:58:42	2025-03-26 14:58:42	4183	Putling Task	View De	ete Download	
Analyze-Huawei-	Zone		2025-03-26 14:28:44	2025-03-26 14:28:44	4279	Pulling Task	View De	ete Download	
172.21.1.93	Policy based routing		2025-03-25 16:28:42	2025-03-25 16:28:42	4183	Pulling Task	View De	ete Download	
TEST			2025 02 25 15 55 44	1015 02 15 15 55 44	3033	Bulling Tark	Mars 1 Per	ate Desitions	
172.21.1.110-url				2007-07-02 10/0011	- COLO	rang lan			
Cisco-172.21.1.160			2025-03-25 09(28)42	2025-03-25 09/28/42	4183	Pulling Task	View De	ste Download	
Balance			2025-03-25 08:58:44	2025-03-25 08:58:44	4279	Pulling Task	View De	ete Download	
Buriners			2025-03-24 23:58:42	2025-03-24 23:58:42	4183	Pulling Task	View De	ete : Download	
172.21.1.191			2025-03-24 23:28:43	2025-03-24 23:28:43	4279	Pulling Task	View De	ete Download	
E FortiGat_172.21.1.162			2025_03_24.05/28:42	2025_03_34.05/28:47	4183	Pulling Task	View De	ete Download	
testcisco			2013-07-07 031076	2023-07-07-07-07-07-07-07-07-07-07-07-07-07-	4105	rang lak			
🔜 panorama192.168.60.100			2025-03-24 04:58:43	2025-03-24 04:58043	4279	Putting Task	View De	ste Download	
gw-020000-1			2025-03-21 01:28:42	2025-03-21 01:28:42	4183	Pulling Task	View De	ete Download	
172.21.1.162-1			2025-03-21 00:58:43	2025-03-21 00:58:43	4279	Pulling Task	View De	ete Download	
E pa-192.168.60.99									

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

utform	颐 Dashboard ^Q & Change 운	२ Analyze 🗇 Search 🎕 Co	nfig					₽ ©	T 🛞 admin
^	Device catalog C	Analyze-Huawei-1	72.21.1.93 🥑 🕕 👭 🍄 🚳 🛗	Operation 🦆					
	Search	R Overview Configutation	Setting Authority						
	• 🚔 frame	Basic properties Advanced settings	Route update						
	- 🔂 Domain	Policy anchor	✓ Enable Repeat	V 30		Minute V	Save		
	172.21.1.184	NAT settings	Execution history			Second			сіф
	manage-juniper-	Connection check	Context ID	Start at	End at	Hour	Execution result	Operation	
	Route-172.21.1.94	Configuration update Configuration cleanup	5d14895d-7df2-4bd7-8b5b-52e663c71eb8	2024-08-06 11:28:40	2024-08-06 11:28:41	Day	RPC :UNCHANGED	查看日志 View	configuration
	Firewall-172.21.1.84	Hitcount update	f3c26059-6259-41e0-8e35-d82513ae081c	2024-08-06 10:58:40	2024-08-06 10:58:41	SUCCESS	RPC JUNCHANGED	查看日志 View	configuration
	Analyze-Huawei- 172.21.1.93		5892f143-2341-45ce-beee-f30ca196d4dd	2024-08-06 10:28:40	2024-08-06 10:28:42	SUCCESS	RPC :UNCHANGED	查看日志 View	configuration
	• TEST		20ce8fd9-9843-4e67-bf1b-0b082e775948	2024-08-06 09:58:40	2024-08-06 09:58:42	SUCCESS	RPC :UNCHANGED	査習日志 View	configuration
^	Clscn-172.21.1.160		deeRQQRh-h5a8-4107-a5ad-47h3hfa3dQ3f	2024-08-06 09:28:40	2024-08-06 09:28:41	SUCCESS	RPC LINCHANGED	春香日主 View	configuration

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.

Device ^	Device catalog	Analyze-Huawei-1	172.21.1.93 🧿 👘 👭 🎌 🎯 🚔 👘 🤅	Operation 🧅			
Catalogue	Search C	Overview Configutation	Setting Authority				
Credential	а.	*					
HA Group	 frame Data 	Configuration Repo Route Repo	Upload Compare Active				CI®
Template	• 📥 Domain	· Policy	Selected 1 Item				Clear
Task Setting	172.21.1.184	NAT policy					
Topology	F5-192.168.60.132	 Object 	Version	Update time	配置长度	Update source	Operation
IDANA	manage-juniper-	Address Object Service Object	2024-17-24 20:58:42 Active	2024-07-24 20:58:42	4183	Pulling Task	View Delete Download
IDAM	Route-172.21.1.94	Time Schedule Object	024-07-24 20:28:42	2024-07-24 20:28:42	2822	Pulling Task	View Delete Download
Model Details ^	Manage-Huawei-	URL Category		2024 07 10 10 20 42		D. How Task	Marcol Databa - Developed
Model	Firewall-172.21.1.84	Network Interface	2024-07-10 10/20142	2024-07-10 10:20142	4103	Putting tesk	view Delete Download
Relation	Analyze-Huawei-	Zone	2024-07-18 09:58:42	2024-07-18 09:58:42	4279	Pulling Task	View Delete Download
Association	• = TEST	Router	2024-07-13 15:58:42	2024-07-13 15:58:42	4183	Pulling Task	View Delete Download
Library A	😬 172.21.1.110-url	Policy based routing	2024-07-13 15:28:42	2024-07-13 15:28:42	4279	Pulling Task	View Delete Download
Lonary	Cisco-172.21.1.160		2024-07-12 15:58:42	2024-07-12 15:58:42	4183	Pulling Task	View Delete Download
Application(Huawel)	+ 🚔 Balance		2024-07-12 15-28-42	2024-07-12 15-28-42	4370	Dulling Task	View Delete Devening
Antivirus(PA)	192.168.60.132		2024-07-12 13:20:42	2024-07-12 13(20)42	4279	Putting task	view Delete Download

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:

0	INET platfo	rm	颐 Dashboard 약১ Change 원	Analyze 🖾 Search 🏨 Co	infig								لھ)	⊚ T ⊗ ad
:=	Device	^	Device catalog C	Analyze-Huawei-1	72.21.1.93	↓ # •	* 6 🕁	Operation 🕹						
	Catalogue		Search. Q	Overview Configuration	Setting	Authority								
	Credential		🕶 frame	Configuration Repo	default	radiony								
	Template		• 🗞 DATA	Route Repo Policy	L Export	Policy query	Expand of	oject details			Policy	V Please inp	ut Policy na	0.00
~	Task Setting		172.21.1.184 55-192.168.60.132	NAT policy • Object	Seq	Policy name	Source zone	© Destination area		Destination address	Service		on ⊽ Time	Operation
7. 品	IPAM		Route-172.21.1.94	Address Object Service Object Time Schedule Object	1	202404171 111_51d0	any	any	🗯 any	2 202404171111_cb38	🛊 any	any	🋊 any	命中详细
	Model Details Model	î	Manage-Huawei- Firewall-172.21.1.84 Analyze-Huawei-	URL Category Vetwork Interface	2	202404171 111_599d	any	any	2 202404171111_cb38	🌲 any	🛊 any	any	🛊 any	命中洋橋
	Relation Association		172.21.1.93	Zone Router Policy based routing	3	2023_09_18 _ed9bb	any	any	202309181528_b90f	🋊 any	🛊 any	any	🛊 any	命中详情
圇	Library Application(Huawei)	î	Clsco-172.21.1.160		4	2024_03_08 _78ea7	any	any	202403080930_dba8	202403080930_4dbe	2024030809	any	🛊 any	命中详情
	Antivirus(PA)		 Balance 192.168.60.132 Buringer 		5	2023_09_18 _35c79	any	any	2 202309181527_aee7	🌲 any	2023091815	any	🋊 any	命中详情
	Object Management	12.0	 Dosmess 172.21.1.161 FortiGat_172.21.1.162 		6	2023_09_18 _d127b	any	any	202309181509_bac8	🛊 any	2023091815	any	🌲 any	由中洋橋
			testcisco		7	2023_08_10 _0dec4	any	any	202308101518_4485	🛊 any	🛊 any	any	🛊 any	命中详情
			gw-020000-1 172.21.1.162-1		8	2023_07_21 aedfc	any	any	2 202307211421_3995	2 202307211421_178c	🛊 any	any	🛊 any	命中详惯
			Cisco-172.21.1.160-2							1-20 of 194	4 items < 1 2 3 4	5 10 3	20/nace V	Go to Par

- **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 \oslash Permit or Allow, \bigotimes represents Deny or Drop
- Policy query

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

Ø	INET platfor	m	國 Dashboard 원 Change 원	Analyze 🔞 Search 🏨 Co	nfig								<u>ل</u>	ЭT	(8) admir
=	Device	^	Device catalog C	Analyze-Huawei-1	72.21.1.93	o ⊨#+•	*© ∰	Operation \downarrow							
	Catalogue		Search Q	Overview Configutation	Setting	Authority									
	Credential		* 🚔 frame	Configuration Repo	default										
	HA Group		• 🚳 DATA	Route Repo			-								
	Template		👻 📴 Domain	Policy Security policy	ය. Export	Policy query	Expand obj	ect details			Policy V	Please input Pol	licy na	2 4	≎ ≎
	Task Setting		172.21.1.184	NAT policy			Source _	Destination							
K	Topology		F5-192.168.60.132	Object Address Object	Seq	Policy name	zone	area	 Source address 	Destination address	Service V	Application V	Time	Opera	ition
吊	IPAM		Route-172 21 1 94	Service Object		202404171				0 202404171111 -528	*			-	
	Model Details		Manage-Huawei-	Time Schedule Object		111_51d0	any	any	🗢 any	202404171111_C036	acry	any	· acty		- II.
	Model		Firewall-172.21.1.84	 Network 	2	202404171			202404171111 cb38	* 200	* ***		* 100	-	
	Delation		🔝 Analyze-Huawei-	Interface		111_599d	any	any	5 L0000000000	- any	any any	any	- eny		
	Nelation		172.21.1.93	Router		2023_09_18			202309181528 b00F	* are:	* ***		* ***	-	
	Association		 TEST 172 21 1 110 uni 	Policy based routing		_ed9bb	arty	any				any			- II.
⊜	Library	^	Cisco-172.21.1.160		4	2024_03_08	No.	No.	202403080930 dba8	202403080930 4dbe	2024030809		* ***	800	
	Application(Huawei)		• 🚘 Balance			_78ea7	- y	arry	•	•		any	•		
	Antivirus(PA)		192.168.60.132		5	2023_09_18	2011	anv	202309181527_aee7	🔹 arry	2023091815	anv	* any	命中道	6
	Object Management2	2.0	🝷 📥 Business			_35c79			-						
			172.21.1.161		6	2023_09_18	any	any	202309181509_bac8	🛊 any	2023091815	any	🛊 any	命中详	14

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

S Policy query			×
Action :	Please select	= ~	
Source address	Please enter the IP address and click ente	= ~	
Destination add	Please enter the IP address and click ente	= ~	
Protocol :	Please select V	=	
	Cancel	NOT IN Advanced query	Query

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"

=	\sim
=	
IN	
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:

Protoco	ol :	Please select	٩
		TCP 6	
		UDP 17	,
2 1	11	IP 4	
		ICMP 1	
2 3	202	ICMPv6 58	
-	ed'	HOPOPT 0	
, 2	202	IGMP 2	
4 -	78	GGP 3	
2	202	ST 5	

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.

Policy query			×
Action :	Please select	=	\sim
Source address	Please enter the IP address and click ente	=	\sim
Destination add	Please enter the IP address and click enter	=	\sim
	Heave enter their douress and ener entern		
Protocol :	TCP 6		
Protocol : Source port :	TCP 6 V Please input Source port	=	~

19 / 50

• 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.

E Device		^	Device catalog C	paloato Internet-172.21.1.	BO 🥑 🔢 👬	今 6 🗄	Operation 4							
Catalog	ue		Seath Q	Overview Configutation	Setting A	uthority								
Credent	tial		• 🚔 trama	Configuration Rang	NAT policy									
HA Grou	up		• 🚳 DATA	Route Repo	-									
Templat	te		- 🚔 Domain	Policy	Export Bg	and object details					Policy name	V Please input Policy	name	9 0 6
Task Set	tting		El Internet-172.21.1.80	NAT policy					Source		Destination	Destintaion	Source address(Before	Destination ad
Topolog	ay		172.21.1.184	Object Address Object	□ Sed #	Policy name	type v	Status V	zone	Source interface	area	interface	conversion)	conversion)
R IPAM			F5-192.168.60.132	Service Object										
Model [Details	•	Route-172.21.1.94	Time Schedule Object		95	SNAT	\odot	any	12	unturst	ethernet1/2	& W5-172.20.1.53_255.255	2 WS-202.2.1.5
Ale del			Manage-Huawei-	User object										
Model			Firewall-172.21.1.84	应用组	2	iNet_77c5f_0	DNAT	\odot	unturst		dmz1	ethemet1/1	2 CTC	& WS-172.20.1
Relation	1		Analyze-Huawei-	interface										
Associat	tion		172.21.1.93	Zone	3	iNet_37ca408	DNAT	۲	unturst	5 - C	dmz1	ethernet1/1	& W5-202.2.1.42_255.255.2	& WS-172.20.1
Library		^	 TEST 172.21.1.110-url 	Router Policy based routing		~								

- 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.

Device	^	Device catalog	palato Internet-172.21.1.	80⊘ \$\$\$	🌵 🌀 🚊 🗆	Operation	Ŷ						
Catalogue		Search Q	Overview Configutation	Setting Au	thority								
Credential			Conferentine Base	NAT policy									
HA Group			Route Repo	_									
Template		+ 🚔 Domain	Policy Security policy	Export Exp	ind object details					Policy name	✓ Please input Polic	ty name	Q (C) (\$
Task Setting		Internet-172.21.1.80	NAT policy	Seq #	Policy name	Type	7 Status N	Source	☑ Source interface	Destination	Destintaion	Source address(Before	Destination addre
Topology		F5-192,168.60.132	Address Object					zone		area	internace	conversion)	conversiony
Model Details	•	Route-172.21.1.94	Service Object Time Schedule Object	. 1	iNet_e163be 95	SNAT	۲	any		unturst	ethernet1/2	& WS-172.20.1.53_255.255	& ws-202.2.1.5
Model		Manage-Huawei- Firewall-172.21.1.84	User object 应用组	2	iNet_77c5f_0	DNAT	۲	unturst		dmz1	ethernet1/1	2 стс	& WS+172.20.1
Relation Association		Analyze-Huawei- 172.21.1.93	Network Interface Zone		iNet_37ca408	DNAT						Q WE 200 0 (40 000 0 C 20 0 C	9 105-172 20 1
} Library	^	 TEST 172 21 1 110 url 	Router Policy based routing	3	5	UniAl	U	untuist	-	amz I	etnemet1/1	 ws-cuc.c.1Ac_200.2002 	5 wa-1/220.1
Application(Huav	wei)	Cisco-172.21.1.160		□ x	iNet_d59bab	DNIAT	•					• WC.172 20 1 122 255 25	0 wc.202211

• Before expanding object details

• After expanding the object details

:=	Device	^	Device catalog	patoatto Internet-172.21.1.8	i0⊘ ##	∲ © ☆ I	Operation \downarrow							
	Catalogue		Search Q	Overview Configutation	Setting Au	hority								
	Credential			Conferenting Data	NAT policy									
	HA Group		• 🔂 DATA	Route Repo										
	Template		🕶 🚔 Domain	Policy Security policy	Export	pse object details					Policy name	 Please input Policy 	rame	0.0
	Task Setting		El Internet-172.21.1.80	NAT policy	C. See 8	Delineerse	Terre VI	Status 17	Source	T. Course interface	Destination	Destintaion	Source address(Before	Destination addre
¥	Topology		172.21.1.184	 Object Address Object 	- Jud -	Policy name	type a	Juliu U	zone	5 Source memore	area	interface	conversion)	conversion)
읆	IPAM		F5-192.168.60.132	Service Object Time Schedule Object	1	iNet_e163be	SNAT	⊙	anv		unturst	ethemet1/2	172.20.1.53/32	202.2.1.53/
	Model Details	^	Route-172.21.1.94	URL Category		95								
	Model		Firewall-172.21.1.84	User object 应用组	2	iNet_77c5f_0	DNAT	۲	unturst		dmz1	ethemet1/1	202.2.1.1/24	172.20.1.5/
	Relation		Analyze-Huawei-	 Network Interface 		iNet_37ca408	ONIST							
圇	Library	<u>`</u>	• 🔤 TEST	Zone Router	3	5	DINAI	U	unturst	-	dmz1	ethemet1/1	2022.13252	1722013/
	Application(Huawei)	Clsco-172.21.1.160	Policy based routing	4	iNet_d59bab	BNAT	•	devr1		unturst	ethemet1/2	172.20.1.133/32	202.2.1.1/3
	Antivirus(PA)		🕶 🚔 Balance			d6		-						
	Object Managemen	it2.0	 192.168.60.132 Business 172.21.1.161 		5	iNet_1a9b4a 64	SNAT	•	dmz1		unturst	ethemet1/2	• 172.20.1.48/32	 202.2.1.48/

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.

6	INET platf	arm	뛯 Dashboard 원 Change 원	Analyze 🔞 Search 🚳 Cor	nfig							GI (⊚ T ⊛ad	lmin
=	Device	^	Device catalog C	Analyze-Huawei-17	72.21.1	1.93 📀 🕕 👫 🍫 🎯 🗁	Operatio	n J						
	Catalogue		Search Q	Overview Configutation	Settin	g Authority								
	Credential HA Group		• 💼 frame	Configuration Repo Route Repo								Name V Please input Name	9.0	٢
	Template		 Domain Internet-172.21.1.80 	 Policy Security policy NAT policy 		Name	Туре	Managed state state	Predefined V	Interface / Zone	Members	Exclude members	Operation	
¥	Topology		172.21.1.184	Object		WS_10.1.1.5_255.255.255.255	Object		False	global	10.1.1.5/255.255.255.255			î
品	IPAM Model Details		15 F5-192.168.60.132 manage-juniper- Boute-172.211.94	Service Object Time Schedule Object		WS_10.1.1.44_255.255.255.25 5	Object		False	global	10.1.1.44/255.255.255.255			l
-	Model		Manage-Huawei- Firewall-172.21.1.84	Network Interface		WS_172.18.1.5_255.255.255.2 55	Object	-	False	global	172.18.1.2/255.255.255.255 172.18.1.5/255.255.255.255	-		l
	Relation Association		Analyze-Huawei- 172.21.1.93	Zone Router Policy based routing	Interface 5 Zone Router V Policy based routing 5	WS_172.20.1.4_255.255.255.2 55	Object		False	global	172.20.1.4/255.255.255.255			1
।	Library Application(Huaw	ei)	 T2.21.1.110-url Clsco-172.21.1.160 			WS_10.1.1.41_255.255.255.25 5	Object		False	global	10.1.1.41/255.255.255.255			
	Antivirus(PA)		• 🚔 Balance			WS_172.18.1.35_255.255.255.	Object	-	False	global	172.18.1.35/255.255.255.255			

- 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

😑 Device 🔺 🗿 Device catalog C 🙌 Analyze-Huawei-172.21.1.93 Ο 🗰 🖓 🚳 🛱 Cρωτείου 4		
Catalogue Search. Q. Overview Configuration Setting Authority		
Credential		
HA Group Report Former Configuration Report Export Name V	ame V Please input Name Q	0
Template Poly Manager		
remplate Comain Security policy □ Name Type V state Predefined V Portocol Long connecti	ig connection ReferenceDescription Op	peration
Task Setting NAT policy		
Y Topology Topology TOP.log 42 Object False TCP.log 42 Topology	4 created by Servio	
IPAM Environment initiation Environment		
Model Datality A Route-172-211.94 Electrony 20230628094 Chiefer Comp	service merge by	
A Manaa-Huavei	bc63d79d	Hosting
Model Firewall-172.21.1.84 Interface		
Relation Zone 29 Object - False TCP: Target 6 -	o -	
Association 172.21.1.93 Policy based routing TCP 3321 Object - False TCP tanget 321 -	g created by Service	
□ 26 Object - False TCP: Terret 4 -	0 -	
Application(Huave) 51 Object - Edua 70 Tene 7		
Antivirus(PA) - Balance	· · ·	
Object Management2.0 LS 192.168.60.132 35 Object - False TCP: Target 9 -	o -	
- 🚔 Business		
172.21.1.161 UDP_34654 Object - Halse UDP_Target 54654 -	1 created by Servio	
E FortiGat_172.21.1.162 20230714093 Chief course antifunction Enter	service by inet bk	
testcisco	65965e2f	nouning
Separarana 192.168.60.1	and the first land late	

- 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

6	INET platform	뛓 Dashboard 약à Change 원	Analyze 🖾 Search 🎕 Co	nfig				6	T	@ a	idmi
=	Device ^	Device catalog C	Analyze-Huawei-1	72.21.1.93 🕑 🔢 👯 🍫	🎯 🔓 🕴 Operation 🗸						
	Catalogue	Search Q	Overview Configutation	Setting Authority							
	Credential HA Group	• 🚔 frame • 🗞 DATA	Configuration Repo Route Repo	Export		Terrardonia	Please input Name		٩	0	\$
	Template Task Setting	 Domain Internet-172.21.1.80 	Security policy NAT policy	Name	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	21 -				h
ų K	Topology	 172.21.1.184 F5-192.168.60.132 	 Object Address Object Service Object 	10	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				-
m ⊜	Model Details	Route-172.21.1.94	Time Schedule Object URL Category	. 11	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
	Model	Manage-Huawei- Firewall-172.21.1.84	Network Interface Tage	. 111	Object group	2022-12-01 15:44:18 - 2024-01-06 15:43:35 Tuesday 02:00:01 - 03:00:00	1 -				
	Association	Analyze-Huawei- 172.21.1.93	Router Policy based routing	12	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
⊜	Library ^	 TEST 172.21.1.110-url 		13	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
	Application(Huawei)	Clsco-172.21.1.160		. 14	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
	Object Management2.0	• Balance [13] 192.168.60.132		15	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
		 Business 172 21 1 161 		16	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
		FortiGat_172.21.1.162		17	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				
		testcisco		18	Object group	2022-12-01 15:44:18 - 2023-04-28 15:55:35	0 -				

- **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:

6	INET plat	form	圆 Dashboard 🗞 Change - 쉱	Analyze 🔯 Search 🤹 C	onfig								- Gi	⊚ T ⊚ adr	min
:=	Device	^	Device catalog C	Analyze-Huawei-	172.21.1	.93⊘ ା ∰ 🎌 🎯 🗄	- Operatio	n U							
	Catalogue		Search	Overview Configutation	Settin	g Authority									
	Credential		🝷 🚔 frame	Configuration Repo	Physical	Loop VLAN Tunn	el Aggregatio	on virtualif							
	Template		 DATA Domain 	Route Repo Policy							Nam	e V Pla	ase input Name	۹ 0	10
	Task Setting		Internet-172.21.1.80	NAT policy • Object		Name	Status 🛛	Address	IPv6 addre	ess Zone	Log	ical 😗	Virtual routing table	Description	
出	Topology		F5-192.168.60.132	Address Object Service Object	+	GigabitEthernet1/0/4	Enable	192.168.1.1/24	2001::2/64		pub	dic	global		
	Model Details	^	Route-172.21.1.94	Time Schedule Object URL Category	+	GigabitEthernet1/0/3	Enable	10.60.1.2/24			pub	dic	global		
	Model		Manage-Huawei- Firewall-172.21.1.84	Network Interface	+	GigabitEthernet1/0/2	Enable	10.172.1.1/24			pub	dic	global		
	Relation		Analyze-Huawei-	Zone Router	+	GigabitEthernet1/0/1	Enable	10.28.1.2/24			pub	dic	global		
圇	Library	^	+ EST	Policy based routing	+	GigabitEthernet1/0/0	Enable	172.23.1.2/24			pub	lic	global		
	Application(Huaw	vei)	Clsco-172.21.1.160		+	GigabitEthernet0/0/0	Enable	172.21.1.93/24			pub	lic	global		
	Antivirus(PA)												1-6 of 6 items	< 1 > 20/pag	je N
	Object Managem	ient2.0	 Business 												

- 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:

Ø	INET platf	arm	國 Dashboard 🗞 Change - 영	Analyze 🔞 Search 🤹 Co	nfig						🕼 💿 T 🛞 admin
:=	Device	^	Device catalog C	Analyze-Huawei-17	72.21.1.93 🕑 👫 *	🎙 🎯 📩 🕴 Operation 🤅					
	Catalogue		Search Q	Overview Configutation	Setting Authority						
	Credential HA Group		• 📅 frame	Configuration Repo Route Repo						Name V Please input Na	me Q O 🕸
	Template		• 🔂 DATA	Policy Ceruity policy	Name	Logical system	Interface	Description	Priority	Туре	Regional flow control
	Task Setting		Linternet-172.21.1.80	NAT policy	dmz1	public	1	-	55	LAYER2_3	Not enabled
¥	Topology		5 F5-192.168.60.132	Object Address Object	dmz	public	1		50	LAYER2_3	Not enabled
品	IPAM		manage-juniper-	Service Object Time Schedule Object	untrust	public	0		5	LAYER2_3	Not enabled
	Model Details	^	Route-172.21.1.94 Manage-Huawei-	URL Category • Network	trust	public	1		85	LAYER2_3	Not enabled
	Model		Firewall-172.21.1.84	Interface Zone	local	public	0		100	LAYER2_3	Not enabled
^	Association		Analyze-Huawei- 172.21.1.93	Router Policy based routing						1-5 of 5	items < 1 > 20 / page \vee

- 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:

6	INET platform	B Dashboard 약ය Change 운	Analyze 🔯 Search 🍓 Config								Ð	۲	Т	(8) adn	
=	Device •	Device catalog C	Analyze-Huawei-172.2	21.1.93	o 🕕 👬 🍫 🚳 E	3 I 9	peration \downarrow								
	Catalogue	Search Q	Overview Configutation Se	etting	Authority										
	Credential HA Group	• frame	Configuration Repo Route Repo	Uploa	d L Export				IPv4 IPv6	Please input Destination		Q	С	I	
	Template	- Domain	 Policy 		Virtual routing table	Ŧ	Destination	Next hop	Metric		Interface			Ŧ	
	Task Setting	Internet-172.21.1.80	NAT policy		Public		0.0.0.0	172.21.1.1	0	STATIC	GigabitEtherr	et0/0/0			
¥	Topology	172.21.1.184	Object Aritiess Object		Public		10.1.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1			
品	IPAM	manage-juniper-	Service Object Time Schedule Object URL Category	Service Object	Service Object	Public		10.25.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1		
	Model Details	Route-172.21.1.94			Public		10.26.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1			
	Model	Manage-Huawei-	 Network Interface 		Public		10.27.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1			
	Relation	Analyze-Huawei-	Zone		Public		10.28.1.0/24	10.28.1.2	0	DIRECT	GigabitEtherr	et1/0/1			
	Association	172.21.1.93	Policy based routing		Public		10.28.1.2/32	127.0.0.1	0	DIRECT	GigabitEtherr	et1/0/1			
⊜	Library ^	• 🚞 TEST			Public		10.29.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1			
	Application(Huawei)	Clsco-172.21.1.160			Public		10.30.1.0/24	10.28.1.1	0	STATIC	GigabitEtherr	et1/0/1			
	Antivirus(PA)	👻 🚔 Balance			Public		10.60.1.0/24	10.60.1.2	0	DIRECT	GigabitEtherr	et1/0/3			
	Object Management2.0	192.168.60.132			Public		10.60.1.2/32	127.0.0.1	0	DIRECT	GigabitEtherr	et1/0/3			
		 Business 172.21.1.161 			Public		10.172.1.0/24	10.172.1.1	0	DIRECT	GigabitEtherr	et1/0/2			
		FortiGat_172.21.1.162			Public		10.172.1.1/32	127.0.0.1	0	DIRECT	GigabitEtherr	et1/0/2			

- 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.

🚫 INET platform	뗼 Dashboard 🖓 Change 😡	Analyze 🔯 Search 🎕 Co	onfig			
E Device	Device catalog C	Analyze-Huawei-1	172.21.1.93 📀	耕 🍄 🎯 🔓 Operation 🎍		
Catalogue	SearchQ.	Overview Configutation	Setting A	luthority		
Credential	A (1997)					
HA Group		Advanced settings	Basic proper	rties		
Template	- Domain	Policy anchor	* Device name:	Analyze-Huawei-172.21.1.93		
Task Setting	Internet-172.21.1.80	NAT settings				
Topology	172.21.1.184	▼ Task	* Vendor:	Huawei 🗸		
IRAM	f5 F5-192.168.60.132	Connection check Configuation update	* Model:	USG6000 V		
	manage-juniper-	Configuration cleanup	t Marrie a			
Model Details	Route-1/2.21.1.94	Route update	* Version :	V100R001C305PCa00		
Model	Firewall-172.21.1.84	incount apoute	* Business domai…	Domain		
Relation	Analyze-Huawei-	-	Description:			
Association	172.21.1.93					
Library ^	🕶 💼 TEST			li di		
Application(Huawei)	🔜 172.21.1.110-url		* Management I…	172.21.1.93		
Aptivious(PA)	Cisco-172.21.1.160		* Portocol :	V H22		
Antivirus(PA)	 Dalance 192 168 60 132 					
Object Management2.0	Business		* Port:	22		
	172.21.1.161		* Credentials:	华为 🗸		
	EnrtiGat_172.21.1.162					
	testcisco		* Management ···	Collect only		
	panorama192.168.60.1		Working mode:	Routing		
	gw-020000-1	HA group;				
	172.21.1.162-1					
	Cisco-172 21 1 160-2		Logical system :	Please enter		
	GIGCO-172121111100-2 V					

- **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 dropdown 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.

Ø	INET platform	n	B Dashboard 원 Change 원	Analyze 🗔 Search 🎕 Co	onfig	
:=	Device 🔺	•	Device catalog C	Analyze-Huawei-1	72.21.1.93 🧭 👘 👫 🍫 🌘	多 品 Operation ↓
	Catalogue		Search Q	Overview Configutation	Setting Authority	
	Credential			-		
	HA Group		 frame DATA 	Basic properties Advanced settings	Advanced settings	
	Template		• 😥 DATA	Policy anchor		
	Tack Sotting		Internet-172.21.1.80	NAT policy anchor	* Coding :	UTF-8
	Task Setting		172.21.1.184	 Task 	* Time zone :	Asia/Shanghai \lor
<u>~</u>	lopology		f5 F5-192.168.60.132	Connection check	* Object group reference :	Object group reference object
꿃	IPAM		manage-juniper-	Configuration update Configuration cleanup	object group references	object group receive object
03	Model Details	•	Route-172.21.1.94	Route update	øbject reference:	referencing object name \lor
	Model		Manage-Huawei-	Hitcount update	Set the new config as active :	True
	Relation		Firewall-172.21.1.84			
	Accoriation		172 21 1 93		Master device identification:	False V
~	Association		- TEST			Save
	Library	`	🚨 172.21.1.110-url			
	Application(Huawei)		the Clsco-172.21.1.160			
	Antivirus(PA)		👻 🖶 Balance			
	Object Management2.0	0	f5 192.168.60.132			

- 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.

() INET platfo	rm	颐 Dashboard 원 Change 등	Analyze 🔞 Search 🚳 Co	onfig					Q ©	Т	le admin
	Device	^	Device catalog C	◆ paloaito か公网互联网防火が	墻PA-172.21.1.80 ⊙	🕴 🍄 🎯 🎰 🕴 Operation 🕹						
	Catalogue		Search O	Overview Configutation	Setting Authority							
	Credential HA Group		172.21.1.93	Basic properties	NAT settings							
	Template		 TEST 172.21.1.110-url 	Policy anchor NAT policy anchor	Policy delivery settings							
	Task Setting		Cisco-172.21.1.160	NAT settings	NAT Predefined rules NAT 3	地址地						
K	Topology		 Balance 192.168.60.132 	Task Connection check	New Delete Export	Import					C	. I ©
E G	IPAM Model Details	^	 Business 172 21 1 161 	Configuration update Configuration cleanup	Source address	Destination address	Service	NAT Type T Sou	arce address(After conversion)	Destination add	Operation	1
260	Model		FortiGat_172.21.1.162	Hitcount update User collection		172.20.1.5/32		DNAT -		conversion)	Edit	Delete
	Relation		testcisco		172.20.1.0/24			SNAT 20	02.2.1.5/32		Edit	Delete
	Association		gw-020000-1		<							•
Ê	Library Application(Huawei	î	pa-192.168.60.99							1-2 of 2 items <	1 >	20/page ∨

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".

0	INET plat	lorm	행 Dashboard 약6 Change 원	Analyze 🔯 Search 🕵 Co	onfig						ц.	0	I' (® admir
	Device	^	Device catalog C	Analyze-Huawei-1	72.21.1.93	> ↓ # � © ☆	Operation 4						
	Catalogue		Search	Overview Configutation	Setting	Authority							
	Credential HA Group		+ 🚔 frame	Basic properties Advanced settings	Connectio	on check							
	Template		+ 🧰 Domain	Policy anchor NAT policy anchor	🛃 Enable	Repeat	~ 5		Minute 💚	Save			
	Task Setting		Internet-172.21.1.80	NAT settings Tesk	Execution	history						(CI ©
k	Topology		F5-192.168.60.132	Connection check	Context ID		Start at	End at	Status	Execution result		Opera	tion
- -	IPAM Model Details	•	Route-172.21.1.94	Configuration optime Configuration cleanup Route update	5a9c4165-e	eac5-4fb0-ba21-5be8b2e9467a	2024-08-06 16:59:36	2024-08-06 16:59:37	SUCCESS	RPC RUNNING		285	18
	Model		Manage-Huawei-	Hitcount update	b25dc2c4-	1937-406f-b355-df443e5b7da5	2024-08-06 16:54:36	2024-08-06 16:54:37	SUCCESS	RPC RUNNING		200	18
	Relation		Analyze-Huawei-		4ac686a8-c	856e-49cd-a429-2568891c1ca0	2024-08-06 16:49:36	2024-08-06 16:49:37	SUCCESS	RPC RUNNING			Batt
	Association		172.21.1.93		a547c0ea-b	945a-4a4f-8dbd-c042e126e10c	2024-08-06 16:44:36	2024-08-06 16:44:37	SUCCESS	RPC RUNNING		-	at
	Library	•	• 172.21.1.110-url		dbb7e4cb-	4109-4691-6009-3c29e4c76916	2024-08-06 16:39:36	2024-08-06 16:39:37	SUCCESS	RPC RUNNING		200	38
	Antivirus(PA)	et)	Cisco-172.21.1.160 Balance		e182cc1d-b	e64-4694-8e0a-69070f8635e0	2024-08-06 16:34:36	2024-08-06 16:34:37	SUCCESS	RPC RUNNING		285	38

29 / 50

• 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.

6	INET platform	ම Dashboard ^ල යි Change ල	Analyze 🔞 Search 🍓 Co	nfig					🖓 💿 T 🛞 admin
:=	Device •	Device catalog C	Analyze-Huawei-1	72.21.1.93 ② 🛛 👭 🍄 🎯 🚖	Operation 🧅				
	Catalogue	Search Q	Overview Configutation	Setting Authority					
	Credential	🔹 🚍 frame	Basic properties	Connection check					
	HA Group	 Mane DATA 	Advanced settings	Connection check					
	Template	+ 🚘 Domain	Policy anchor	Z Enable Repeat	V 5		Minute 🗸	Save	
	Task Setting	Let Internet-172.21.1.80	NAT settings	Everytian bistory					ст е
¥	Topology	172.21.1.184	Task Connection check	Context ID	Shart at	End at	Chabur	Evention rendt	Operation
品	IPAM	manage-juniper-	Analyze Stand Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration spatiate Configurate	CONCILID	June of		Status	Creation (Call	operation
	Model Details	Route-172.21.1.94		5a9c4165-eac5-4fb0-ba21-5be8b2e9467a	2024-08-06 16:59:36	2024-08-06 16:59:37	SUCCESS	RPC :RUNNING	重要日志
	Model	Manage-Huawei-	Hitcount update	b25dc2c4-1937-406f-b355-df443e5b7da5	2024-08-06 16:54:36	2024-08-06 16:54:37	SUCCESS	RPC :RUNNING	查看日志
	Relation	Firewall-172.21.1.84	User collection	4ac686a8-db6e-49cd-a429-2568891c1ca0	2024-08-06 16:49:36	2024-08-06 16:49:37	SUCCESS	RPC :RUNNING	童智日志
	Association	172.21.1.93							
命	Library A	🔹 🧰 TEST		ab47c0ea-b4ba-4a4f-8dbd-c042e12be10c	2024-08-06 16:44:36	2024-08-06 16:44:57	SUCCESS	KPC :RUNNING	皇皇曰志
-114	Application(Huawei)	172.21.1.110-url		dbb7e4cb-4f09-4d9f-b009-3c29e4c7b9fb	2024-08-06 16:39:36	2024-08-06 16:39:37	SUCCESS	RPC :RUNNING	童君日志
	Antivious(PA)	Cisco-172.21.1.160		e182cc1d-bef4-4b94-8e0a-69070f8b35e0	2024-08-06 16:34:36	2024-08-06 16:34:37	SUCCESS	RPC RUNNING	重要日志
	Object Management2.0	 Balance 192.168.60.132 		1de76714-3d75-4d7c-82ea-908b116e2e35	2024-08-06 16:29:36	2024-08-06 16:29:37	SUCCESS	RPC :RUNNING	空間日志

• 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.

N INET platform Sp Dubboard % Change A Analyze E Search € Config © □												
=	Device	^	Device catalog C	Analyze-Huawei-1	72.21.1.93 🧭 👘 👫 🍄 🎯 🚔	Operation 🧅						
	Catalogue		Search Q	Overview Configutation	Setting Authority							
	Credential HA Group		• 🚔 frame • 🗞 DATA	Basic properties Advanced settings	Configuation update							
	Template		🔹 🚘 Domain	Policy anchor NAT policy anchor	Z Enable Repeat	× 1		Hour V	Save			
	Task Setting		Internet-172.21.1.80	NAT settings Task	Execution history						CI\$	
r	lopology		F5-192.168.60.132	Connection check	Context ID	Start at	End at	Status	Execution result		Operation	
응	IPAM Model Details	^	manage-juniper- Route-172.21.1.94	Configuration update Configuration cleanup ce	cef6fb0c-30c6-43bd-8d4d-938f33c871fe	2024-08-06 16:46:49	2024-08-06 16:46:51	SUCCESS	RPC :UNCHANGED		查查日志 View configuration	
	Model		Manage-Huawei-	Hitcount update User collection	22bafbbe-1457-4573-9c92-1f3e3bcd2792	2024-08-06 15:46:49	2024-08-06 15:46:51	SUCCESS	RPC :UNCHANGED		查看日志 View configuration	
	Relation		Analyze-Huawei-		f5ba4d84-064c-4320-ba94-412db651fae3	2024-08-06 14:46:49	2024-08-06 14:46:51	SUCCESS	RPC :UNCHANGED		宣誓日志 View configuration	
	Association		172.21.1.93		79ad16fe-50e1-41ad-aa35-d6022dbed10f	2024-08-06 13:46:49	2024-08-06 13:46:51	SUCCESS	RPC :UNCHANGED		查看日志 View configuration	
	Library	î	172.21.1.110-url		94c814d9-7bce-4f16-9dc3-500fbab10e53	2024-08-06 12:46:49	2024-08-06 12:46:51	SUCCESS	RPC :UNCHANGED		查看日志 View configuration	
	Application(Huawe	ei)	Cisco-172.21.1.160		3a71b48a-80c9-4a6a-9a9a-8H4HdH46af23	2024-08-06 11:46:49	2024-08-06 11:46:51	SUCCESS	RPC JUNCHANGED		查查日志 View configuration	
	Ohiart Mananama	ant2.0	192.168.60.132		#10266706-5080.00%626-#35-404#0	2024-08-06 10-86-49	2024-08-06 10:46-61	CHANGES	PDC-HINCHANGED		aant Max configuration	

• 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.

\bigotimes	INET plat	form	圆 Dashboard 🗞 Change 🛞	Analyze 🔯 Search 🥵 Co	onfig						🕼 🛞 T 🛞 admir
:= ,	Device	^	Device catalog C	Analyze-Huawei-1	172.21.1.93	◎ ↓ 井 � ◎ ⇔	Operation &				
	Catalogue		Seath	Overview Configutation	Setting	Authority					
+	Credential HA Group		frame And DATA	Basic properties Advanced settings	Configura	tion cleanup					
07	femplate		• 💼 Domain	Policy anchor NAT policy anchor	Enable						
K	fask Setting		internet-172.21.1.80	NAT settings • Task		Max version of config to keep					
吊	PAM		F5-192.168.60.132	Connection check Configuation update		Nax duration of config to kee	10 (in the second se				
	Model Details	•	Route-172.21.1.94	Configuration cleanup		Max version of route to keep					
	Vlodel		Manage-Huawei-	Hitcount update		Max version of route to keep				Seve	
F	Relation		Analyze-Huamei-		Execution I	history					CIO
	Association		172.21.1.93		Context ID		Start at	End at	Status	Execution result	Operation
ê l	Library	^	 TEST 172.21.1.110-ort 		0c4eff6c-40	0a-4c23-ba77-eb1c33cb4c57	2023-09-18 11:57:24	2023-09-18 11:57:24	SUCCESS	RPC:SUCCEED	建春日本
1	Application(Huav	ivei)	Cisco-172.21.1.160		a70c1d8b-c	a48-4a20-9156-1b5ecd07c93f	2023-09-17 11:57:24	2023-09-17 11:57:24	SUCCESS	RPC SUCCEED	2253
1	Antivirus(PA) Dhiart Mananam	n Street	 Balance 192.168.60.132 		7d7cd4e1-6	819-4499-b118-26fe948138b5	2023-09-16 11:57:24	2023-09-16 11:57:24	SUCCESS	RPC:SUCCEED	2005

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.

=	Device	^	Device catalog C	Analyze-Huawei-17	72.21.1.93 (シ᠃╫ゃ๏싎	Operation 🕹				
	Catalogue		Search Q	Overview Configutation	Setting	Authority					
	Credential		a. 1								
	HA Group		 frame R DATA 	Basic properties Advanced settings	Route up	iate					
	Template		• 🚰 Domain	Policy anchor NAT policy anchor	🗹 Enable	Repeat	V 30		Minute	Save	
	Task Setting		Internet-172.21.1.80	NAT settings	Execution	istory					C T M
۶ť	Topology		172.21.1.184	Task Connection check	Execution	listory	6	P. 1. 1	0	for the second	
P	IPAM		F5-192.168.60.132	Configuation update	Context ID		start at	End at	Status	Execution result	Operation
~	Madel Details		manage-juniper-	Configuration cleanup	19b#60b5~e	546-49fe-a18b-e060e7b9e797	2024-08-06 16:58:40	2024-08-06 16:58:41	SUCCESS	RPC:UNCHANGED	董君日志 View configuration
1	Model Details	^	Koute-1/2.21.1.94	Route update					(autorea	886 (1)(d)(1)(d)	
	Model		Einemall 172 21 1 84	User collection	eated518-e	sea-4331-8770-977a3C316293	2024-08-06 16:28:40	2024-08-06 16:28:41	SUCCESS	RPC JUNCHANGED	Table View configuration
	Relation		Analyze-Huawei-		538a76ef-3	e71-49e7-98b8-a0b6a0c1567f	2024-08-06 15:58:40	2024-08-06 15:58:43	SUCCESS	RPC :UPDATED	查看日志 View configuration
	Association		172.21.1.93		8c364bbb-	2e3-4f23-bfd2-81df1f2e627a	2024-08-06 15:28:40	2024-08-06 15:28:43	SUCCESS	RPC :UPDATED	查看日志 View configuration
⊜	Library Application/Huawe	â	172.21.1.110-url		dafa677b-b	78a-4d96-8917-0H76011c742	2024-08-06 14:58:40	2024-08-06 14:58:41	SUCCESS	RPC (UNCHANGED	重看日志 View configuration

• 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.

Ø	INET plat	tform	똃 Dashboard 약a Change 응	Analyze 🔞 Search 🎕 Co	nfig					₩ © T ®	admin
=	Device	^	Device catalog C	Analyze-Huawei-1	72.21.1.93 🧭 🕕 👭 🍄 🚳 🚖	Operation \downarrow					
	Catalogue		Search Q	Overview Configutation	Setting Authority						
	Credential HA Group		• 🚔 frame	Basic properties Advanced settings	Hitcount update						
	Template		• 🚰 Domain	Policy anchor NAT policy anchor	✓ Enable Repeat	✓ 1		Day V	Save		
	Task Setting		Internet-172.21.1.80 172.21.1.184	NAT settings Task	Execution history					CI	٢
k	Topology		f5 F5-192.168.60.132	Connection check	Context ID	Start at	End at	Status	Execution result	Operation	
吊	IPAM		manage-juniper-	Configuation update	+120/201-064-4420-0820-6+(541100-6+	2024-08-06 11/67-24	2024-08-06 11/57/26	CHARGE	PDC JIEDATED		_
	Model Details	^	Route-172.21.1.94	Route update		2000-00-00-00-00-00-00	2029-08-00 113720		N°C DPORED	12 CHIO	
	Model		Manage-Huawei- Firewall-172.21.1.84	Hitcount update User collection	03b5d2db-feca-44ad-85b9-f84996e6416f	2024-08-05 11:57:24	2024-08-05 11:57:26	SUCCESS	RPC :UPDATED	堂書日志	
	Relation		🙆 Analyze-Huawei-		64c5d8e3-c8dd-49d6-87cd-f0c621741cd9	2024-08-04 11:57:24	2024-08-04 11:57:25	SUCCESS	RPC :UPDATED	查看日志	
	Association		172.21.1.93		998eb294-90e0-484b-9dba-ce6dd709ea80	2024-08-03 11:57:24	2024-08-03 11:57:25	SUCCESS	RPC (UPDATED	度要日本	_
।	Library	^	 TEST 172.21.1.110-url 		e4108def-d393-4ab9-82a5-34707d90932c	2024-08-02 11:57:24	2024-08-02 11:57:26	SUCCESS	RPC (UPDATED	東晋日本	-
	Application/Hua	wei)	_								

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"

🚫 INET platform	뛯 Dashboard 원	Change 🛛 An	alyze 🔯 Sear	rch 🙉 Co	onfig								₽ ⊚	T 🛞 adm
Policy Search	Source add	Iness: 10.1.1.1 ×	_			N		Destination address	Please enter the IP address a	nd click enter to finish	N			
	A	tion: ALLOW ×						Protoco	Please select					
	L Export Expa	nd object details									Query	Reset Ad	vanced query	0
	Policy table	Device 7	7 ^{Seq} ≎ Poli # Poli	icy name S	tatus ⊽ Action			7 Source user	Source address			n Description	Operation	n
	default	核心防火墙 juniper- 172.21.1.91	28 _fb3	23_05_09 231_0	0	test			2 WS-10.1.1.1_32	trust			Delete	Disable
	default	核心防火墙 juniper- 172.21.1.91	16 def	fault- mit	0	test			2 Net-10.1.1.0_255.255.2	dmz			Delete	Disable
	🗌 default	边界墙huawei- 172.21.1.93	37 _c4	23_04_04 4fc_0	0	dmz1	-	-	 W5_10.1.135_32 W5_10.1.137_32 Net_10.1.1.0_24 	dmz	-		Delete	Disable
	default	Analyze- Huawei- 172.21.1.93	37 _c4	23_04_04 4fc_0	0	dmz1	-	-	 W5_10.1.1.35_32 W5_10.1.1.37_32 Net_10.1.1.0_24 	dmz	-		Delete	Disable
	default	pa- 192.168.60.99	б 1to	-z (0	bizt		any	2 net_10.1.1.0_24	biz2			Delete	Disable
	() (_ 202	23_11_08					•					• • •
Ξ										1-20 of	52 items < 1	2 3 > 20/1	page \vee Goto	Page

policy Search Method 1

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

🚫 INET platform	题 Dashboard					⊌ ⊚	T 🛞 adm
Policy Search	Source address: Please enter the IP address and click enter to finish	N	Destination address:	Please enter the IP address and click enter to finish	IN		
	Actions' Please select v		Protocol:	Please select V			
	L Export Expand object details Earth Delete Earth Disable				Query Reset	Advanced query	0 0

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".

Delicy Search			
	Source address: 10.1.1.1 ×	IN V	
	Action: ALLOW × V	-	
		IN	
	<u>t</u> Export Expand object details Batch Delete Batch Disable	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;

•				-			
👩 Policy Search							
	Source address:	10.1.1.1 ×			IN	\vee	C
	Action :	ALLOW ×	٩				
		ALLOW					
	L Export	DENY	tch lusabl	e			
	Policy table De	UNKNOW	- courviname	Status 🛛 Action	n 🛛 Source zo	ne 🛛 Source interfa	ice 🛛

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																
	Source add	dress: 10.1.1.1 ×					IN		Destinat	ion address :	Please enter the IP addr	ess and click enter to finish	IN	l.		
	A	ction: ALLOW ×								Protocol	: Flease select	9				
	L Export Expa	and object details									TCP 6 UDP 17		Query	Reset Ad	vanced query	
	Policy table	Device	⊽ <mark>#</mark> ¢	Policy name	Status 🖓	Action		☑ Source interface	v ⊽ Soure	user	S ICMP 1	Des intaion zone	∇ Destintai	on Description	Operation	
	default	核心防火墙 juniper- 172.21.1.91	28	2023_05_09 _fb231_0	۲	Ø	test	-			ICMPv6 58 HOPOPT 0 IGMP 2	tra t			Delete Dis	sable
	default	核心防火墙 juniper- 172.21.1.91	16	default- permit	۲	0	test	-			GGP 3	dn t	-		Delete Dis	sab
Ery Search			_	_												
uncy search	Source addre	ess: 10.1.1.1 ×					IN		Destination	address:	Please enter the IP address	and click enter to finish	IN			
	Acti	on: ALLOW×								Protocol:	IFCP 6	Q.				
	Source p	ort: Please input !	iource port				-	V	Destinat	ion port:	Please input Destination po	ort	-		~	
	L Export Expans	d object details	Batch Delete	Batch Disable	1								Query	Reset Advan	red avery O	18

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.

🚫 INET platform	뛮 Dashboard 약à Cha	inge 🕀 Analyze	👿 Search 🔹	Config									90	T 🛞 admin
D Policy Search														
	Source address:	10.1.1.1 ×				IN		Destination address	Please enter the IP address	and click enter to finish	1	N		
	Action	ALLOW×						Protoco	I: TCP 6					
	Source port:	Please input Source po						Destination por	ti Please input Destination po					
	Policy table :	Please input Policy tab	le					Policy group	Please select					
	Status	Please select						Policy ID	Please input Policy ID					
	ID	Please input ID						Source zone	Please select					
	Destintaion zone:	Please select						Source interface	Please select					
	Destintaion interface:	Please select						Source use	Please input Source user					
	Application:	Please select						Policy name	Please input Policy name					
	Description	Please input Descriptio												
	L Export Expand of	ject details Batch D										Query	Reset Hide	0
	Policy table D	Device ⊽ Seq #	Policy name	Status ⊽	Action 3	7 Source zone 🚿	7 Source in	terface 🐨 Source user	Source address		♥ Destinta	ion Descript	ion Operati	ion
	default ju 1	杂心防火填 uniper- 28 72.21.1.91	2023_05_09 _fb231_0	٥	Ø	test			2 WS-10.1.1.1_32	trust			Delete	Disable
	≗ ⊡ default ji 1	会心防火増 uniper- 16 72.21.1.91	default- permit	•	Ø	test			2 Net-10.1.1.0_255.255.2	dmz	-		Delete	Disable
									•					*

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.

🚫 INET platform	國 Dashboard 🛛 🗞 Change 🧟 Analyze	e 🔯 Search 🎕 Config				G 💿 T 🛞 adm
Security Policy						
ổ Connectivity	Please input Name Search Q.	frame				Analyze now
Business View	👻 🧰 frame	Report name: - Start time: - Report generation	on time: • Time Consuming: • Report Con	iguration: - History report		
Internet Service Publish	* 🚳 DATA	Overview Optimize Analysis Complian	nce Analysis Hit Analysis			
Access Internet Reques!	👻 🚔 Domain					
Compliance Library	Internet-172.21	Optimization Analysis-Object				
Ordinary Rules	172.21.1.184	Total	Empty Object	Not-ref	Expired Object	Repeat Object
Customize Rules	Manage-Huawei	0	N/A	N/A	N/A	N/A
Zone Rules	Analyze-Huawei					
Analysis lask Report Configuration	👻 🚔 TEST	Optimization Analysis-Policy				
	172.21.1.110-url		Invalid Policy	Expired Policy	Shadow Policy	Conflict Policy
	Cisco-172.21.1.1	Total	N/A	N/A	N/A	N/A
	🚔 Balance	0	Redundancy Policy	Irrelevant Policy	Useless Policy	Mergeable Policy
	👻 🚔 Business		N/A	N/A	N/A	N/A
	172.21.1.161					
	🖴 FortiGat_172.21	Hit Analysis-Unused Objects				
	testcisco	Total Unused Objects	Source Address Objects	Destination Address Objects	Service Objects	Applications
	🔛 panorama192.1	0	0	0	0	0
æ	gw-020000-1	v	v	v	v	v

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.

🚫 INET platform	题 Dashboard	ce 🖾 Search 🎕 Config	~			🖓 💿 T 🛞 admir
Security Policy Connectivity Business View Internet Service Publish Access Internet Request	Please input Name Search Q @ * frame * ODTA * DotTa * DotTa DotTa * DotTa * DotTa * DotTa	frame Report name: - Start time: - Report generations Overview Optimize Analysis Complete	stion time : - Time Consuming : - Report Com iance Analysis - Hit Analysis	figuration: - Historyreport		Analyze now
Compliance Library A Ordinary Rules Customize Rules Zone Rules	 Internet-172.21 172.21.1184 Manage-Huawei 	Optimization Analysis-Object Total	Empty Object	Not-ref	Expired Object	Repeat Object
Analysis Task Report Configuration Convergence	Analyze-HuaveL Analyze-HuaveL TEST If 172.21.1.110-url Clsco-172.21.1.1 Balance	Optimization Analysis-Policy Total	Invalid Policy N/A Redundancy Policy	Expired Policy N/A Irrelevant Policy	Shadow Policy N/A Useless Policy	Conflict Policy N/A Mergeable Policy
	 Business 172.21.1.161 FortiGat_172.21 testcisco panorama192.1. 	Hit Analysis-Unused Objects Total Unused Objects	N/A Source Address Objects	N/A Destination Address Objects	N/A Service Objects	N/A Applications
-	gw-020000-1	0	0	0	0	0

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)

행 Dashboard 🗞 Change 😋 Analyze	🗑 Search 🤹 Config			₽ ⊚	T 🛞 admin
Please input Name Search Q	Analyze-Huawei-172.21.1.93 © Analysis Sociented Report name: 333 Start time: 2024-08-09 11:02:18 Time Consuming: 0h Omin Max Report C	onfiguration: 2222 Hist	ry report	White List Ana	lyze now
* 💩 DATA	Overview Optimize Analysis Compliance Analysis Hit Analysis				
 Domain Internet-172.21 	Batch Action V				Í
172.21.1.184	Object Name	Туре	Reference	Operation	- 1
Manage-Huawei	20	Service Object	0	View White List Dele	to
Analyze-Huawei	13	Service Object	0	View White List Dele	te
* 💼 TEST	9	Service Object	0	View White List Dele	te
172.21.1.110-url	202307140935_5fed	👗 Service Object	0	View White List Dele	te
Cisco-172.21.1.1	. 11	Service Object	0	View White List Dele	te
📫 Balance	. 7	Service Object	0	View White List Dele	te
👻 🧰 Business	. 17	Service Object	0	View White List Dele	te
172.21.1.161	. 19	Service Object	0	View White List Dele	te
E FortiGat_172.21	. 18	Service Object	0	View White List Dele	te
testcisco			1-10 of 17 i	tems < 1 2 > 10/pa	
🛤 panorama192.1					
gw-020000-1	No Reference				

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.

ண Dashboard 🗞 Change 😣 Analyze	🗇 Search 🔹 Config	ß	0 T	() admin
Please input Name Search Q. 4	Analyze-Huawei-172.21.1.93 O Anayos Successful Report name: 133 Start lime: 2024-08-09 1101:38 Report generation time: 2024-08-09 1102:14 Time Consuming: 0h Omin 36s Report Configuration: 2222 History report	White List	Analyz	e now
* \delta DATA	Overview Optimize Analysis Compliance Analysis Hit Analysis			
👻 🚔 Domain				Â
Internet-172.21	Type: Al o v			
172.21.1.184	Empty Object			
Manage-Huawei	Batch Action V			
Analyze-Huawei	Chirdt Name Tupe Reference (Operation		
* 💼 TEST	20 • Service Object 0	View White List	Delete	
172.21.1.110-url	□ 13 ● Service Object 0	View White List	Delete	
Cisco-172.21.1.1	9 Service Object 0	View White List	Delete	
🚔 Balance	202307140935_5fcd & Service Object 0	View White List	Delete	
👻 🧰 Business	11 Service Object 0	View White List	Delete	
172.21.1.161	7 Service Object 0	View White List	Delete	
FortiGat_172.21	17 Service Object 0	View White List	Delete	
testcisco	19 Service Object 0	View White List	Delete	
panorama192.1	The second secon	View White List	Delete	
gw-020000-1		view white the	verete	-

• **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;

國 Dashboard	e 🔞 Search 🎕 Config			P	⊚ T ⊚ admin
Please input Name Search Q.	Analyze-Huawei-172.21.1.93 O Analysis Successful			White List	Analyze now
* 🚔 frame	Report name: 333 Start time: 2024-08-09 11:01:38 Report generation time: 2024-08-09 11:02:14 Time Consuming: 0h Omin 36s Report C	Configuration: 2222 Hist	pry report		
* 💩 DATA	Overview Optimize Analysis Compliance Analysis Hit Analysis				
* 🚔 Domain	18	Service Object	0	View White List	Delete
Internet-172.21			1-10 of 17 it	tems < 1 2 > 1	0/page V
172.21.1.184	No Reference				
Manage-Huawei	Path Action of				
Analyze-Huawei	batti Actori V				
👻 🚔 TEST	Object Name	Туре	Reference	Operation	
172.21.1.110-url	addr1.1.1.15	Address Object	0	View White List	Delete
Cisco-172.21.1.1	add1.1.1.12	Address Object	0	View White List	Delete
Balance	add1.1.1.9	Address Object	0	View White List	Delete
* 🚔 Business	202307140935_d615	Å Address Object	0	View White List	Delete
172.21.1.161	add1.1.1.5	Address Object	0	View White List	Delete
FortiGat_172.21	addr1.1.1.6	Address Object	0	View White List	Delete
testcisco	- 10	A Time Schedule Object	0	View White List	Delete
panorama192.1	2	A Time Schedule	0	View White List	Delete
gw-020000-1		ospect	_		÷

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

窗 Dashboard 🗞 Change 🔒 Analyze	e 👿 Search 🤹 Config			۵	© T ⊗a	Idmin
Please input Name Search Q &	Analyze-Huawei-172.21.1.93 August Sammale Report name: 333 Start line: 2024-04-91 1102138 Report Configuration Overview Optimize Analysis Compliance Analysis Hit Analysis	ion: 2222 History r	eport	White List	Analyze now	•
* 🚔 Domain	□ 18 ● Se	ervice Object	0 Vi	ew White List	Delete 🕌	•
Internet-172.21			1-10 of 17 items	< 1 z > [10/page \vee	
172.21.1.184	No Reference					1
Manage-Huawei	Batch Action V					
Analyze-Huawei	Object Name Type		Reference O	eration		
* 🚔 TEST	addr.1.1.15	ddress Object	0 Vi	ew White List	Delete	
172.21.1.110-url	add1.1.1.12	ddress Object	0 Vi	ew White List	Delete	
CI800-1/221.1.1	add1.1.1.9	ddress Object	0 Vi	ew White List	Delete	
 Business 	202307140995_d615	ddress Object	o vi	ew White List	Delete	
172.21.1.161	add1.1.15	ddress Object	o vi	w White List	Delete	
FortiGat_172.21	addr1.1.1.5	ddress Object	o vi	ew White List	Delete	
testcisco	□ 18 ▲ ^{Tir} ot	me Schedule bject	o vi	ew White List	Delete	
😫 panorama192.1	2 A	me Schedule bject	o v	w White List	Delete	
gw-020000-1			_		*	

• **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;

shboard Rà Change 🔒 Analyze	Search & Config				9 © T 8:
e input fiame Search Q	Analyze-Huawei-172.21.1.93 © Analysis Successful				White List Analyze now
frame	Report name: 333 Start time: 2024-08-09 11:01:38 Report generation	n time: 2024-08-09 11:02:14 Time Consuming: 0h 0min 36s	Report Configur	ition: 2222 History report	
🗞 DATA	Overview Optimize Analysis Compliance Analysis Hit A	nalysis			
* 🚔 Domain	Expired Object				
Minternet-172.21	Batch Action \vee				
172.21.1.184	Object Name	Type	Reference	Schedule	Operation
 Manage-Huawei Analyze-Huawei 	18	Chipect	0	2022-12-01 15:44:18 - 2023- 04-28 15:55:35	View White List Delete
* 🧰 TEST	0,1	Citie Schedule	21	2022-12-01 15:44:18 - 2023- 04-28 15:55:35	View White List Delete
Char 172.21.1.110-url	0.2	Citize Schedule	0	3022-12-01 1544-18 - 2023- 04-28 15:55:35	View White List Delete
Balance	19	Citize Schedule	0	2022-12-01 15:44:18 - 2023- 04-28 15:55:35	View White List Delete
* 🚔 Business	. 4	Cibject	0	2022-12-01 15:44:18 - 2023- 04-28 15:55:35	View White List Delete
 Tr2.21.1.161 FortiGat_172.21 	15	Citie Schedule	o	2022-12-01 1544-18 - 2023- 04-28 155535	View White List Delete
 testoisco panorama 192.1, 		Tima Sebarbila		1-10 of 22 item	• 15 (] 2 3 > 10/page ~

• **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.

뛓 Dashboard 원 Change 🔒 Analyze	🗊 Search 🔹 Config					Ģ	© T	⊗ admin
Prese input Name Search Q. e	Analyze-Huawei-172.21.1.93 Okonyas Secondat Report name: 211 Start Sime: 2024-06-09/1101.38 Report generation Sime: 2024-06-09/1102-1	4 Time Consuming: Oh Omin 36s	Report Configu	ration: 2222 History report	Wh	ite List	Analyze	now
 * Some Domain * Internet-172.21 	Overview Optimize Analysis Compliance Analysis Hit Analysis Repeated Object Batch Action							
172.21.1.184Manage-Huawei	Object Name first	Type	Reference	Repeated Object	Operat View	ion White List	Delete	
 Analyze-Huawei TEST 	21	Service Object Service Object	0	22	View	White List	Delete	
 172.21.1.110-url Cisco-172.21.1.1 Balance 	202305041541_36+8	👗 Service Object	0	202306290946_c6a4; 202306290944_d61; 202305111003_2ab6 202305111015_f1(3	View	White List	Delete	
 ✓ Business ■ 172,21.1.161 	202309181509_eec5	👗 Service Object	0	202309181513_46c0; ssh; 202309181527_5f39; 202403080930_s866	View	White List	Delete	
FortiGat_172.21	29 707307140985 75c3	Service Object Address Object	0	30 202307211419-23x9	View	White List	Delete Delete	
gw-020000-1	I Invalid Policy			1-10 of 36 items	< 1 2	34>	10 / page	2

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.

shboard 🗞 Change 🗎 Analys	re 🕼 Search 🚳	Config				G	© Т	8
input Name Search Q d	Analyze-Hua	awei-172.21.1.93	Analysis Successful		White	List	Analyze	ie no
frame	Report name: 333	Start time: 2024-08-09 11:01:3	8 Report generation time: 2024-08-09 11:02:14 Time Consumi	ng: Oh Omin 36s Report Configuration: 2222 History	report			
🚳 DATA	Overview Opt	imize Analysis Compliant	e Analysis Hit Analysis					
* 🚔 Domain								
Internet-172.21	Invalid Poli	cy.						
172,21,1,184	Batch Action	n ~						
Cl. Manage Hypers	Policy type	e Reason	Description	Policy	Operation			
Analyze-Huawei	Security policy	1, Unknown action 2, Policy not enabled	The policy action is "unknown"The policy status is" disable"	Policy Table: default Seq #: 193: Name: 5	View White List	Delete	Clean	Î
• 💼 TEST	Security policy	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seq #1 191: Name: 656	View White List	Delete	Clean	l
Cisco-172.21.1.1.	Security policy	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seg #: 190: Name: 666	View White List	Delete	Clean	l
Balance	Security policy	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seg #1: 188; Name: 221	View White List	Delete	Clean	l
 Business 172.21.1.161 	Security policy	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seq #: 182: Name: merge_policy_c1e7d5db	View White List	Delete	Clean	ĺ
Fort/Gat_172.21	Security policy	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seq #: 181: Name: zz11	View White List	Delete	Clean	
testcisco	Canorito							
🛤 panorama192.1					1-10 of 17 items	2 >	10 / page	
aw-020000.1								

 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;

put Name Search Q e	Analyz	e-Huawa	ai-172 21 1 93 👩	Australia Georgeonde d			White I	ist	Analyze
	Analyz	enuawe	EI-172.21.1.95 0	Anayus successful					
frame	Report nan	me: 333 Sta	rt time: 2024-06-09 11:01:3	 Beport generation time: 2024-08-09 11:02:14 Time Consumit 	19: Oh Omin 36s Report Configuration: 2222 History	eport			
So DATA	Overview	Optimiz	e Analysis Compliano	e Analysis Hit Analysis					
🚔 Domain	-		-						
Minternet-172.21	Inva	lid Policy	1						
_	Bato	ch Action 🗸							
1/2.21.1.184		Policy type.	Reason	Description	Policy	Opera	tion		
Manage-Huawei		Constant of Constant	* Helenen enter						
Analyze-Huawei	•	policy	2, Policy not enabled	The policy action is "unknown"The policy status is" disable"	Policy Table: default: Seq #1: 193; Name: 5	View	White List	Delete	Clean
TEST	0	Security	1. Unknown action	The policy action is "unknown"	Policy Table: default: Seq #: 191; Name: 656	View	White List	Delete	Clean
172.21.1.110-url		poincy							-
Cisco-172.21.1.1	•	policy	1, Unknown action	The policy action is 'unknown'	Policy Table: default: Seq #: 190: Name: 666	View	White List	Delete	Clean
🚔 Balance	o	Security	1, Unknown action	The policy action is "unknown"	Policy Table: default: Seq #: 180: Name: zz1	View	White List	Delete	Clean
💼 Business		Cequibu			Dellas Table (defends Can &) (87) Manual				- 1
172.21.1.161		policy	1. Unknown action	The policy action is "unknown"	merge_policy_c1e7d5db	View	White List	Delete	Clean
	192	Security	1. Unknown action	The policy action is "unknown"	Policy Table: default: Seq #: 181: Name: 2211	View	White List	Delete	Clean
FortiGat_172.21		poncy							

• **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;

Dashboard Pa Change Analyz	ze 🔞 Search 🎕 Config			ə (∋ T ⊛adm
Please input Name Search Q 🖉	Analyze-Huawei-172.21.1.93 @Analysis Successful Report name: 333 Start time: 2024-08-09 11:01:38 Report generation time: 202	4-09-09 11:02:14 Time Consumi	ng: Oh Omin 36s Report Configuration: 2222 Hist	White List	Analyze now
* 🗞 DATA	Overview Optimize Analysis Compliance Analysis Hit Analysis				
 Domain Internet-172.21 172.21.1.184 	Expired Policy Batch Action				
Manage-Huawei	Policy type Reason	Description	Policy	Operation	
Analyze-Huawei	Security 1. The policy has an expired schedule object policy	Expired objects: [111]	PolicyTable: default: Seq #: 154: Name: 365	View White List Delete	Clean
👻 🚔 TEST	Security 1. The policy has an expired schedule object	Expired objects: [1]	PolicyTable: default: Seg #: 88: Name: 168	View White List Delete	Clean
Cisco-172.21.1.10-un	Security 1. The policy has an expired schedule object	Expired objects: [1]	PolicyTable: default: Seg #: 87: Name: 171	View White List Delete	Clean
Balance	Security 1. The policy has an expired schedule object	Expired objects: [1]	PolicyTable: default: Seq #: 86: Name: 170	View White List Delete	Clean
 Business 172.21.1.161 	Security 1. The policy has an expired schedule object	Expired objects: [1]	Policy Table: default: Seg #: 85: Name: 169	View White List Delete	Clean
FortiGat_172.21	Security 1. The policy has an expired schedule object	Expired objects: [1]	PolicyTable: default: Seq #: 84: Name: 167	View White List Delete	Clean
testcisco	Canolity				-
🛤 panorama192.1				1-10 of 23 items < 1 2 3 > 10	7/ page ∨
gw-020000-1	Hidden Policy				

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

똃 Dashboard 약à Change 😔 Analyz	回 🗇 Search 纔 Config		Ģ ⊚ T ⊗ admin
Plesse input Name Search Q a	Analyze-Huawei-172.21.1.93 © Analysis Secondal Report name: 333 East time: 2024-08-09 11:01:38 Report generation time: 2024-08-0 Overview Optimize Analysis Compliance Analysis Hit Analysis	9 110214 Time Consuming: 6h Omin 16s Report Configuration: 2222	White List Analyze now History report
 Domain Internet-172.21 172.21.1.184 	I Hidden Policy Batch Action V		
Manage-Huawei	Policy type Shadow Policy	Hidden Policy	Operation
Analyze-Huawei	Security policy Policy Table: default: Seq #: 117; Name: zzz3	Policy Table : default: Seq #: 118: Name : zzz4	White List Delete Disable Clean
 ✓ ■ TEST ■ 172.21.1.110-url 	Security Policy Table: default: Seg #: 115: Name: zzz1 policy	Policy Table: default: Seq #: 116: Name: zzz2	White List Delete Disable Clean
Clsco-172.21.1.1	Security policy Table: default: Seq #: 113: Name: 322	PolicyTable: default: Seq #1 114: Name: 323	White List Delete Disable Clean
Balance	Security policy Table: default: Seq #: 111: Name: 320	PolicyTable: default: Seq #: 112:Name: 321	White List Delete Disable Clean
172.21.1.161	Security Policy Table: default: Seq #: 109: Name: 318	Policy Table: default: Seq #: 110: Name: 319	White List Delete Disable Clean
FortiGat_172.21	Security policy Policy Table: default: Seq #: 107: Name: 316	PolicyTable: default: Seq #: 108: Name: 317	White List Delete Disable Clean
testcisco	Sanurity		
panorama192.1		1-10 of 87	'items < 1 2 3 4 5 ··· 9 > 10/page ∨
gw-020000-1	Redundant Policy		

• **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;

		er-172.21.1.95 () Analysis baccesetta				White	List	Analyze
ame	Report name: 333 St	art time: 2024-08-09 11:01:38 Report generation time: 2024-08-09	1:02:14 Time Consuming: Oh Omin 36s Report Configuration: 2222	History re	port			
DATA	Overview Optimi	ze Analysis Compliance Analysis Hit Analysis						
Domain	-							
Internet-172.21	Redundant Po	licy						
172.21.1.184	Batch Action							
Manage-Huawei	Policy type	Redundant Policy	Big Policy	Operat	ion			
Analyze-Huawei	Security policy	Policy Table: default: Seg #: 40: Name: 4	Policy Table: default: Seq #: 41: Name: os	View	White List	Delete	Disable	Clean
 TEST 172.21.1.110-url 	Security policy	Policy Table: default: Seq #1 39: Name: 3	Policy Table : default: Seq #1: 41: Name : os	View	White List	Delete	Disable	Clean
Cisco-172.21.1.1	Security policy	Policy Table: default: Seg #: 38: Name: 2	PolicyTable: default Seq #: 41; Name: os	View	White List	Delete	Disable	Clean
Balance	Security	Policy Table: default; Seg #1 35: Name: 2023_04_03_50386_0	Policy Table: default: Seq #: 37; Name: 2023_04_04_c44fc_0	View	White List	Delete	Disable	Clean
172.21.1.161	Security	Policy Table: default: Seg #1 33: Name: 2023_03_24_55fdb_0	Policy Table: default: Seq #: 34: Name: 2023_03_24_705e7_0	View	White List	Delete	Disable	Clean
FortiGat_172.21	Security	Policy Table: default: Can #+ 38: Name: 3038.06.18.bd760.1	Policy Table: default: Seg #: 194 Name: 2024 05 18 bd760 0	View	White List	Delete	Disable	Clean

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.

shboard 🗞 Change 🗟 Analyzi	e 🗊 Search 🎕 Config		9 Q	т
e reput Name Search Q. 4	Analyze-Huawei-172.21.1	.93 🔘 Amalysis Successful	White List	nalyze n
frame	Report name: 333 Start time: 2024-0	-09 11:01:38 Report generation time: 2024-08-09 11:02:14 Time Consuming: 0	h Dmin 36s Report Configuration: 2222 History report	
S DATA	Overview Optimize Analysis	Compliance Analysis Hit Analysis		
* 🚔 Domain				rep:
Internet-172.21	Mergeable Policy			
172 21 1 194	Datch Action	1		
172211104	Batch Action +			
Manage-Huawet	Policy type	Mergeable Policy	Operation	
Analyze-Huawei	Security policy	Policy Table: default: Seg #: 179: Name: 394	View White List Merge	- î
* 🧰 TEST		Policy Table: default; Seq #1 180: Name: 395		- 1
	Security policy	Policy Table : default: Seq #1 177: Name : 392	View White List Merge	- 1
172.21.1.110-un		Policy lable: default; seq #1 1/d: Name: 393		- 1
Cisco-172.21.1.1	Security policy	Policy Table: default: Seg #: 175: Name: 390	View White List Merge	- 1
Balance		Policy lable: default Seg #1 176; Name: 391		_
	Security policy	Policy Table: default: Seq #1 173: Name: 388	View White List Merce	- 1
* 💼 Business		Policy Table: default: Seq #1 174; Name: 389		
172 21 1 161		Policy Table: default: Seg #: 171: Name: 386		
The lines	Security policy	Policy Table: default: Seq #: 172: Name: 387	Wew White List Merge	
E FortiGat_172.21		Prinz Table: default San #: 189 Name: 184		
testcisco	Security policy	Policy Table: default: Seg #: 170: Name: 385	View White List Merge	
		Deline Table - default: Can #1 157- Name: 202		
E panorama192.1				

• 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;

	Analyze-Huawei-	172.21.1.93 (0 Instant Secondal			White List An
frame	Report name: 333 Start S	me: 2024-08-09 11/01/38 Report prevation time: 2	024-08-09 11:02:14 Time Comunity: Oh Dmin 36s A	port Configuration: 2222 History report	
& DATA	Outputer Ontimine A	andreis Compliance Analysis Hit Analysis			
• 💼 Domain	Cibiles Optimizer	and the compact maps		1-10-07 /3-08mt (1) 2 5 4	3 ··· 8 2 10/p
M Internet-172.21	Conflict Policy				
172.21.1.184	Batch Action ~				
Manage-Huawei	Policy type	Normal Policy	Conflict Policy	Suggestions	Operation
Analyze-Huawe			Policy Table: default: Seq #1 54: Name: 220		
• 🚔 TEST			Policy Table: default: Seq #1 56: Name: 221 Policy Table: datach San #1 50: Name: 777	Durk to say if confiction resiries must	
172 21 1 110 uni	Security policy	Policy Table: default Seq #: 16 Name: dm21	PolicyTable: default:Seq #1 60: Name: 223	business and security requirements	Were White Li
-			Policy Table: default: Seq #1 65: Name: 226		
Cisco-17221.1.1			_ toperd		
a Balance			Policy Table: default: Seq #1 54: Name: 220 Relies Table: default: Seq #1 54: Name: 220		
	12 2 2 2 21		Policy Table: default: Seg #1 58 Name: 222	Check to see if conflicting policies meet	
 Evenese 	Security policy	Poky able: default seg #1 15 Name: 1	Policy Table: default: Seq #: 60: Name: 223	business and security requirements	West White La
172.21.1.961			Policy Table1: default: Seq #1: 65: Name1: 226		
FortiGat_172.21					
	Security reliev	PolicyTable: default Seq #1 14 Name:	Policy Table: default: Seg #: 15 Name: 1 Index Table: default: Sec #: 16 Name: dec1	Check to see if conflicting policies meet	View White Lie

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.

몇 Dashboard 원 Change 음 Analyz	e 🖾 Search 🦚 Config				Ģ	⊚ T ⊗ admir
Plane ropat Name Search Q 4	Analyze-Huawei-172.21 Report name: 333 Start time: 2024-	1.93 Anelysing 08-09 13:01:39 Report generation time	: 2024-08-09 13:02:17 Time Consuming: 0h 0m	in 38s Report Configuration: 2222	White List	Analyze now
* 🗞 DATA * 🚔 Domain	Overview Optimize Analysis	Compliance Analysis Hit Analysi	8			
Internet-172.21	RiskLevel: All 0	v				
172.21.1.184	Risk Level	Type	V Name	Hit Policy	Description	
Manage-Huawei	• High	Inter-zone rule	trust to untrust	20		1
Analyze-Huawei	• High	Inter-zone rule	untrust to trust	21		- 11
* 🚔 TEST						

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.

	192.168.60.99	 Analysis Successful 			L	L Export report White List Analyze n
🖬 mtk_config	Report name: manual	admin_202408051515 Start time: 2024-08-05 15:14:	32 Report generation time: 2	024-08-05 15:14:39 T	ime Consuming: Oh Omin 7s Rep	ort Configuration: MTK报告配置 History report
📕 fgt_192.168.60.98	Overview Optima	ze Analysis Compliance Analysis Hit Analy	-			
172.21.1.93	L Hannah Ballai					
2222	Condition of the second	<u> </u>				
192.168.60.99	Batch Action	 Insufficient Data(0) 				
172.21.1.164	Policy type	Policy	Description	User	Source address	De: Operation
1 72.21.1.113						i i
auto_test_51434397	Security policy	Policy Table: default: Seq #1: 29: Name: awen_test21		any	& w5-20.20.20.66_32	2 White List Delete Disable Clean
auto_test_28286783						
8 则试用操优化所有设备						
🚔 方戰對法	Security policy	Policy Table: default: Seg #1 28: Name: 2024_06_11_3f860		any	& WS-10.1.1.89_32	& White List Delete Disable Clean
172.21.1.122						8
🖴 "ध्यस्त्रहण्य	Security policy	Policy Table: default: Seg #1 27; Name: 2024,06,11,28ab8		any .	& WS-10.1.1.89_32	2 White List Delete Disable Clean
DP ###						
🚔 助火壊	Security	Policy table: default; Seq #1 26: Name1			0 w/ 1511 85 37	O White Lies Roberts Parable Class.
E 1						1-10 of 27 items (1 2 3 > 10 / name V

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.

Security Policy									
Connectivity	New Batch deletion Status d	hange				Please input Rule name		9,0	0
😴 Connectivity Batch	Rule name	Status	Risk level	∇ Rule type	7 Remarks	Opr	aration		
Business View ^	+ C Port 50030	Enable	High	Predefined	MapReduceJobTracker default port	Cog	y Disable		
Internet Service Publish	+ 🗇 Port 50070	Enable	High	Predefined	HDFSNameNode default port	Copy	Disable		
Access Internet Request	+ Port 27018	Enable	High	Predefined	Mongodb unauthorized access port	Copy	/ Disable		-1
Confinance Library ~	+ Port 27017	Enable	High	Predefined	Default port for MongoD8 server	Copr	y Disable		-1
Customize Rules	+ D Port 11211	Enable	High	Predefined	Default port for memcached service under windows	Copy	Disable		-1
Zone Rules	+ 🗌 Port 9092	Enable	High	Predefined	Default port number for kafka learning	Cop	J Disable		- 1
Analysis Task	+ 🗌 Port 9090	Enable	High	Predefined	TCP port, this port is not the system default port, it is a custom port.	Copy	Disable		- 1
語 Report Configuration	+ Port 9080-9081	Enable	High	Predefined	Webshpere application, default port number	Cope	/ Disable		- 1
Convergence	+ Port 8080-8089	Enable	High	Predefined	Used for WWW proxy services, enables web browsing.	Copy	Disable		-1
	+ C Port 8069	Enable	High	Predefined	Default port for Odoo(OpenERP) Server	Copy) Disebie		-1
	+ 🗌 Port 8443	Enable	High	Predefined	Default port for tomcat opening SSI, text service	Copy	Disable		-1
	+ Dort 8000	Enable	High	Predefined	Server port	Copy	/ Disable		- 1
	+ Port 7778	Enable	High	Predefined	Kloso host control panel login.	Copy	/ Disable		- 1
	+ Dort 7002	Enable	High	Predefined	User and group database port	Copy	Disable		
	+ C Port 7001	Enable	High	Predefined	Freak38, Weblogic default port	Copy	Disable		-1
	+ Dort 6379	Enable	High	Predefined	Redis default port number	Copy	y Disable		- 1
	+ Port 5984	Enable	High	Predefined	CouchDB default open Restful API interface for database management functions	Copy	/ Disable		
	+ Port 5902	Enable	High	Predefined	VNC port for virtual network computers	Copy) Disable		
						1 Martillana (11 2 2 4 2 1		Calle	-

6.2.1. Customize regular rules

In Analyze \rightarrow Compliance Library \rightarrow 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.

0	Security Policy										
s,	Connectivity	New					New rule N	lew high risk part		×	
s?	Connectivity Batch		Rule name		Status	Risk level	8 1	• •			
ō	Business View	+	Port 50030		Enable	High	* Name :	Please input Name			
	Internet Service Publish	+	Port 50070		Enable	High	* Risk level:	High \lor			
	Access Internet Request	+	Port 27018		Enable	High	Action:	ALLOW			
8	Compliance Library	-	Dort 27017		Enable	High	Source address:	Please input Source address	in v		
	Ordinary Rules		Ded 11011		Cashla		Der Freihender	Proceeding a Province from a data and			
	Customize Rules	+	POIL 11211		Enable	High	Destination addre	Please input Destination address	in v		
	Zone Rules	+	Port 9092		Enable	High	Portocol:	TCP V	in \vee		
	Analysis Task	+	Port 9090		Enable	High	Destination port :	Please input Destination port	in \vee		
ŝŝ	Report Configuration	+	Port 9080-908	1	Enable	High	Source port:	Please input Source port	in \vee		
ľ	Convergence	+	Port 8080-808	9	Enable	High	Permarker '				
			Port 8069		Enable	High	Kennarkan				
		+	Port 8443		Enable	High				_	
		+	Port 8000		Enable	High	h	Cancel		ОК	
		+	Port 7778		Enable	High	Predefined	Kloxo host control panel login			
		+	Port 7002		Enable	High	Predefined	User and group database port			

6.2.2. Custom Rules

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

0	Security Policy	5	Customize rules / New				
4	Connectivity						
√?	Connectivity Batch		Basic Information				
<u>:0</u>	Business View ^		* Name		* Risk Level		
	Internet Service Publish		Please enter		High	\vee	
	Access Internet Reques		Description				
B	Compliance Library		Please input Description				
	Ordinary Rules						
	Customize Rules					11	
	Zone Rules		Filter information				
2	Analysis Task		Filter Conditions				
	Report Configuration		0			Test	
_n ť	Convergence		action				
			app.isAny				
			app.name				
			description				
			dst.ip				
			dst.isAny				
			dst.name				
			dst.negated				
			dstinterface				
			dstZone				
			anshlari		-		

6. 2. 3. Zone rules

In the Analyze \rightarrow Compliance Library \rightarrow 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.

 Security Policy Connectivity 	Rule Security Zone								
ổ Connectivity Batch	Please input Name Search Q	G Securit							
Business View ^		New Export Impo	Please input CIDR Q						
Access Internet Request	100 trust	 Security Zone 	∀ Туре	CIDR	Description	Operation			
Compliance Library ^	1 untrust	trust	IPv4	10.1.1.0/24		Edit Delet			
Ordinary Rules Customize Rules						1-1 of 1 literus (1)> [
Zone Rules									
Analysis Task									
2 Report Configuration									
Convergence									
	1								
	+ Add Security 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.

3 Zone Rules / Add rules	
	Inter-zone rule information (2) Security zone rule matrix
	Basic Information
	* Name
	Please enter
	Description
	Please input Description
	security zone
	Security zone selection
	□ ∨ 3 items Available security zones □ ∨ 0 item Available security zones
	✓ Root
	No Data
	Inter-zone rule matrix configuration
	Allow all intra-zone traffic
	Cancel Generate matrix

፼ Dashboard 校 Change	🕼 Search 🎕 Config				
	Security zone rule matr	⊘ Inter-zone rule infor	rmation 🧕 Security zone rule r	natrix	
	To	untrust (5)	trust (80)		
	untrust (5)	\checkmark	×		
	trust (80)	x	\checkmark		
		Cance	Prev Step Save		

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

N INET platform	🔯 Dashboard 🗞 Change 😝 Analyze 🔯 Search 🎕 Config	🐺 💿 T 🛞 adm
Security Policy	图 Zone Rules / 輸銷規則	
Connectivity		
Business View 🔺	Inter-zone rule information	ation 🛛 2 Security zone rule matrix
Internet Service Publish	L Cocurity zone rule matrix	
Access Internet Request	Security zone rule matrix	
海通-外访内	То	
🗒 Compliance Library 🔺	From From	trust (80)
Ordinary Rules	Security zone rule matrix: From untrust	To untrust ×
Customize Rules	untrust /5	
Zone Rules	• Type	
Analysis Task	Allow	v
E Report Configuration	trust (80) * Risk Level	
Convergence	Low	 V
	Exclusion Rule	
	Press enter after entering to add rules	
	Description	
	Please input Description	
		Cancel
æ	Cancel	Prev Step Save

6.3. Analysis Task

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

\odot	Security Policy													
⊲°	Connectivity	Scheduled Task	Task Qu	ieue										
0	Business View 👻	New											C	â
Ę	Compliance Library													
	Ordinary Rules	Name	De	wice/Group	Status	Creator	Report Configuration	CRON	Creation Time	÷	Update Time	\$ Description	Operation	
	Customize Rules	333	1414	务域	Enable	admin	2222	0 0/59 * * * ? *	2024-03-11 10:17:34		2024-03-11 10:17:34		Disabled Edit De	lete 🤶
	Zone Rules	•												•
	Analysis Task											1-1 of 1 item	s < 1 > 20	page \vee
÷:	Report Configuration													
×	Convergence													
-														

- **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.

Scheduled Task	Task Queue					
New						
Name	Device/Group	Status	Creator Report Configuration CRON	Creation Time	Update Time	Description
			New	×		
_			Name: Please enter * Device/Group: 请选师			
			Status:			
			* Report Configur Policy And Object Optimization analysis	New		
			* CRON expressio Please enter	rification		
			Description: Please input Description			
				~		
				Cancel		

Task Queue:

Records of All Executed Analysis Tasks

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

 Security Policy Connectivity 	Scheduled Task Task Queue							
Business View	Queue Setting						0 0	0
Access Internet Reques	Task Name	Device/Group	Initiator	Progress	IF Start time	End time	Cperation	
	333	Domain	admin	 Analysis successful 	2024-12-27 13:03:08	2024-12-27 13:03:09	Cancel	- îÎ
Compliance Library 🔺	333	Manage-Huawei-Firewall-172.21.1.84	admin	🗸 Analysis successful	2024-12-27 13:02:28	2024-12-27 13:03:06	Cancel	
Ordinary Rules	333	Analyze-Huawei-172.21.1.93	admin	 Analysis successful 	2024-12-27 13:01:46	2024-12-27 13:02:27	Carroll	
Customize Rules	333	Internet-172.21.1.80	admin	 Analysis successful 	2024-12-27 13:01:08	2024-12-27 13:01:45		1
Zone Rules	333	Domain	admin	 Analysis successful 	2024-12-27 13:01:06	2024-12-27 13:01:07	Cancel	
Analysis Task	333	Manage-Huawei-Firewall-172.21.1.84	admin	 Analysis successful 	2024-12-27 13:00:26	2024-12-27 13:01:04	Cancel	1
Convergence	333	Analyze-Huawei-172.21.1.93	admin	✓ Analysis successful	2024-12-27 12:59:36	2024-12-27 13:00:24	Cancel	1
	333	Internet-172.21.1.80	admin	 Analysis successful 	2024-12-27 12:59:02	2024-12-27 12:59:34	Cartosi	
	333	Domain	admin	 Analysis successful 	2024-12-27 12:03:06	2024-12-27 12:03:07		
	333	Manage-Huawei-Firewall-172.21.1.84	admin	 Analysis successful 	2024-12-27 12:02:26	2024-12-27 12:03:04	Cancel	
	333	Analyze-Huawei-172.21.1.93	admin	 Analysis successful 	2024-12-27 12:01:44	2024-12-27 12:02:23	Cancel	
	333	Internet-172.21.1.80	admin	✓ Analysis successful	2024-12-27 12:01:04	2024-12-27 12:01:43	Carical	
	333	Domain	arlmin	X Anaborie euroareful	2024.12.22 12:01:02	2024-12-22 12-01-02		

1-20 of 66957 items < 1 2 3 4 5 ··· 3348 > 20 / page </ Go to

6.4. Report Configuration

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

Security Policy			
Connectivity	New		0
Business View	Name	Description	Operation
Access Internet Request	t城间		Edit Delete
Access memor neques	122121	· · · · · · · · · · · · · · · · · · ·	Edit Delete
Compliance Library ^	url	-	Edit Delete
Ordinary Rules	test-all		Edit Delete
Customize Rules	1111		Edit Delete
Zone Rules	1122121		Edit Delete
Analysis Task	2222		Edit Delete
E Report Configuration	testone		Edit Delete
(a) Convergence	test111		Edit Delete
	1.23		Edit Delete
	test	· · · · · · · · · · · · · · · · · · ·	Edit Delete
			1-11 of 11 items < 1 > 20 / page ∨

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

\odot	Security Policy	≅ Report Configuration / New				
\$	Connectivity					
0	Business View		Basic Information			
	Internet Service Publish		• Name			
	Access Internet Reques:					
			Description			
B	Compliance Library					
	Ordinary Rules					
	Customize Rules		Task configuration-Optin	mization analysis		
	Zone Rules		Name	Setting Item		
9	Analysis Task		Empty Object			
-	Report Configuration		No-ref Object			
, K	Convergence		Repeat Object			
			Expired Object	0	Hour	0
			Expired Policy	0	Hour V	0
			Invalid Policy			
			Shadow Policy			
			Conflict Policy			
			Redundancy Policy			
			Atazanakia Balini			
-=						

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.

🚫 INET platform	🖾 Dashboard የგ Change 🤤 Analyze	圆 Search			🕼 💿 T 🛞 admin
Security Policy	New Export Delete				Please enter the task na Q. C I 🕸
Business View 🔺	Task name Creator	Device Started At	♦ End At ♦ Status	Result Description	operation
Internet Service Publish Access Internet Reques	. 1111111 admin	Analyze-Huawei- 172.21.1.93 2024-03-18 15:27:46	2024-03-19 15:27:46 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
	111111 admin	Analyze-Huawei- 2024-03-11 14:06:59 172.21.1.93	2024-03-12 14:06:59 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
Compliance Library ^ Ordinary Rules	ceshiz admin	Analyze-Huawei- 2024-03-11 11:20:36 172.21.1.93	2024-03-18 11:35:36 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
Customize Rules	111 admin	Analyze-Huawei- 2024-03-11 10:01:50 172.21.1.93	2024-03-12 10:01:50 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
Analysis Task	ddd admin	Analyze-Huawei- 2023-12-04 16:02:47 172.21.1.93	2023-12-05 16:02:47 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
委 Report Configuration	test111 admin	边界墙huawei- 2023-09-27 17:07:07 172-21.1.93	2023-09-28 17:07:07 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
	安全策略收敛01 admin	Analyze-Huawei- 2023-09-20 15:26:52 172.21.1.93	2023-09-27 15:26:52 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
	ERWR admin	Analyze-Huawei- 2023-09-20 11:47:08 172.21.1.93	2023-09-21 11:47:08 FINISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
	01 admin	Cisco-172.21.1.160 2023-09-15 17:25:18	2023-09-16 17:25:18 FINISHED	Result -	Copy View Stop Policy log Analyze immediately Delete
	test10 admin	Cisco-172.21.1.160 2023-08-24 15:23:47	2023-08-25 15:23:47 RNISHED	Result -	Copy View Stop Policylog Analyze immediately Delete
	test11 admin	Cisco-172.21.1.160 2023-07-31 15:56:54	2023-08-01 15:56:54 FINISHED	Result -	Copy View Stop Policy log Analyze immediately Delete
					1-20 of 30 items < 1 2 > 20 / page >
≅					
Recent tasks 99+ Configure view					8

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.

Ø							
Ś	Connectivity	New task	The device does r	not receive syslog. Do you want to receive syslog	×	×	the task na
6	Business View 🔺						
	Internet Service Publish	1 Select	Source Interface :	Please select V		×	avion av
	Access Internet Reques	device	Source Address:	Please select V			cy toy ~
	海通-外访内		Proxy Address:	oxy Address: Please input 代理地址	0		cy log Arr
8	Compliance Library		Transfer protocol :				auton tur
	Ordinary Rules						cy log A
	Customize Rules	2 Select	* Reception Port:	514			cy log Ar
	Zone Rules	poncy			_		
	Analysis Task			Cancel	ОК		cy log Ar
16							extent Arr
		C. Trut					
		parameters					cy log Ar
							cylog Ar
							cy log Ar
							cy log Ar
						Next	cy log Ar

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.

0	Security Policy																
8	Connectivity	New	task													×	Perteckina. Q C I 🖲
	Business View																
	Internet Service Publish	0	Select	Per	Permissiveness measures how widely a rule is defined. You can choose the policy which has a high permissiveness for optimization. The more											cyllog Analice Immediately Delete	
	Access Internet Reques 海通-外访内		device	based on prefixs configured by user.									•				
				Expand object details Policy query				C) I ©	3 ×	cy log (Analyze immediately) Delete						
8	Compliance Library				Permissive	e 0	Policy table	Policy gro T	Policy name	Status T	Action	▼ Source zo ▼	Source in	Source address		cy log	wine these commentances Delates
	Ordinary Rules				HIGH .	58	default	default	2024041711	۲	8	any	14	🛊 any			The second second second second
	Customize Rules	0	policy		HIGH	58	default	default	2024041711.	\odot	(2)	any		202404171	111 cb38	1	cylog Analyze mendicately Delete
	Zone Rules									-	-			-			
0	Analysis Task				HIGH	58	default	default	2023_09_18.,	Θ	\odot	any		Q 202309181	528_b90f	. 1	grog wards manager beets
111	Report Configuration				LOW		default	default	2024_03_08.,	۲	8	any	8	2 202403080	930_dba8		cylog Analyza investigately. Delete
	Convergence	3	Task		HIGH	2	default	default	2023_09_18	•	8	any		2 202309181	1527_aee7		cylog Analyze mmediately. Delete
			heratoranta		MED	5	default	default	2023_09_18	•	0	any		202309181	1509_bac8		
					HIGH	58	default	default	2023_08_10	•	8	any		202308101	518_4485	cy lo	cy log - Analytis immediately - Delete
				1						~	-			•		. *	cylog Analyze immediately Delete
		i i										1-20 of 194 items	1 2 3	4 5 10	> 20/pac	e VI	cylog Analyza incrediately Delete
				Po	licies can n	ot be se	electable where th	e status is disable o	r action is deny/d	isabl LOW 1	-30 MED 31-40	HIGH 41-100			Previous	Next	cy log Analyze annediatory Delete
																1-20 0	of 30 items 🗧 1 2 🗦 20 / page 🖂

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.

Ð	Security Policy								
z	Connectivity		New	task			×	The task na Q C I i	\$
Q	Business View								
	Internet Service Publish			Select	* Task name :	Please input Task name			î
	Access Internet Reques			device	Prefer prefixs for your policy: Analysis period (Please enter the subnet and click enter to finish	0		
	海通-外访内			Select policy		e) day		oy log Analyze immediately Delete	
5	Compliance Library) week			
	Ordinary Rules					month			
	Customize Rules	C.	\odot		Description			cy log Analyze immediately Delete	
	Zone Rules				Description :				
3	Analysis Task							cy log Analyze immediately Delete	
191	Report Configuration							cy log. Analyze immediately Delete	
3	Convergence			Task parameters					8
								cy log Analyze immediately Delete	
								cy log Analyze immediately Delete	
								cy log Analyze immediately Delete	
		C.						cy log Analyze immediately Delete	
		L				Previou	a Finish	cy log Analyze immediately Delete	•
							1-20 of 3	30 items < 1 2 > 20 / page 3	