Ruijie RG-WALL 1600-Z-S Cloud-Managed Firewall

NAT Typical Configuration Examples

Document Version: V1.2
Date: 2024-08-22

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services, or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document will be updated from time to time due to product version upgrades or other reasons. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- The official website of Ruijie Reyee: https://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

Interface Symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Choose **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

This document describes the features and use methods of the product and provides a guide for users to configure and use it in the trial stage.

Contents

1 Overview

Network Address Translation (NAT) is typically used on edge devices that connect two networks. By translating an IP address in a packet header into another IP address, NAT enables mutual access between different types of networks, such as IPv4 and IPv6 networks as well as intranets and extranets.

The following table lists the translation principles and scenarios of different types of NAT.

NAT Type	Principles	Application Scenario
Destination NAT	Translate the destination address (public IPv4 address) in a packet into a private IPv4 address.	Public network users can use public network addresses to access intranet servers.
Twice NAT	Translate the source address (private IPv4 address) and destination address (public IPv4 address) in a packet to other IPv4 addresses separately.	Intranet users can use public network addresses to access intranet servers.
Static NAT-PT	Configure one-to-one static mappings between IPv6 and IPv4 addresses to translate IPv4 and IPv6 addresses.	Fixed mutual access is required between an IPv4 network and an IPv6 network. For example, a host on an IPv4 network needs to access a fixed web server on an IPv6 network.
Dynamic NAT-PT	Configure dynamic mappings between IPv6 and IPv4 addresses to translate IPv4 and IPv6 addresses.	No fixed mutual access is required between an IPv4 network and an IPv6 network. For example, a host on an IPv6 network needs to access multiple servers on an IPv4 network.
Stateless NAT64	Configure NAT64 prefix information to translate source and destination IPv4 or IPv6 addresses using the address translation algorithms defined in RFCs.	Multipoint-to-multipoint mutual access is required between an IPv4 network and an IPv6 network.
Static NAT64	Configure static mappings between IPv6 and IPv4 addresses to translate source and destination addresses in IPv6 packets to IPv4 addresses.	Multipoint-to-point mutual access is required between IPv4 and IPv6 networks.
Dynamic NAT64	Configure dynamic mappings between IPv6 and IPv4 addresses to translate source and destination addresses in IPv6 packets to IPv4 addresses.	Dynamic NAT64 only applies to scenarios where an IPv6 host initiates a request to access an IPv4 network (for example, an IPv6 user needs to access an IPv4 server).
NAT66-source NPTv6	Translate the source IPv6 address prefix in an IPv6 packet into another IPv6 address prefix.	Intranet users proactively access an extranet.

NAT Type	Principles	Application Scenario
NAT66-destination NPTv6	Translate the destination IPv6 address prefix in an IPv6 packet into another IPv6 address prefix.	Servers on an intranet provide services (for example, web services and FTP services) to an extranet.

2 Configuration Example of Enabling Extranet Users to Access Intranet Servers

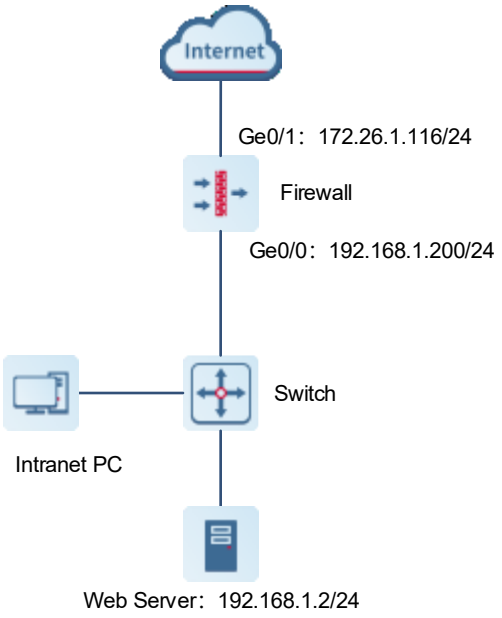
2.1 Applicable Products and Versions

Table 2-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R1P2 or later

2.2 Service Demands

A company has deployed a firewall at the network border as a security gateway. To allow external access to an intranet web server, destination NAT needs to be configured on the firewall. This will map the IP address 192.168.1.2 of the intranet web server to a public IP address 172.26.1.116 assigned to the extranet interface. This configuration allows extranet users to access the web server.



2.3 Prerequisites

Routing and related configurations have been completed in the early stage of network planning.

2.4 Procedure

2.4.1 Completing Basic Network Access Settings

Choose **Network** > **Interface** > **Physical Interface**.

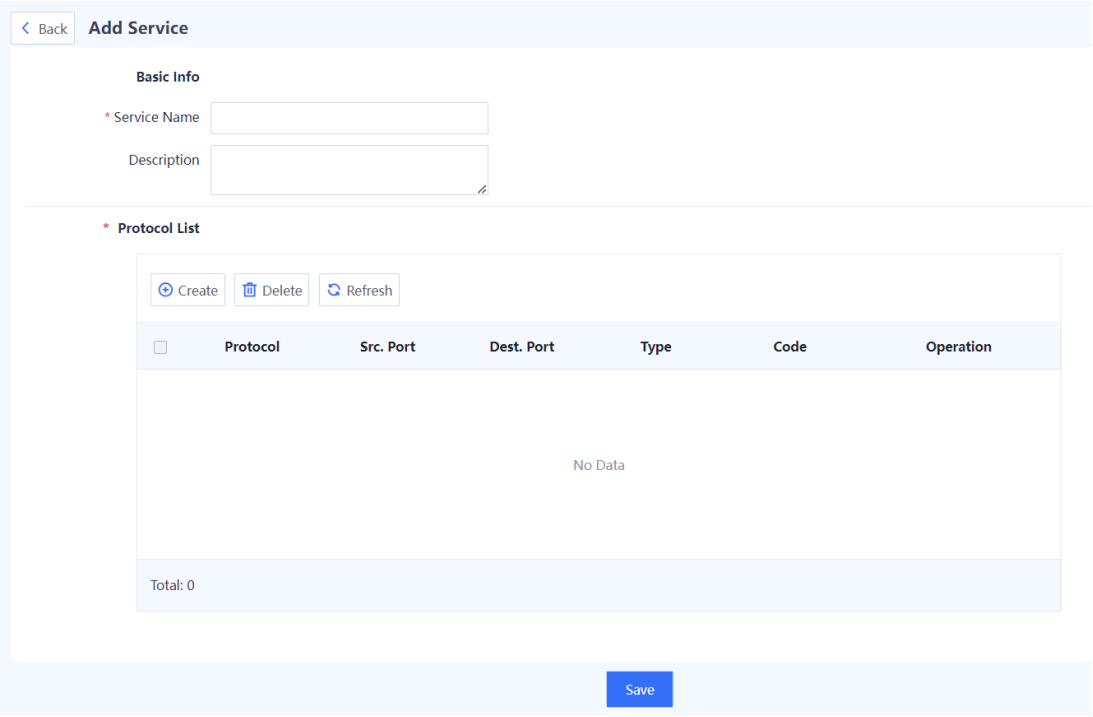
The interface configuration is as follows:

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
Ge0/0	-		Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
Ge0/1	-		Routing	untrust	IPv4: DHCP	172.26.1.116/24	-	1500	Edit

2.4.2 Configuring a Custom Service

(1) Choose **Object** > **Service** > **Custom Service**.

(2) Click **Create** and create a custom service **18080**. In the **Protocol List** area, click **Create**. In the dialog box that is displayed, set the protocol to TCP, the source port to 0-65535, and the destination port to 18080 (external port).



(3) Click **Save**.

2.4.3 Configuring a Security Policy

Choose **Policy** > **Security Policy** > **Security Policy**.

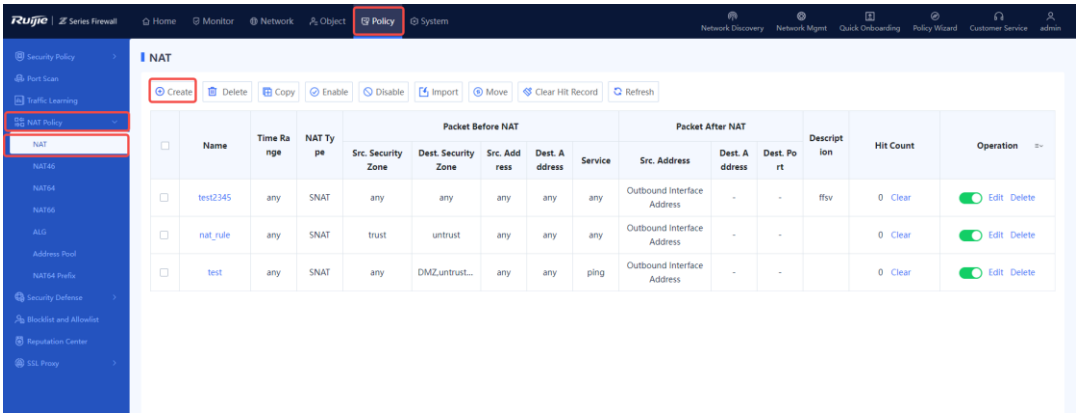
The policy configuration is as follows:

	2	allow_trus...	-	trust	any	untrust	any	any	any	any	Perm
			allow_trust_to_untrust								

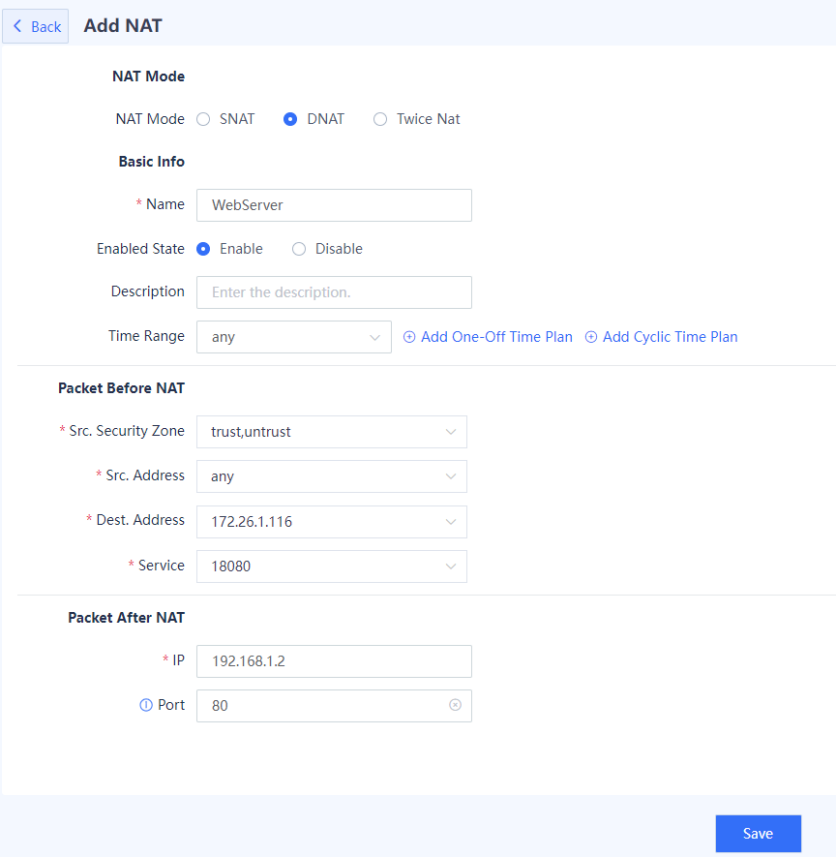
2.4.4 Configuring a Destination NAT Policy

(1) Choose **Policy** > **NAT Policy** > **NAT**.

(2) Click **Create**.



(3) Set parameters of the destination NAT policy.



Item	Description
Basic Info	
Name	WebServer

Item	Description
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	untrust and trust
Src. Address	any
Dest. Address	WAN interface address: 172.26.1.116
Service	Select the custom service **18080** created in 2.4.2 (2) .
Packet After NAT	
IP Address	192.168.1.2
Port	80 (internal port)

(4) Click **Save**.

2.5 Verification

Access the intranet server at 172.26.1.116 from the extranet.

3 Configuration Example of Enabling Intranet Users to Access Intranet Servers Through a Public IP Address

3.1 Applicable Products and Versions

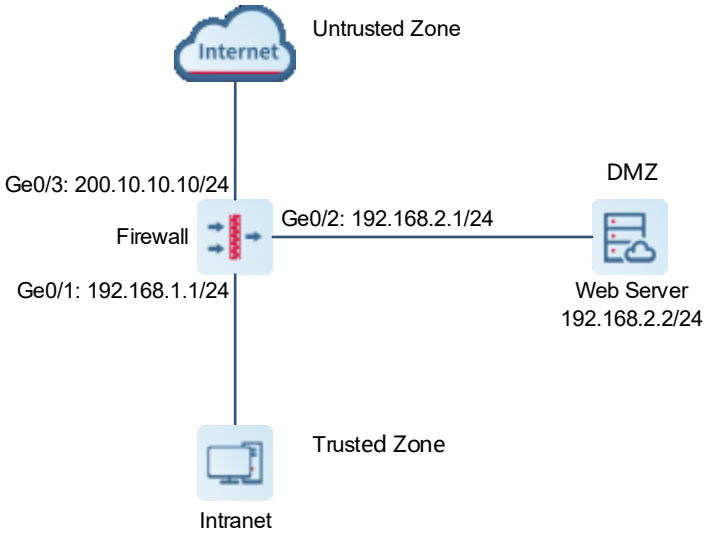
Table 3-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	NGFW_NTOS 1.0R1P2 or later

3.2 Service Demands

A company has deployed a firewall at the network border as a security gateway and a web server on the intranet to provide services to external users. The company requires that the IP address 192.168.2.2 of an intranet web server be mapped to the IP address 200.10.10.10 of an extranet interface so that both intranet and extranet users can access the web server.

- The web server is in the intranet server zone. The web server in the DMZ is at 192.168.2.2 and uses HTTPS.
- Extranet users can access the server through the extranet interface located in the untrust zone at 200.10.10.10 and using port 50000.
- Intranet users in the trust zone can also access the server through the extranet interface located in the untrust zone at 200.10.10.10 and using port 50000, and the extranet interface of the firewall is used as the source address to access the web server.



3.3 Prerequisites

Routing and related configurations have been completed in the early stage of network planning.

3.4 Procedure

3.4.1 Completing Basic Network Access Settings

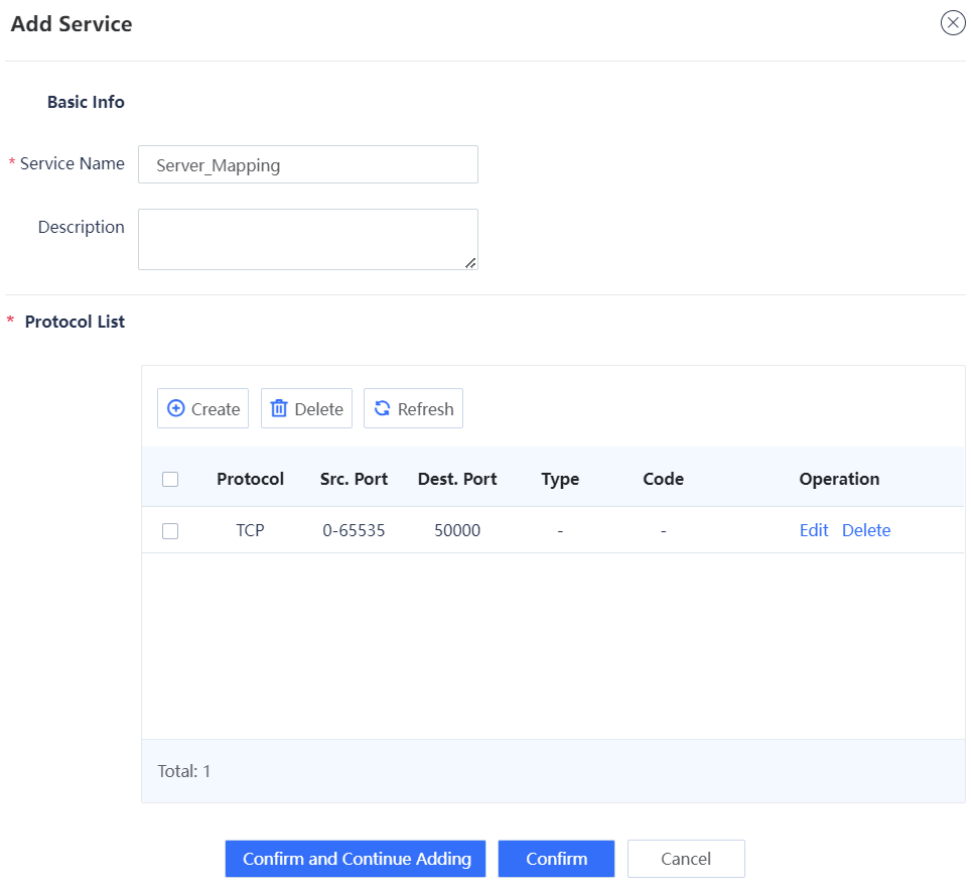
Choose **Network** > **Interface** > **Physical Interface**.

Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

3.4.2 Configuring a Custom Service

(1) Choose **Object** > **Service** > **Custom Service**.

(2) Click **Create** and create a custom service **Server_Mapping**. In the **Protocol List** area, click **Create**. In the dialog box that is displayed, set the protocol to TCP, the source port to 0-65535, and the destination port to 50000.



(3) Click **Save**.

3.4.3 Configuring a Security Policy

Choose **Policy** > **Security Policy** > **Security Policy**.

The policy configuration is as follows:

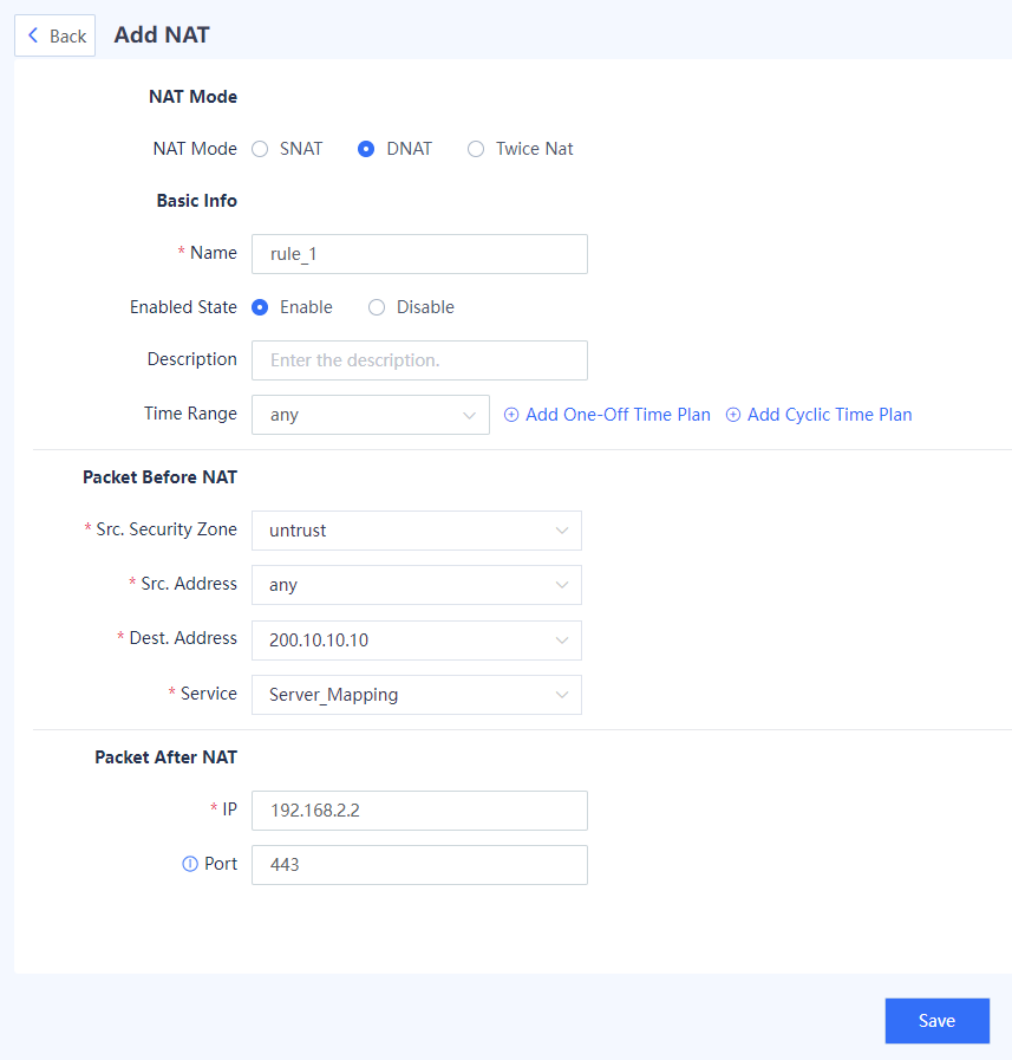
Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hi	Operation
Default Policy Group													
1	permit_loca	IPv4	trust	lan_users	untrust	any	any	any	any	Perm		0	Edit Delete

3.4.4 Configuring a Destination NAT Policy for Extranet Users

(1) Choose **Policy** > **NAT Policy** > **NAT**.

(2) Click **Create**.

(3) On the **Add NAT** page, set parameters of the destination NAT policy.



Item	Description
Basic Info	
Name	rule_1

Enabled State	Select **Enable**.
Packet Before NAT	
Src. Security Zone	Select **untrust**.
Src. Address	Select **any**.
Dest. Address	Extranet interface IP address of the firewall: 200.10.10.10.
Service	Select the custom service **Server_Mapping** created in 3.4.2 Configuring a Custom Service.
Packet After NAT	
IP Address	Set the destination address to the IP address of the web server in the DMZ: 192.168.2.2.
Port	Set the destination port to 443 (web server port).

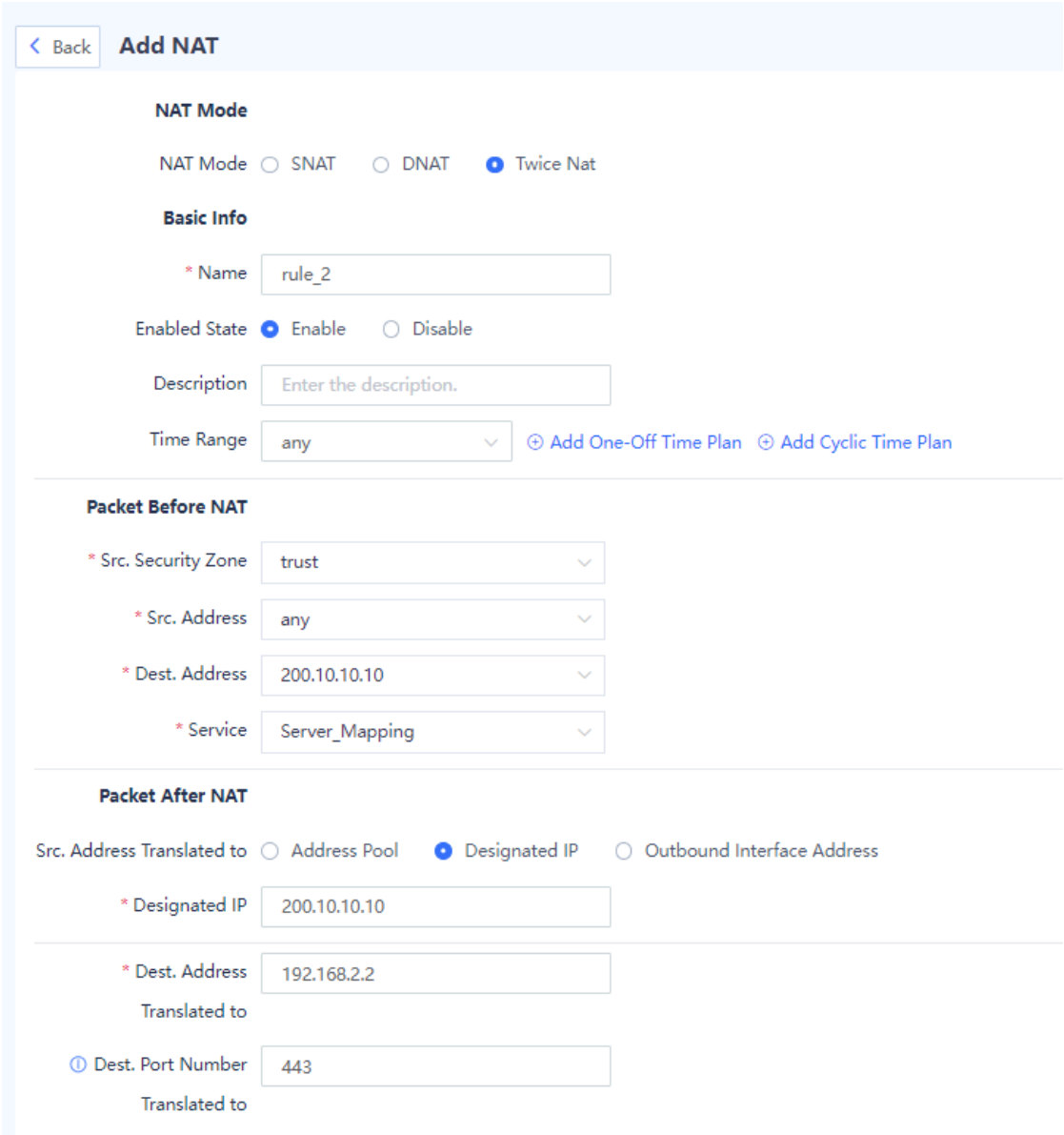
(4) Click **Save**.

3.4.5 Configuring a Twice NAT Policy for Intranet Users

(1) Choose **Policy** > **NAT Policy** > **NAT**.

(2) Click **Create**.

(3) On the **Add NAT** page, set parameters of a twice NAT policy.



Item	Description
Basic Info	
Name	rule_2
Enabled State	Select **Enable**.
Packet Before NAT	
Src. Security Zone	Select **trust**.
Src. Address	Select **any**.
Dest. Address	Outbound interface IP address of the firewall: Ge0/3:200.10.10.10.

Item	Description
Service	Select the custom service **Server_Mapping** created in 3.4.2 Configuring a Custom Service.
Packet After NAT	
Src. Address Translated to	In source NAT, configure the specified IP address 200.10.10.10 as the firewall's extranet address. If the firewall has multiple extranet addresses, you can configure an address pool as the extranet address, and then apply the address pool. Note: If you specify the outbound interface address, the source IP address will be translated into 192.168.2.1, which does not meet requirements.
Designated IP	Firewall's extranet address, for example, 200.10.10.10
Dest. Address Translated to	Set the IP address of the web server in the DMZ: 192.168.2.2.
Dest. Port Number Translated to	Set the web server port number to 443.

(4) Click **Save**.

3.5 Verification

- Visit http://200.10.10.10:50000 from the intranet.
- Visit http://200.10.10.10:50000 from the extranet.

The NAT policy is successfully configured if the intranet web server is accessible both from the intranet and extranet.

4 Configuration Example of Static NAT-PT Networking

4.1 Applicable Products and Versions

Table 4-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

4.2 Service Demands

In a NAT64 networking scenario, NAT-PT policies are typically deployed on the edge devices of IPv4 and IPv6 networks to translate addresses in mutual access packets between the IPv4 and IPv6 networks.

As shown in the following figure, a company is upgrading an IPv4 network to an IPv6 network. Before the network-wide upgrade, a partial network upgrade is performed first, and the network of an existing internal public server has been upgraded from IPv4 to IPv6. In this case, a NAT-PT policy needs to be configured on the firewall to translate IPv4 addresses into IPv6 addresses so that the public server can be accessed by the IPv4 network.

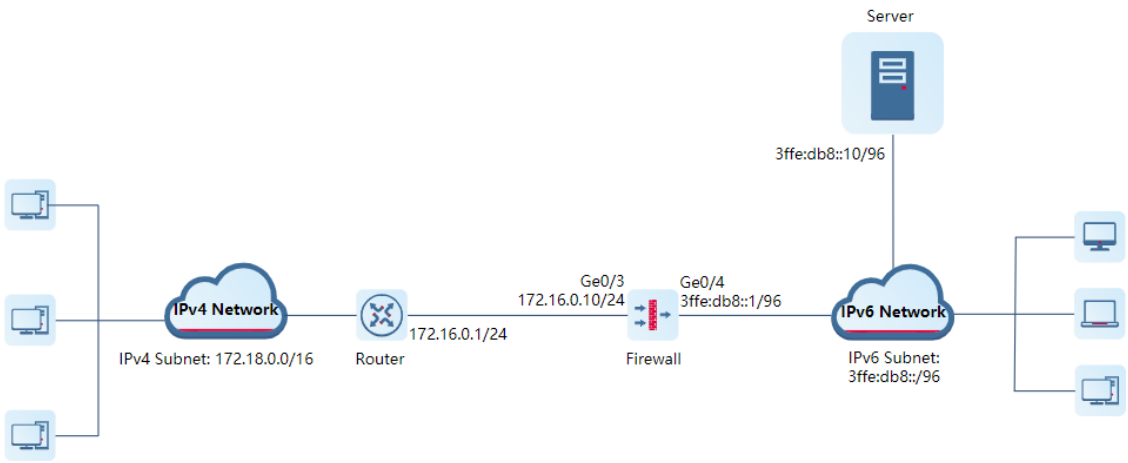


Table 4-2 **Key Configuration Points in the Network Diagram**

Item	Description
Pure IPv4 network	172.18.0.0/16
IPv4 network egress address	172.16.0.1/24
Public server	3ffe:db8::10/96
Pure IPv6 network	3ffe:db8::/96

Item	Description
NAT64 prefix information	2ffe:db8::/96, for route egress selection control
IPv4 address object	172.16.0.1, source IP address for accessing the public server 172.16.0.10, destination IP address for accessing the public server
IPv6 address object	3ffe:db8::10, for refined filtering based on security policies
Source IPv6 address after NAT	2ffe:db8::10
Destination IPv6 address after NAT	3ffe:db8::10
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
Any IPv4 address	0.0.0.0-255.255.255.255

4.3 Restrictions and Guidelines

- The destination IPv4 address that matches a static NAT-PT rule cannot be a non-local interface IP address on the same network segment as the inbound interface (for example, 172.16.0.100). You are advised to configure the destination IPv4 address as the IPv4 address of the inbound interface.
- The source or destination IPv4 address object that matches a static NAT-PT rule can only contain one IP address (that is, only one IP address can be configured). This restriction can be ignored if no device on an IPv6 network proactively accesses the IPv4 network.
- The source IPv6 address after NAT must be on the same network segment as the configured NAT64 prefix. For example, if the NAT64 prefix is 2ffe:db8::/96, the source IPv6 address after NAT is 2ffe:db8::10.
- If a static NAT-PT rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

4.4 Prerequisites

You have completed basic network configurations, including interface IP address and routing information on the router and server. Pay attention to the following points during configuration:

- Ensure that the IP addresses of the router and server are fixed.
- An SNAT rule and a default route have been configured on the router to ensure that packets from the IPv4 subnet are sent out through interface 172.16.0.1/24 and the source IP addresses are replaced with the outbound interface address 172.16.0.1.

4.5 Procedure

4.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

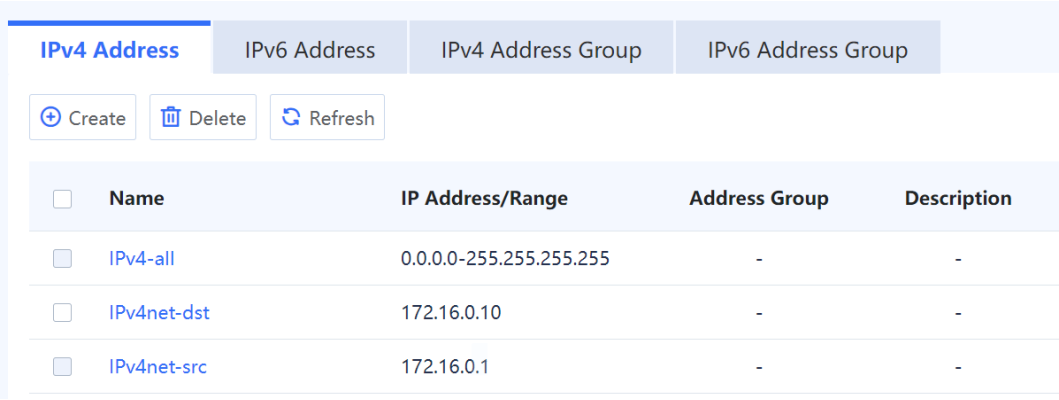
(3) Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

Caution

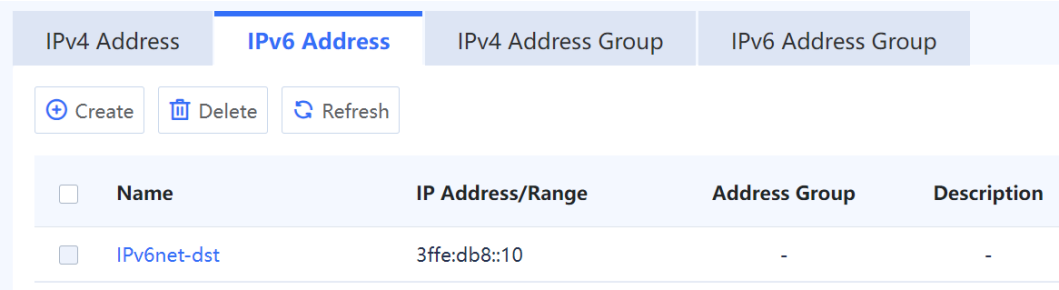
The IP address of an interface must be fixed.

4.5.2 Configuring a Static NAT-PT Rule

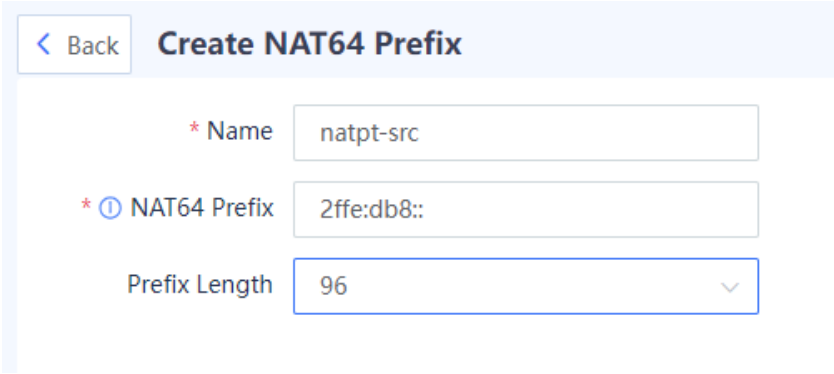
(1) Choose **Object** > **Address** > **IPv4 Address**. On the tab page that is displayed, click **Create** and create three IPv4 address objects according to the following figure.



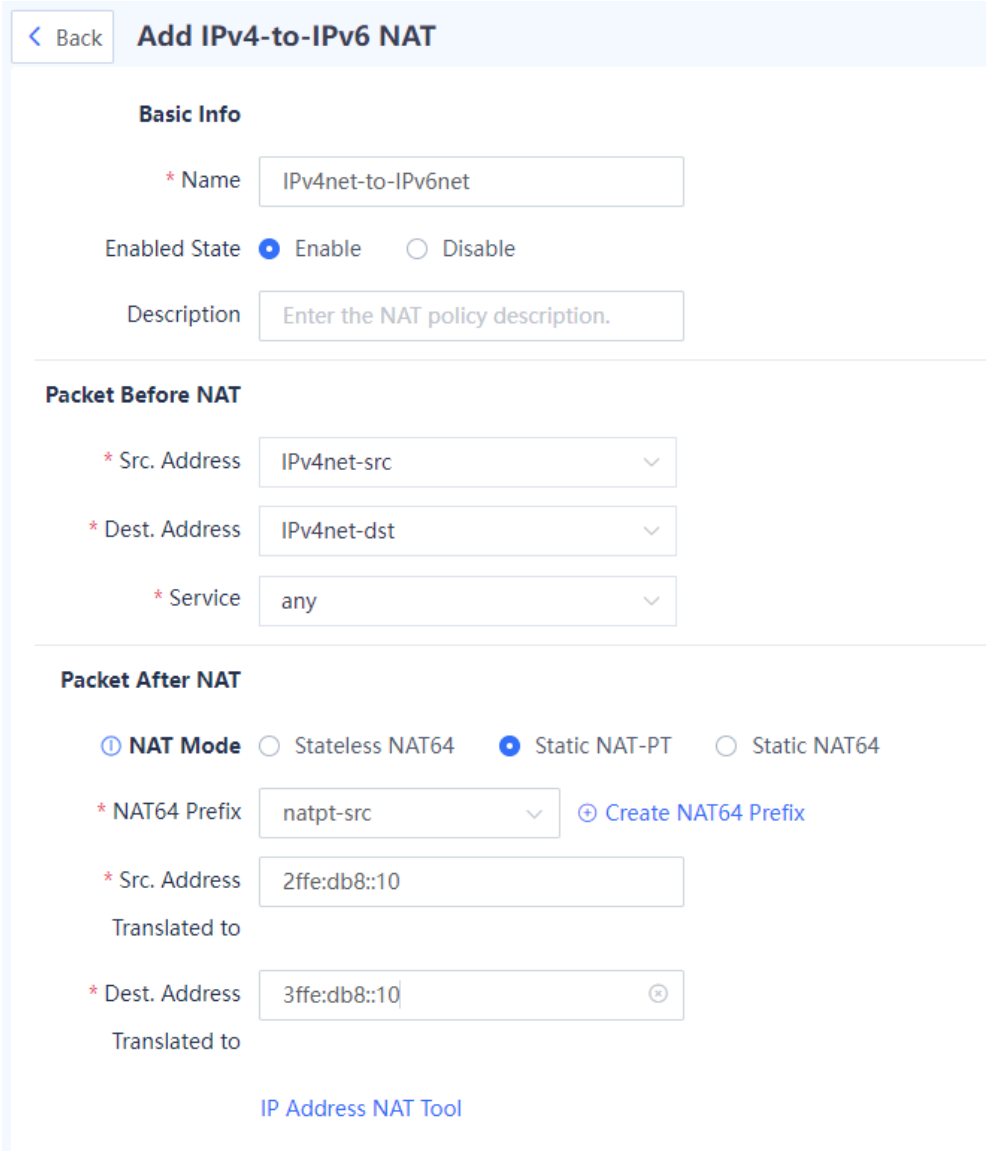
(2) Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.



(3) Choose **Policy** > **NAT Policy** > **NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.



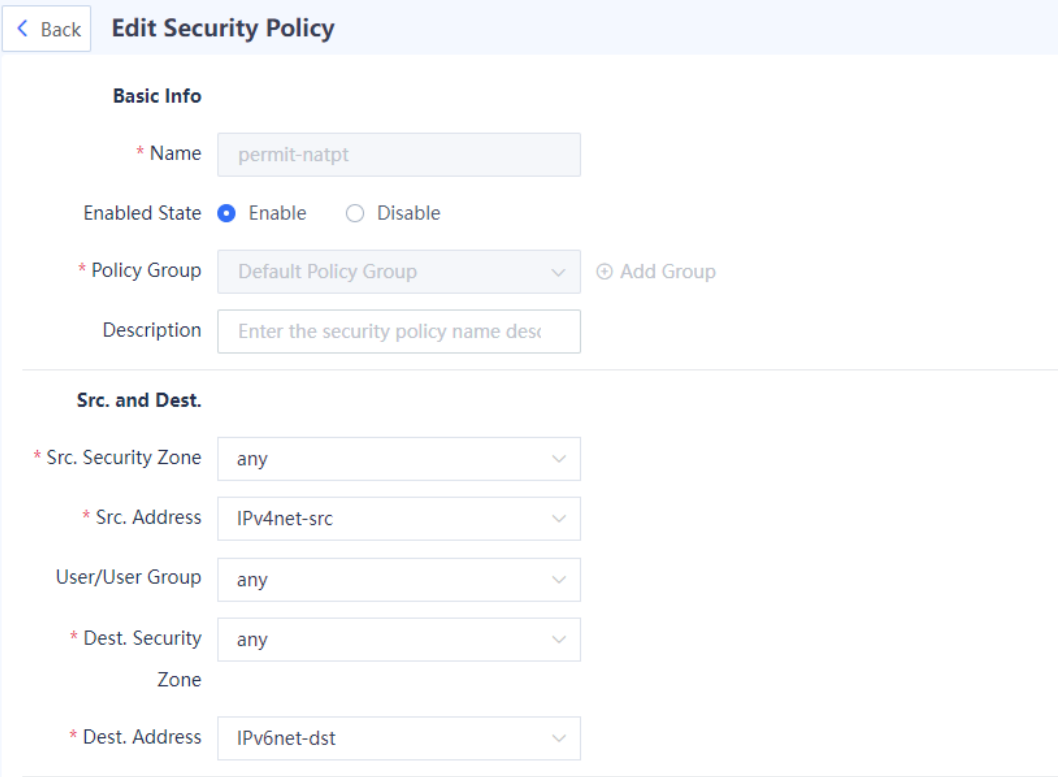
(4) Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a static NAT-PT rule according to the following figure. Configuration items with the asterisk (*) are mandatory.

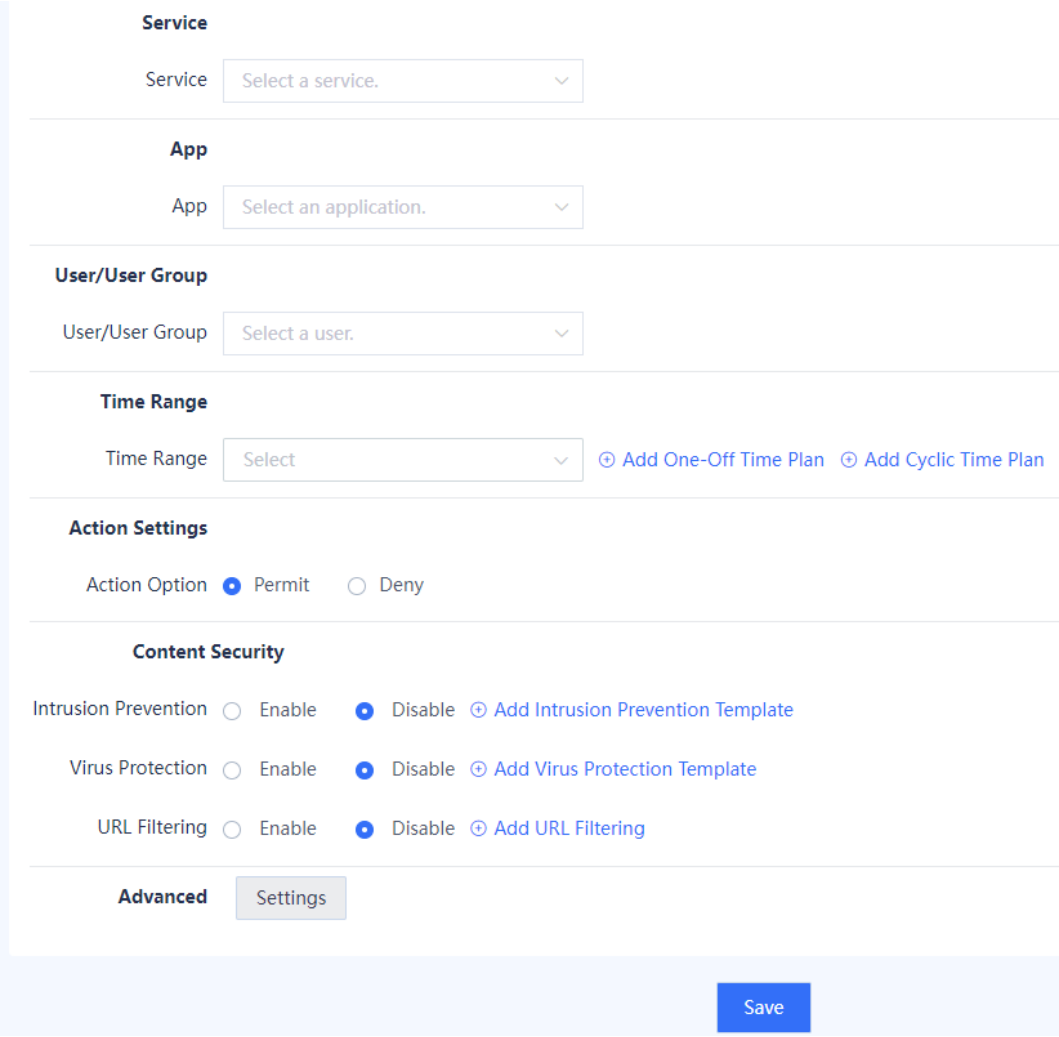


(5) After verifying the configuration, click **Save**.

4.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

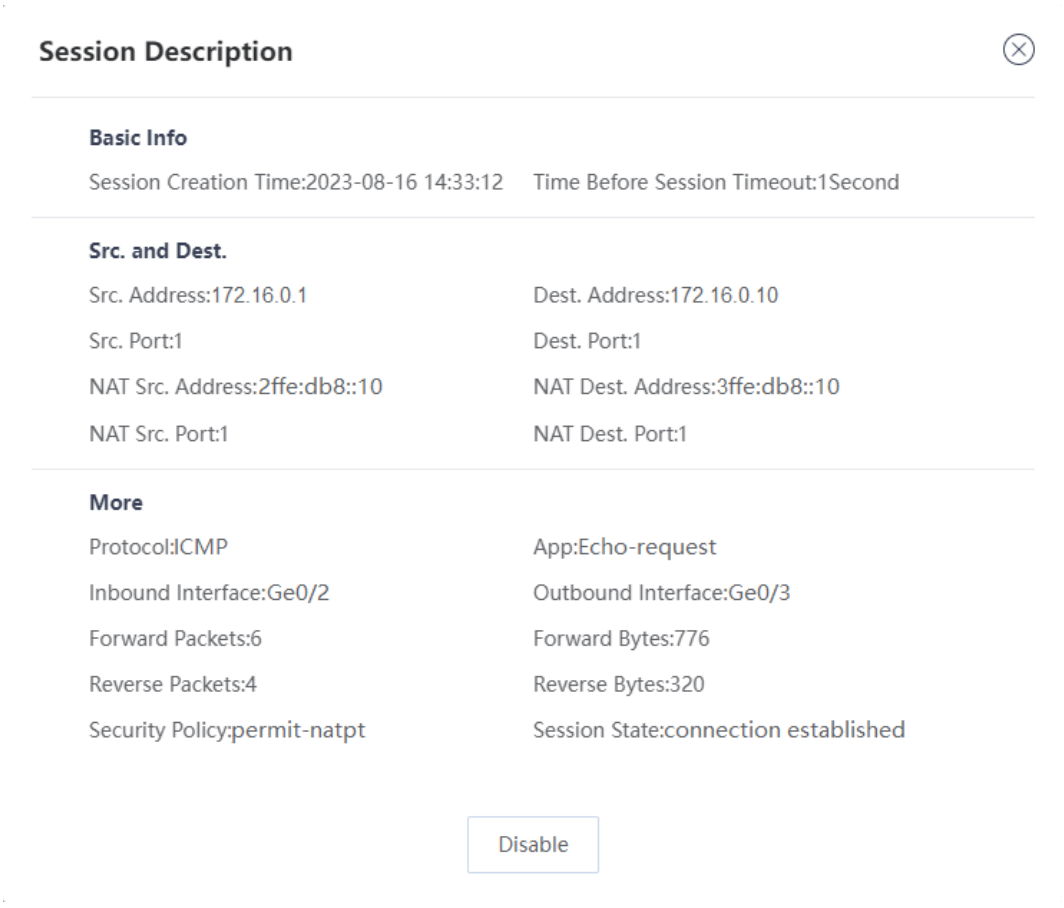




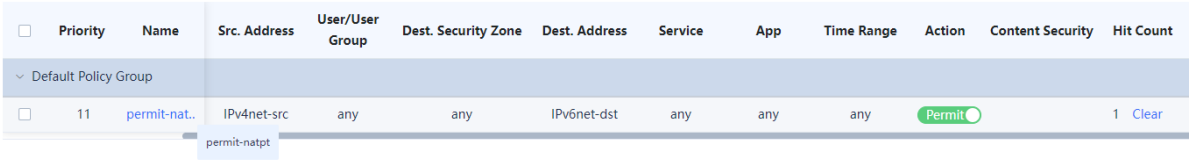
(2) After verifying the configuration, click **Save**.

4.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.



- Choose **Policy** > **Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-natpt** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)



Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
Default Policy Group											
11	permit-nat..	IPv4net-src	any	any	IPv6net-dst	any	any	any	Permit		1 Clear

permit-natpt

- Choose **Policy** > **NAT Policy** > **NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

Name	NAT Mode	Packet Before NAT			Packet After NAT				Hit Count
		Src. Address	Dest. Address	Service	NAT64 Prefix	Src. Address Translated to	Dest. Address Translated to	Dest. Port Number Translated to	
IPv4net-to-IPv6net	Static NAT-PT	IPv4net-src	IPv4net-dst	any	natpt-src	2ffe:db8::10	3ffe:db8::10	-	1 Clear

5 Configuration Example of Dynamic NAT-PT Networking

5.1 Applicable Products and Versions

Table 5-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

5.2 Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. To ensure the continuity of production and office services during the network upgrade, of the company, some servers that are frequently accessed cannot be migrated or upgraded in the early stage. Therefore, a NAT-PT policy needs to be configured on the firewall to ensure that departments that have been upgraded to an IPv6 network can access these IPv4 servers.

During network upgrade planning, fixed-mapped IPv6 addresses need to be assigned to these IPv4 servers to allow access from an IPv6 subnet.

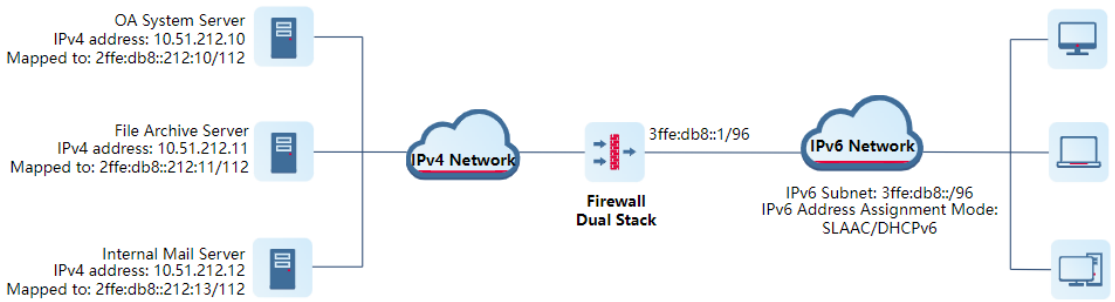


Table 5-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200

Item	Description
NAT64 prefix information	2ffe:db8::/96, IPv6 subnet mapped from the destination IPv4 address
IPv6 subnet	3ffe:db8::/96
IPv6 address object 1	3ffe:db8::/96
IPv6 address object 2	2ffe:db8::212:10, mapped IPv6 address of the OA system server
IPv4 address object 1	10.51.212.10, IPv4 address of the OA system on the IPv4 network
IPv4 address pool	172.16.10.100-172.16.10.139
Port range	11001-12000
Source NAT mode	Port Address Translation (PAT), that is, reusing IP addresses
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

5.3 Restrictions and Guidelines

- Dynamic NAT-PT does not support NAT hairpinning.
- If a dynamic NAT-PT rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- If the address pool object referenced by the source NAT address pool is referenced by a NAT64 rule and the specified NAT mode is NO-PAT, the address pool object cannot be referenced by other NAT64 rules with a NAT mode of PAT.

5.4 Prerequisites

(1) During network planning, you have verified that routes are available for diverting traffic from the IPv4 network to the device (firewall) where the IPv4 address pool is located.

(2) During network planning, you have verified that routes are available for diverting traffic from the IPv6 address to the device (firewall) that performs NAT64. That is, the destination addresses are reachable from both the IPv4 and IPv6 networks.

5.5 Procedure

5.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

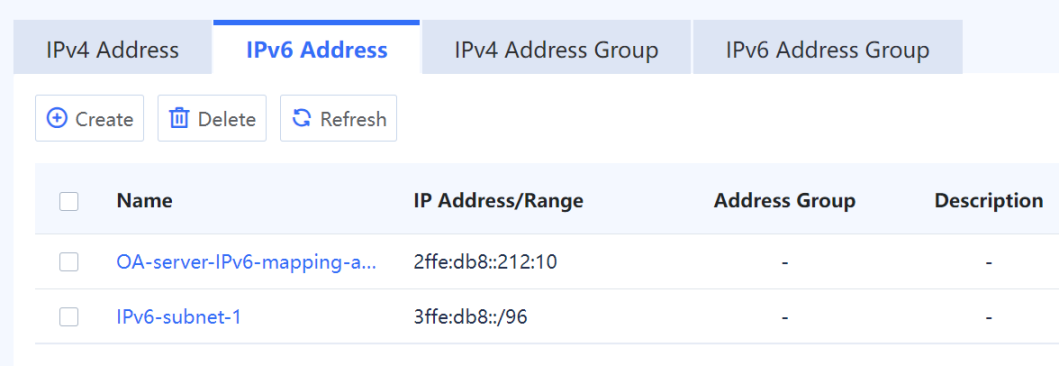
(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

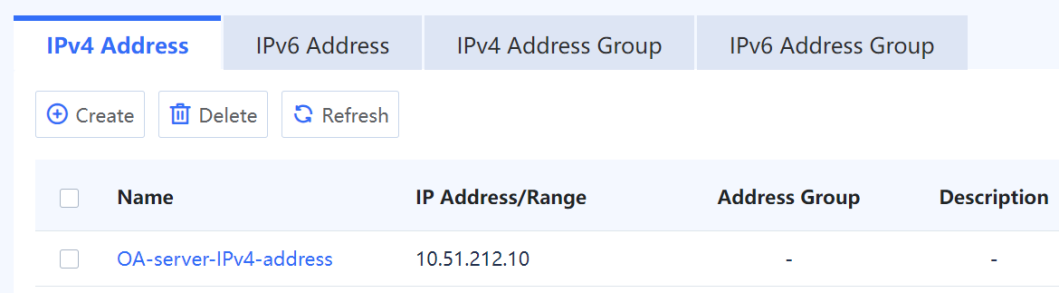
(3) Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

5.5.2 Configuring a Dynamic NAT-PT Rule

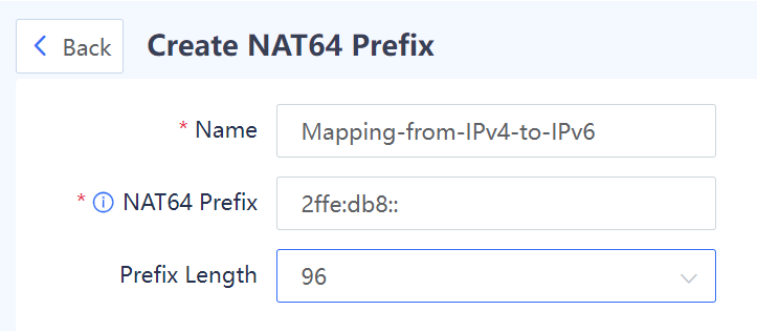
(1) Choose **Object** > **Address** > **IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.



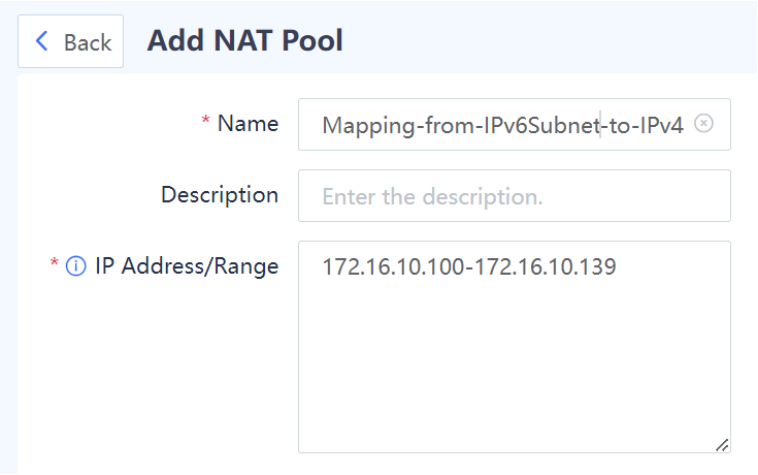
(2) Choose **Object** > **Address** > **IPv4 Address**. On the tab page that is displayed, click **Create** and create an IPv4 address object according to the following figure.



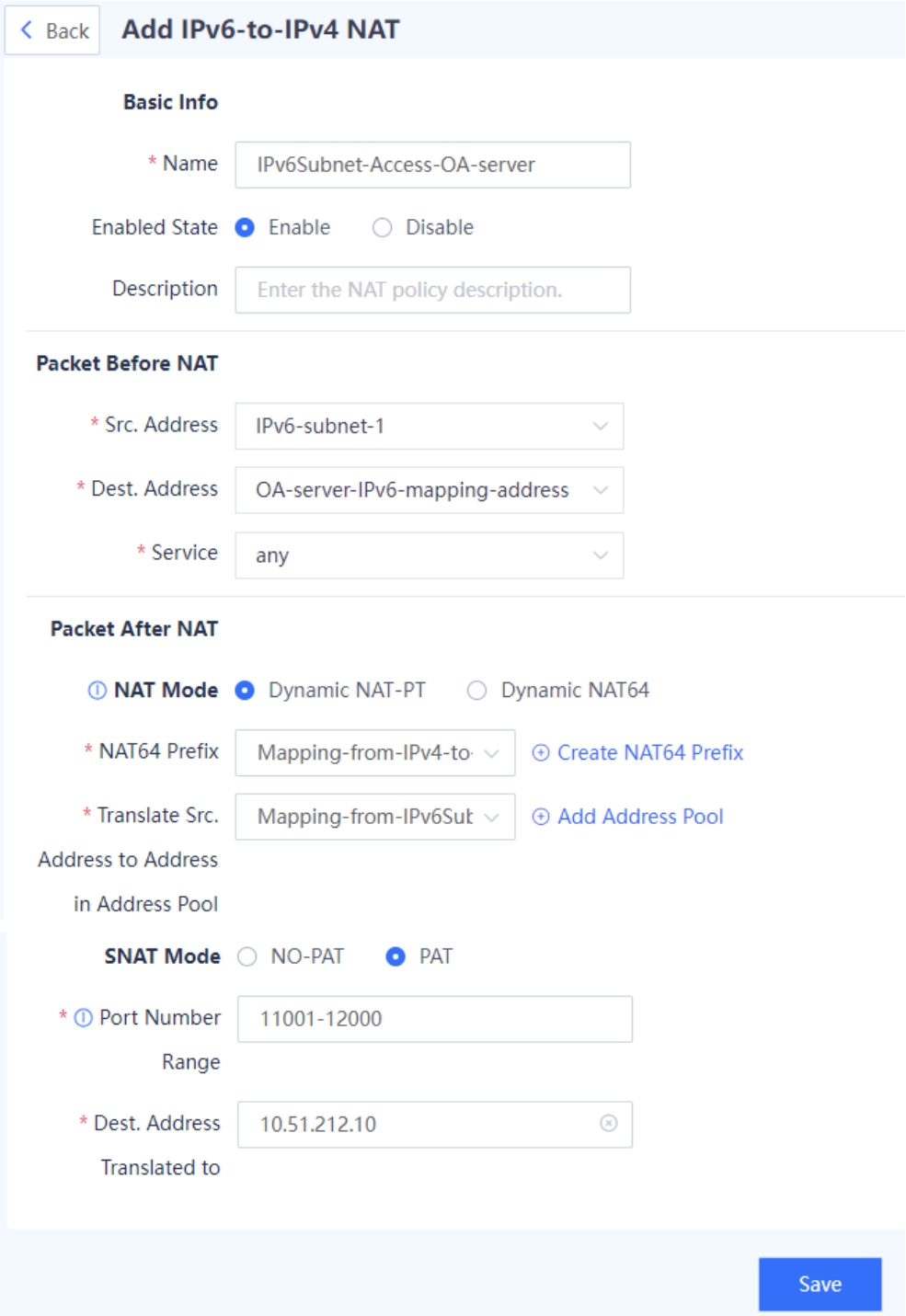
(3) Choose **Policy** > **NAT Policy** > **NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.



(4) Choose **Address Pool** from the navigation pane. On the page that is displayed, click **Create** and configure a NAT pool for the IPv6 subnet.



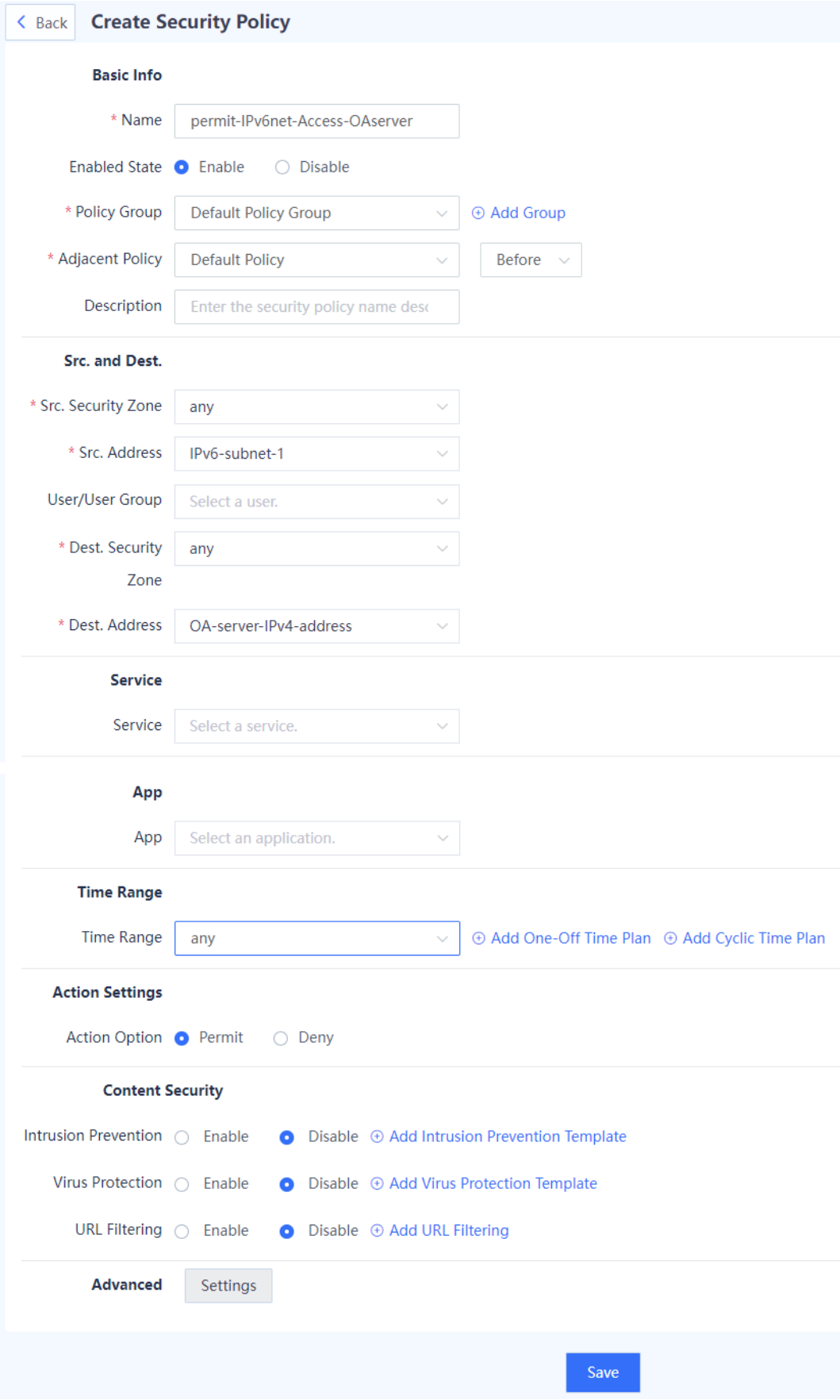
(5) Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a dynamic NAT-PT rule according to the following figure. Configuration items with the asterisk (*) are mandatory.



(6) After verifying the configuration, click **Save**.

5.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

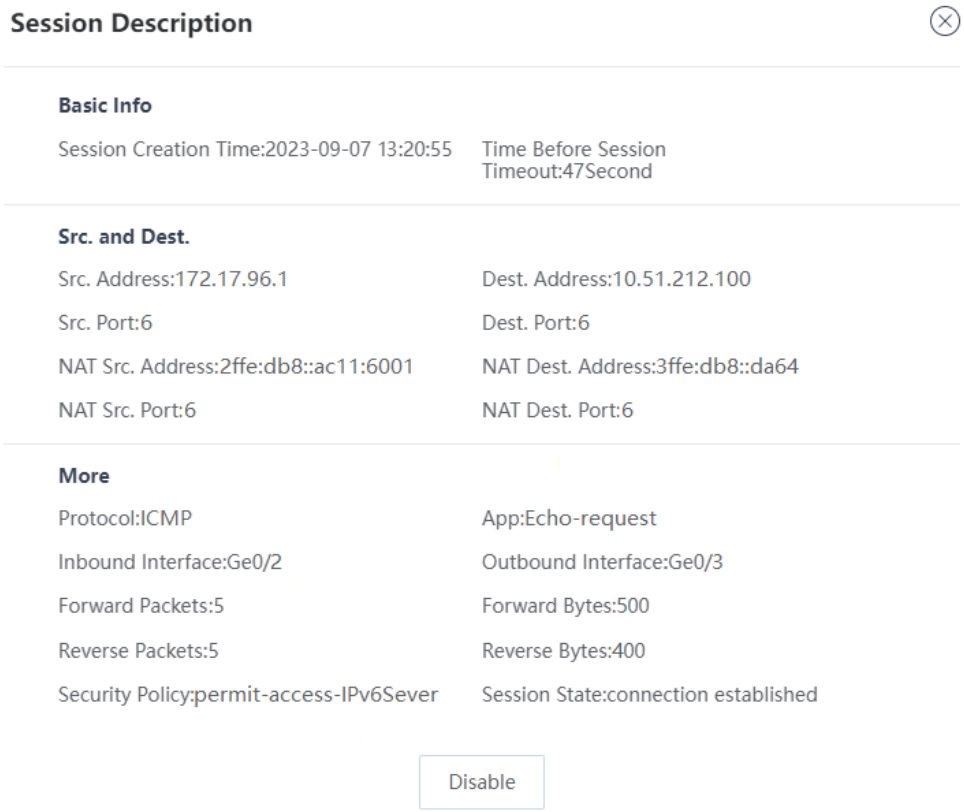
(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.



(2) After verifying the configuration, click **Save**.

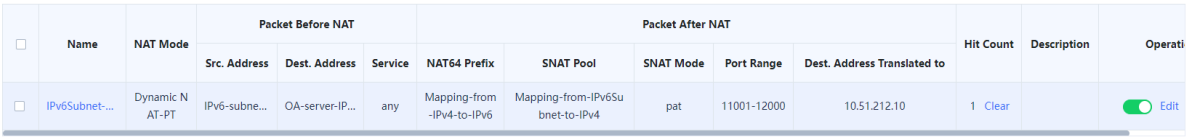
5.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.



- Choose **Policy** > **Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6net-Access-OAserver** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

- Choose **Policy** > **NAT Policy** > **NAT64**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)



6 Configuration Example of Stateless NAT64 Networking

6.1 Applicable Products and Versions

Table 6-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

6.2 Service Demands

In a NAT64 networking scenario, NAT-PT policies are typically deployed on the edge devices of IPv4 and IPv6 networks to translate addresses in mutual access packets between the IPv4 and IPv6 networks.

A company is upgrading an IPv4 network to an IPv6 network. Hosts on the IPv4 network need to access the public server, and hosts on the IPv4 and IPv6 networks can access each other.

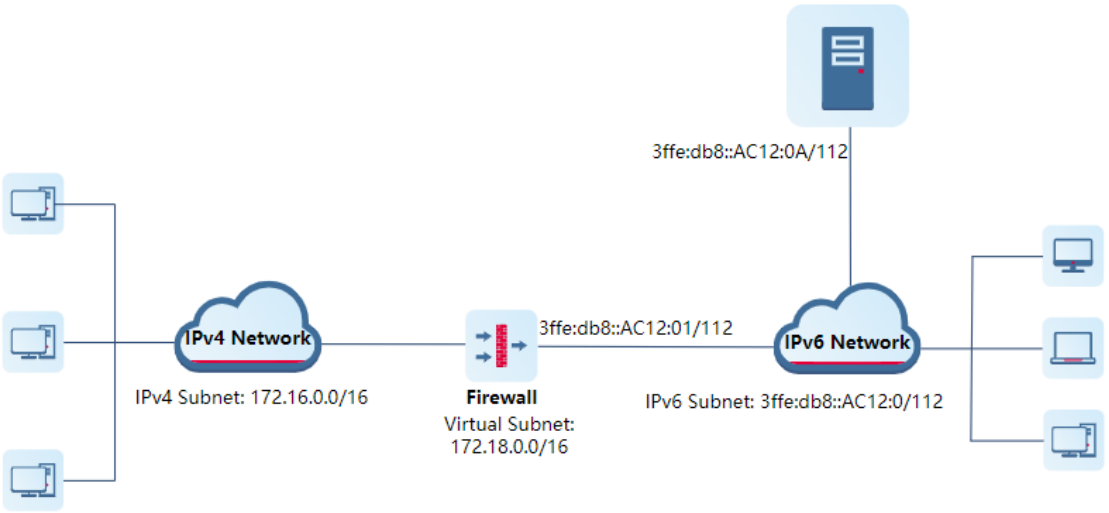


Table 6-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the	192.168.1.200

Item	Description
firewall management port	
NAT64 prefix information	3ffe:db8::/96
Virtual subnet	172.18.0.0/16, virtual subnet address mapped from an IPv6 address when a host on the IPv4 network accesses the IPv6 network
IPv6 subnet	3ffe:db8::AC12:0:0/112, for planning IPv6 addresses obtained by devices on an IPv6 network. The number of addresses it contains is equal to that of the virtual subnet, and the IPv4 subnet represented by the last 32 bits is the same as the virtual subnet.
IPv4 address object 1	172.16.0.0/16
IPv4 address object 2	172.18.0.0/16
IPv6 address object 1	3ffe:db8::AC12:0/112
Any IPv4 address	0.0.0.0-255.255.255.255

6.3 Restrictions and Guidelines

- Stateless NAT64 does not support NAT hairpinning.
- If a stateless NAT64 rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

6.4 Procedure

6.4.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

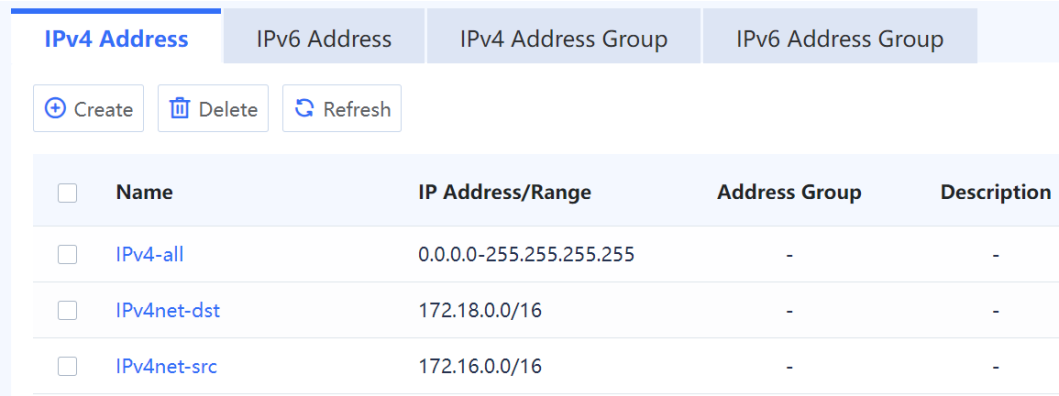
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

6.4.2 Configuring a Stateless NAT64 Rule

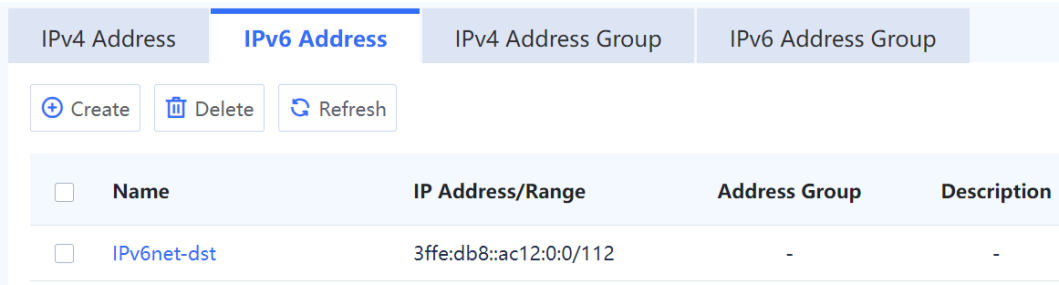
Caution

The address of the virtual subnet 172.18.0.0/16 does not exist on a physical network device interface.

(1) Choose **Object** > **Address** > **IPv4 Address**. On the tab page that is displayed, click **Create** and create IPv4 address objects according to the following figure.

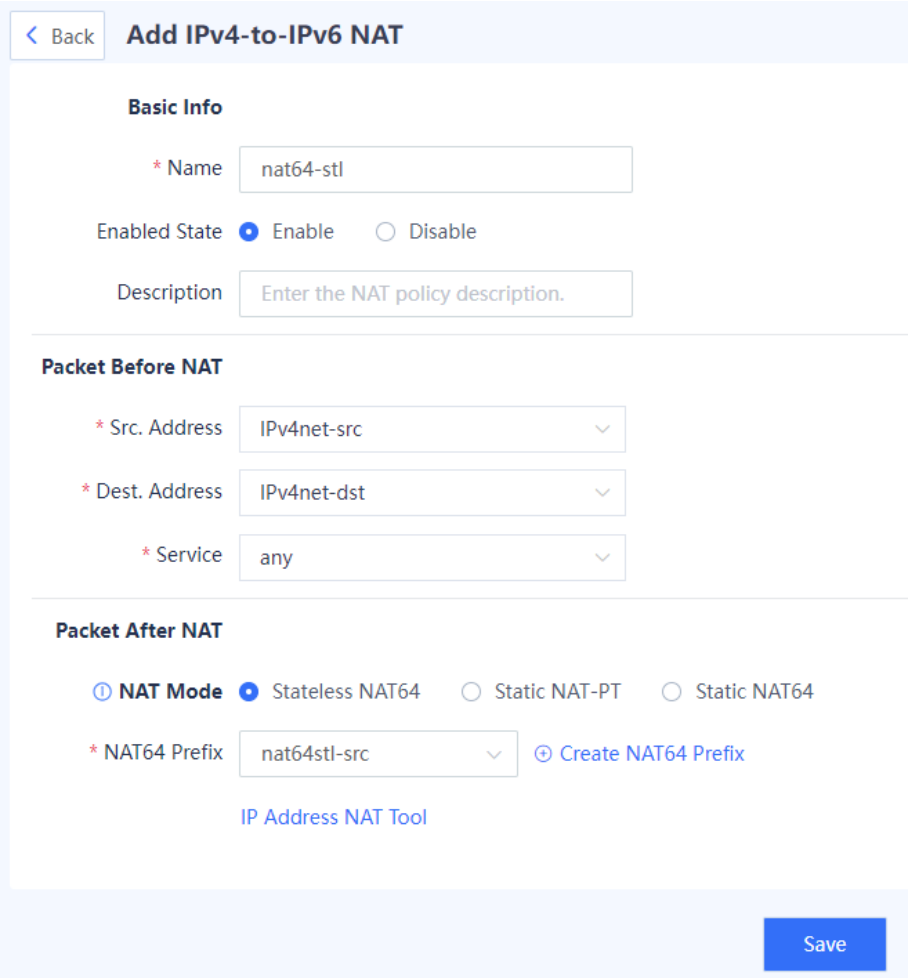


(2) Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.



(3) Choose **Policy** > **NAT Policy** > **NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.

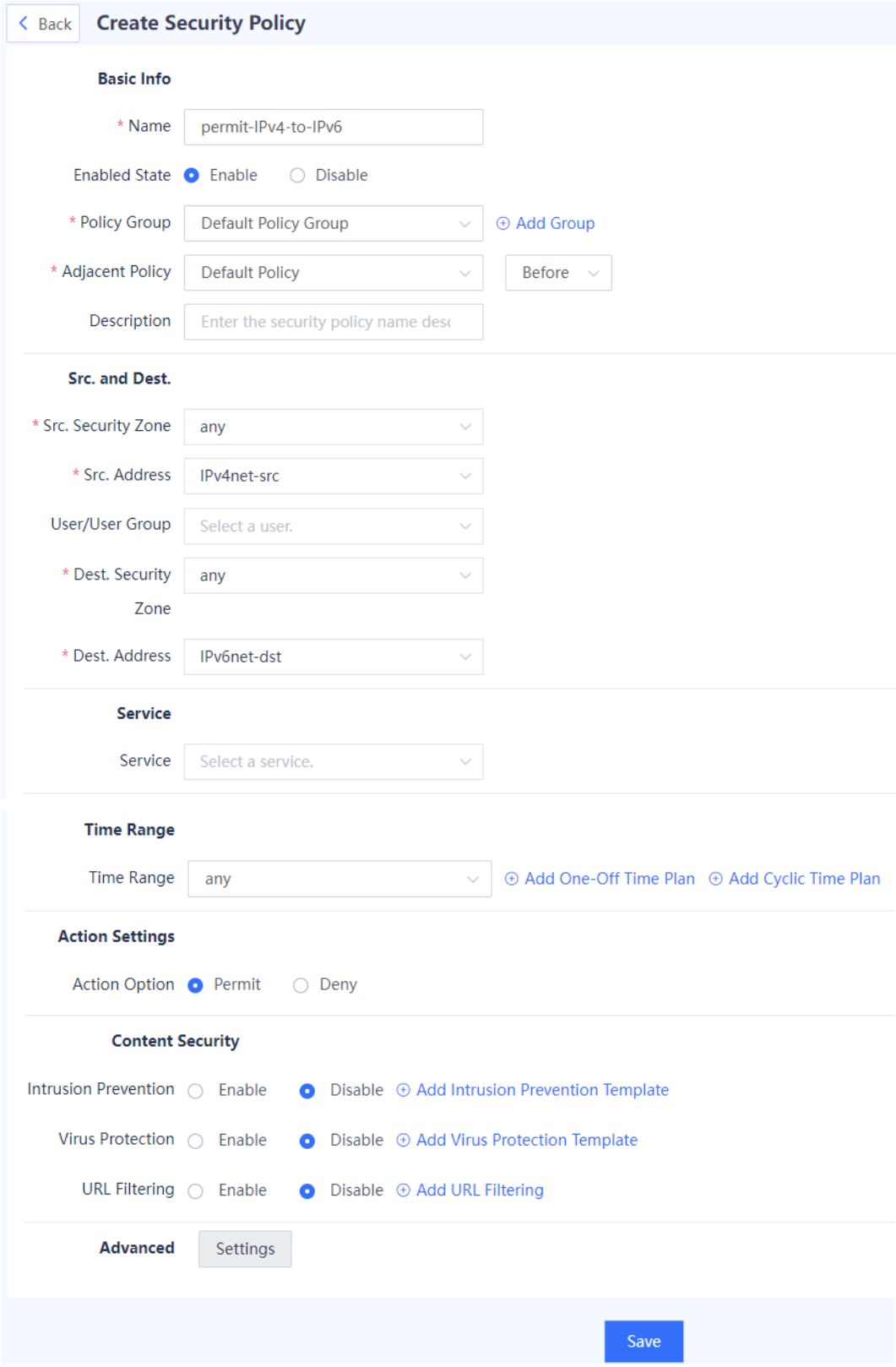
(4) Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a stateless NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.



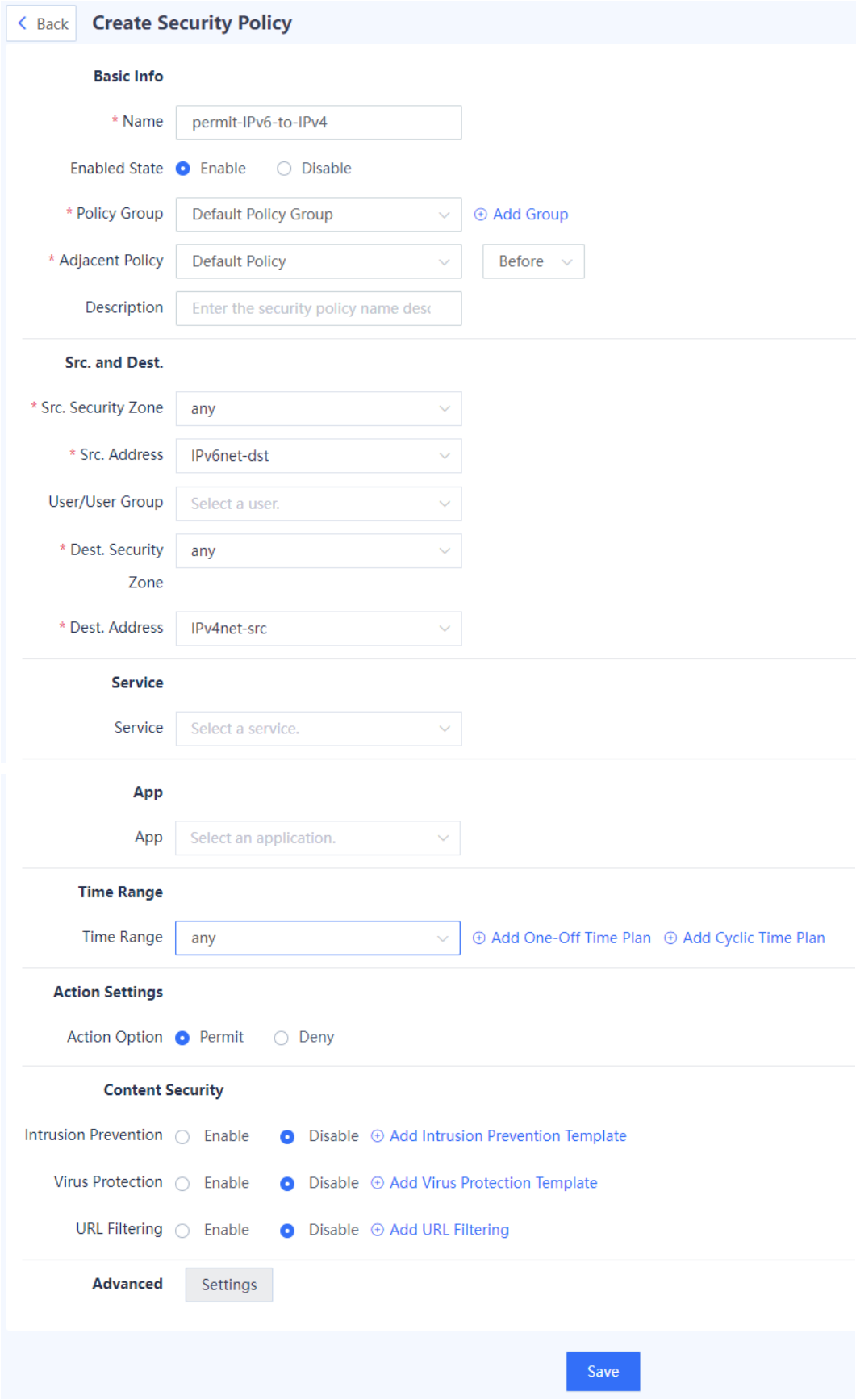
6.4.3 Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

Configure security policy 1 to permit packets from the IPv4 network to IPv6 network. Configure the source and destination addresses to reference address objects **IPv4net-src** and **IPv6net-dst**, respectively. Set the action to **Permit**.



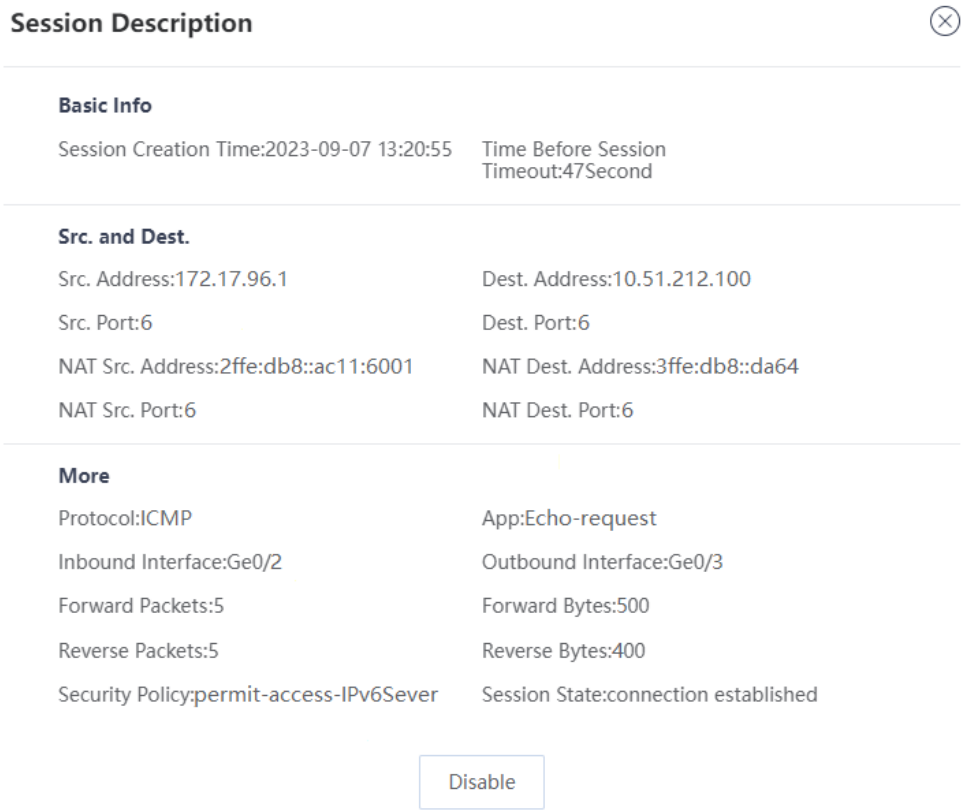
Configure security policy 2 to permit packets from the IPv6 network to IPv4 network. Configure the source and destination addresses to reference address objects **IPv6net-dst** and **IPv4net-src**, respectively. Set the action to **Permit**.



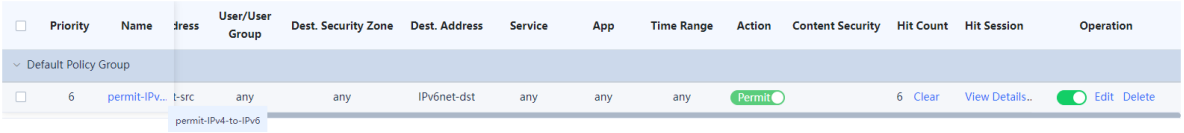
(2) After verifying the configuration, click **Save**.

6.5 Verification

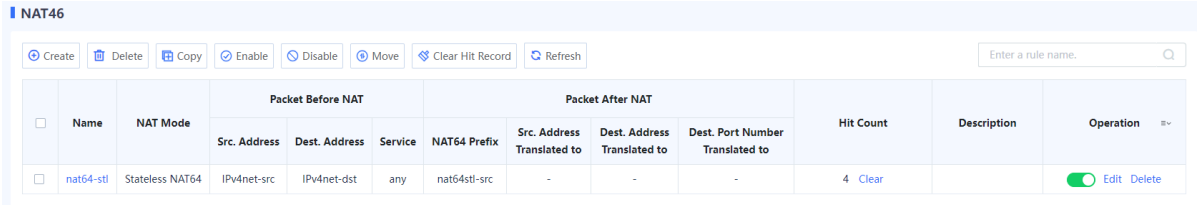
- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.



- Choose **Policy** > **Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6-to-IPv4** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)



- Choose **Policy** > **NAT Policy** > **NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)



7 Configuration Example of Static NAT64 Networking

7.1 Applicable Products and Versions

Table 7-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

7.2 Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. A server at the HQ has been upgraded to the IPv6 network, and branches in other cities need to access this server (using a domain name). Therefore, during network planning, this server needs to be mapped to an address on the IPv4 network.

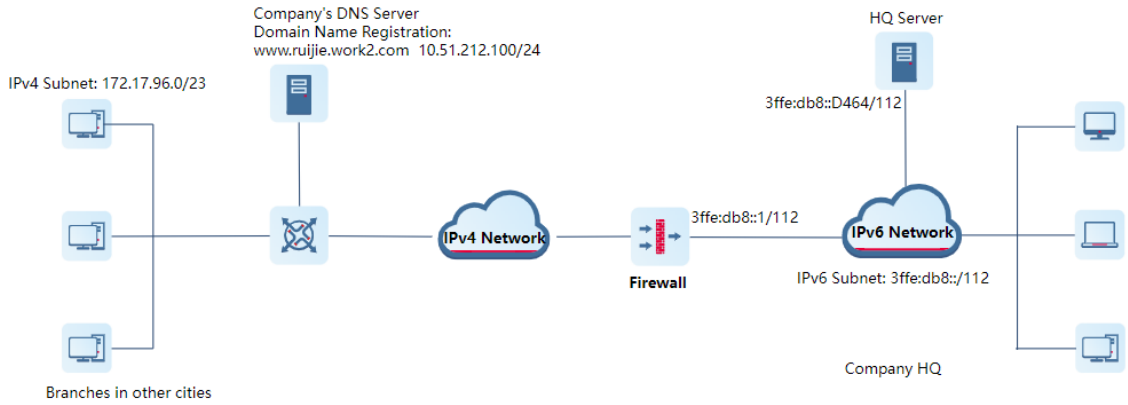


Table 7-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix information	2ffe:db8::/96
IPv6 subnet	3ffe:db8:: /112, for planning IPv6 addresses obtained by devices on an IPv6 network. The number of addresses it contains is equal to that of the virtual subnet, and the IPv4 subnet represented by

Item	Description
	the last 32 bits is the same as the virtual subnet.
IPv4 address object 1	172.17.96.0/23
IPv4 address object 2	10.51.212.100
IPv6 address object 1	3ffe:db8::D464
Any IPv4 address	0.0.0.0-255.255.255.255

7.3 Restrictions and Guidelines

- Static NAT64 does not support NAT hairpinning.
- If a static NAT64 rule needs to match any IPv4 address, you need to configure an any IPv4 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.

7.4 Prerequisites

You have registered the HQ server domain name **www.ruijie.work2.com** to be accessed by the IPv4 network on the company's DNS64 server. Traffic can be diverted to the edge firewall of the HQ based on the resolved address.

7.5 Procedure

7.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

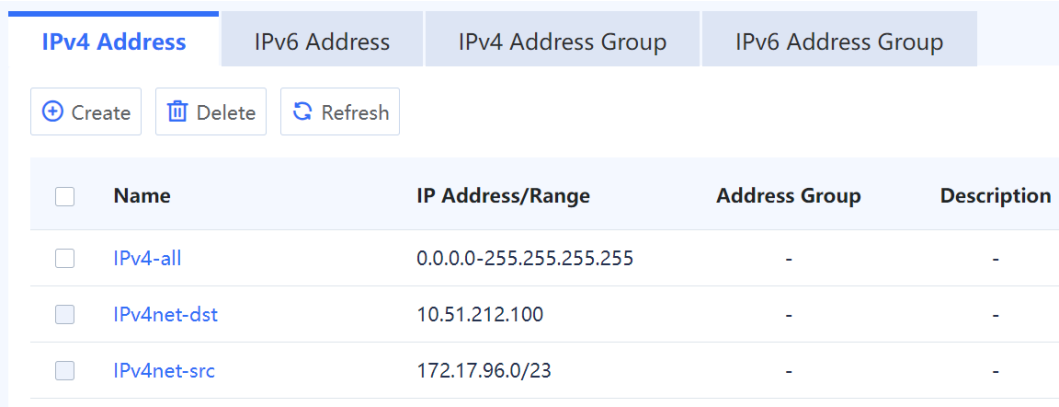
(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

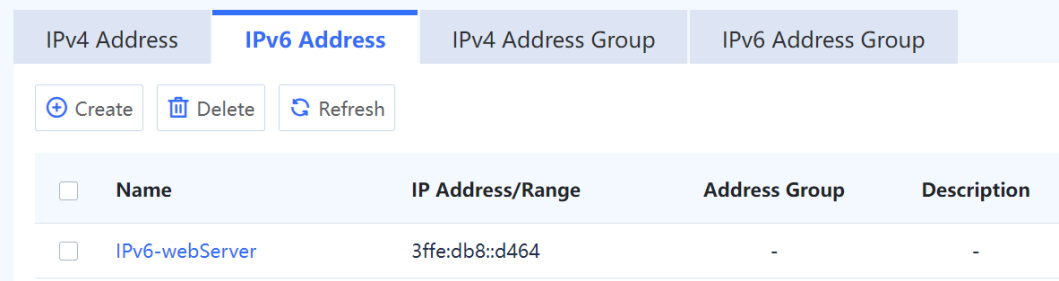
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

7.5.2 Configuring a Static NAT64 Rule

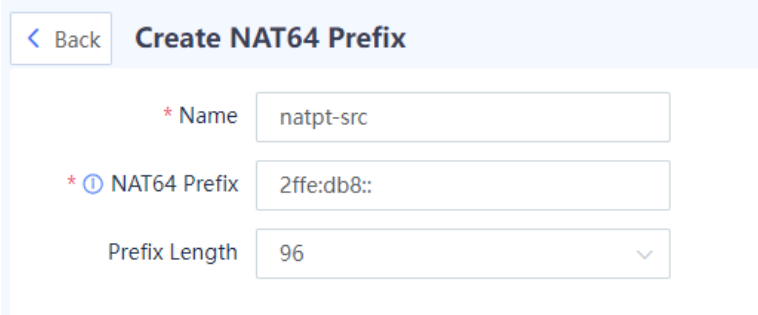
(1) Choose **Object** > **Address** > **IPv4 Address**. On the tab page that is displayed, click **Create** and create IPv4 address objects according to the following figure.



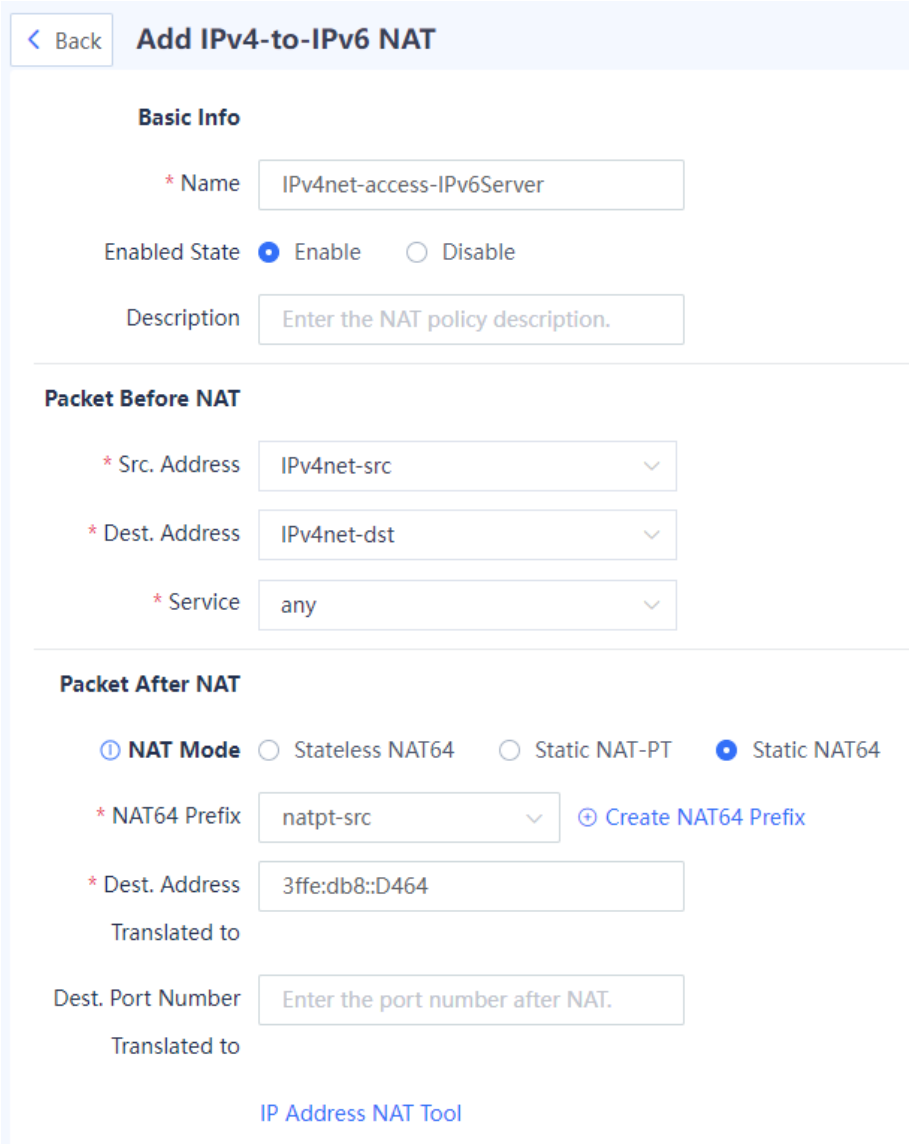
(2) Click the **IPv6 Address** tab. On the tab page that is displayed, click **Create** and create an IPv6 address object according to the following figure.



(3) Choose **Policy** > **NAT Policy** > **NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.



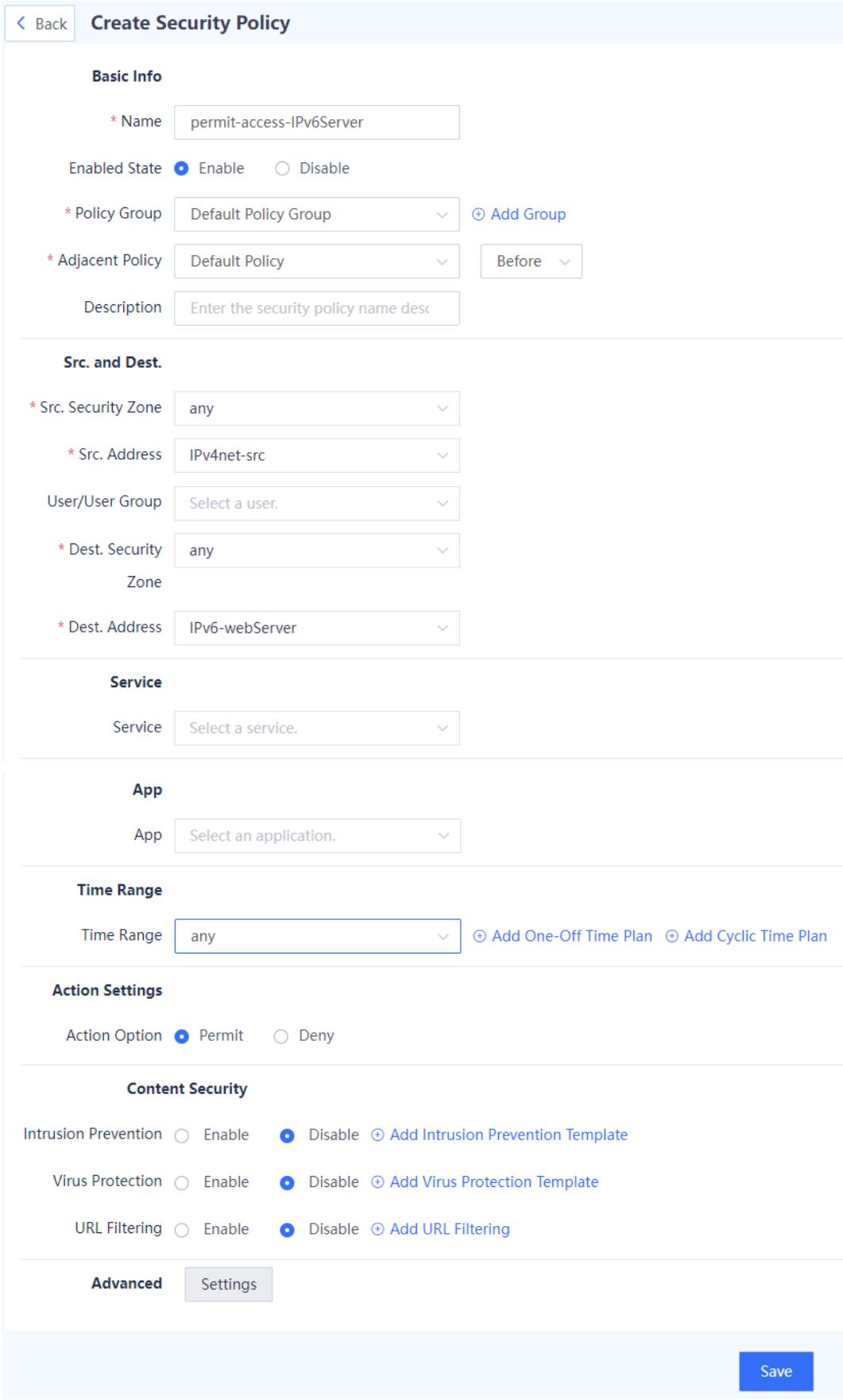
(4) Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a static NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.



(5) After verifying the configuration, click **Save**.

7.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

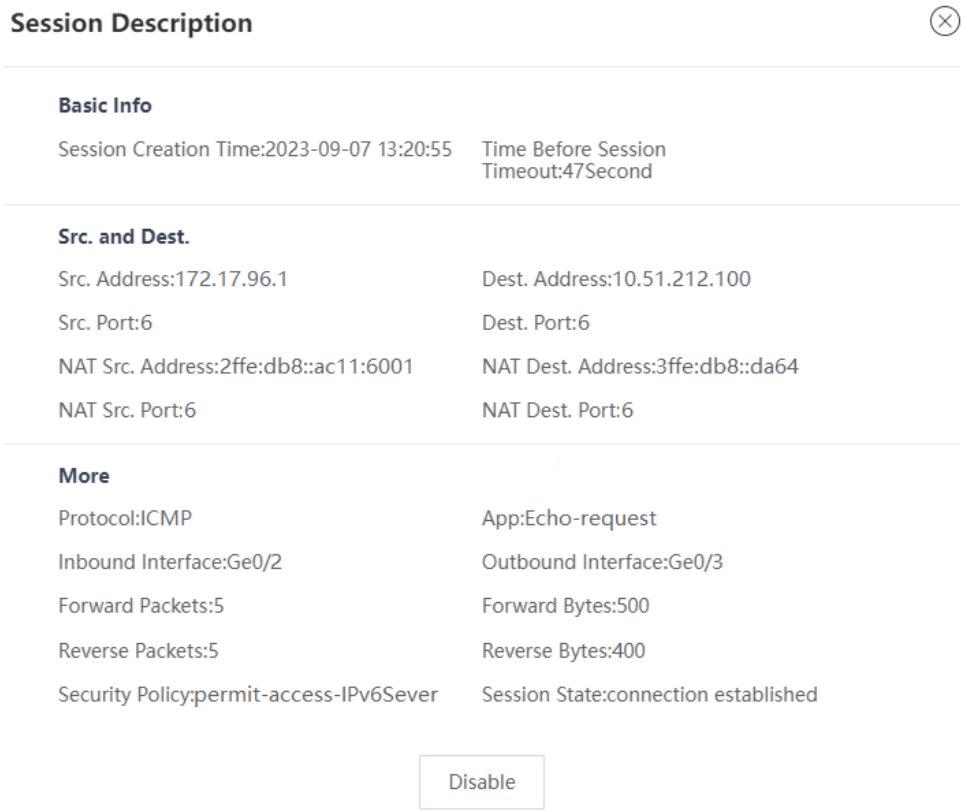
(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.



(2) After verifying the configuration, click **Save**.

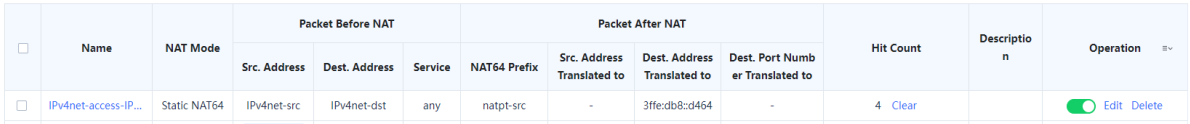
7.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.



- Choose **Policy** > **Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-access-IPv6Server** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

- Choose **Policy** > **NAT Policy** > **NAT46**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)



8 Configuration Example of Dynamic NAT64 Networking

8.1 Applicable Products and Versions

Table 8-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

8.2 Service Demands

A company HQ is upgrading an IPv4 network to an IPv6 network. To ensure the continuity of production and office services during the network upgrade, of the company, some servers that are frequently accessed cannot be migrated or upgraded in the early stage. Therefore, a NAT-PT policy needs to be configured on the firewall to ensure that departments that have been upgraded to an IPv6 network can access these IPv4 servers.

During network upgrade planning, fixed-mapped IPv6 addresses can be assigned to these IPv4 servers to allow access from an IPv6 subnet. However, fixed mappings make network maintenance difficult if device addresses on the network change. If fixed mappings exist on the firewall, a series of firewall rules need to be modified upon device address changes, posing potential security risks. In addition, the customer requests that domain names be used to access the servers.

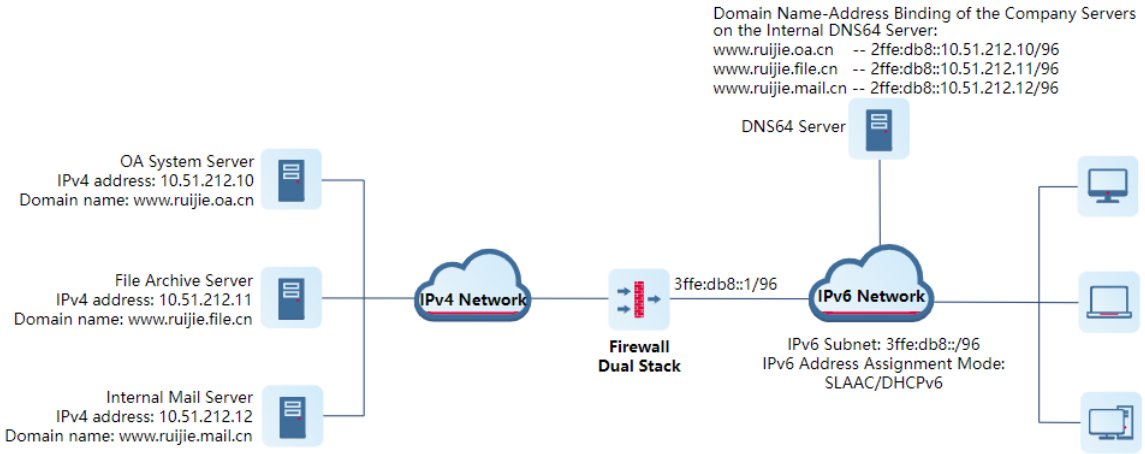


Table 8-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
NAT64 prefix information	2ffe:db8::/96, IPv6 address public prefix information that all IPv4 servers register with the DNS64 server
IPv6 subnet	3ffe:db8::/96
IPv6 address object 1	3ffe:db8::/96
IPv6 address object 2	2ffe:db8::/96
IPv4 address object 1	10.51.212.10-10.51.212.12
IPv4 address pool	172.16.10.100-172.16.10.139
Port range	11001-12000
Source NAT mode	PAT, that is, reusing IP addresses
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

8.3 Restrictions and Guidelines

- Dynamic NAT64 does not support NAT hairpinning.
- If a NAT64 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- If the address pool object referenced by the source NAT address pool is referenced by a NAT64 rule and the specified NAT mode is NO-PAT, the address pool object cannot be referenced by other NAT64 rules with a NAT mode of PAT.

8.4 Prerequisites

(1) Destination addresses are reachable from both the IPv4 and IPv6 networks.

(2) IPv6 hosts can access the DNS64 server without passing through the firewall. (In the preceding network diagram, the DNS64 server is deployed on the right of the firewall.)

(3) You have correctly configured domain name-address binding information for the IPv4 servers on the DNS64 server.

8.5 Procedure

8.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

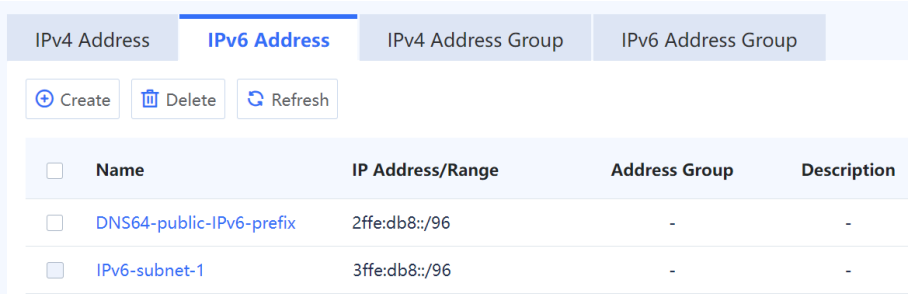
(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

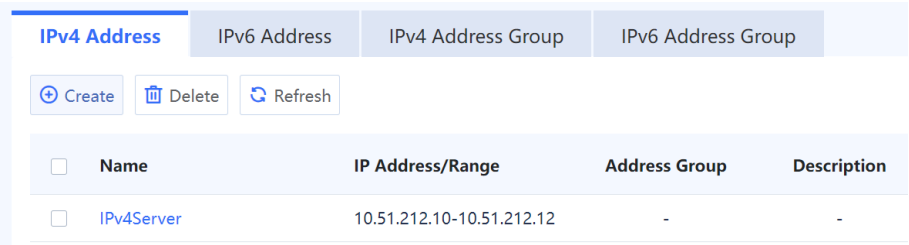
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

8.5.2 Configuring a Dynamic NAT64 Rule

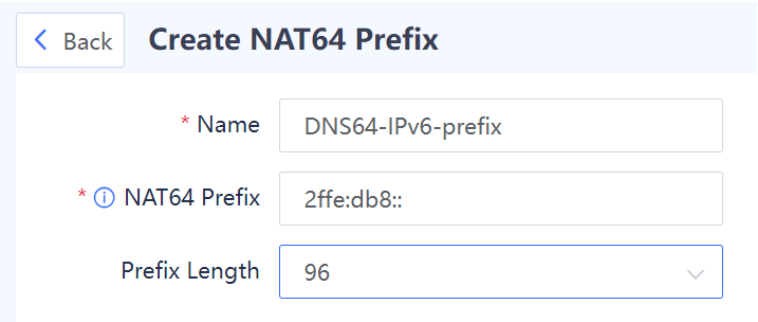
(1) Choose **Object** > **Address** > **IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.



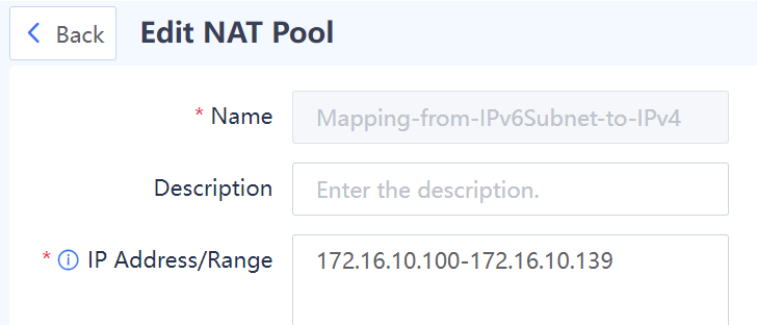
(2) Click the **IPv4 Address** tab. On the tab page that is displayed, click **Create** and create an IPv4 address object according to the following figure.



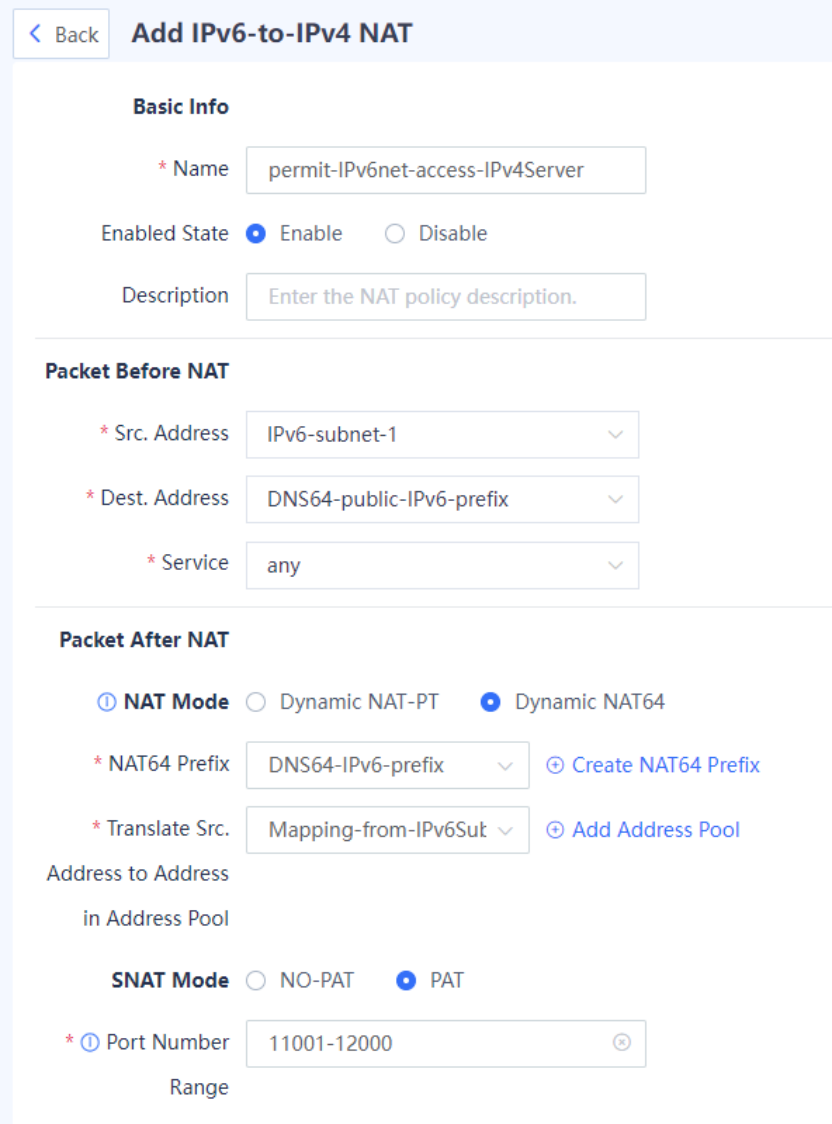
(3) Choose **Policy** > **NAT Policy** > **NAT64 Prefix**. On the page that is displayed, click **Create** and configure NAT64 prefix information according to the following figure.



(4) Choose **Address Pool** from the navigation pane. On the page that is displayed, click **Create** and configure a NAT pool for the IPv6 subnet.



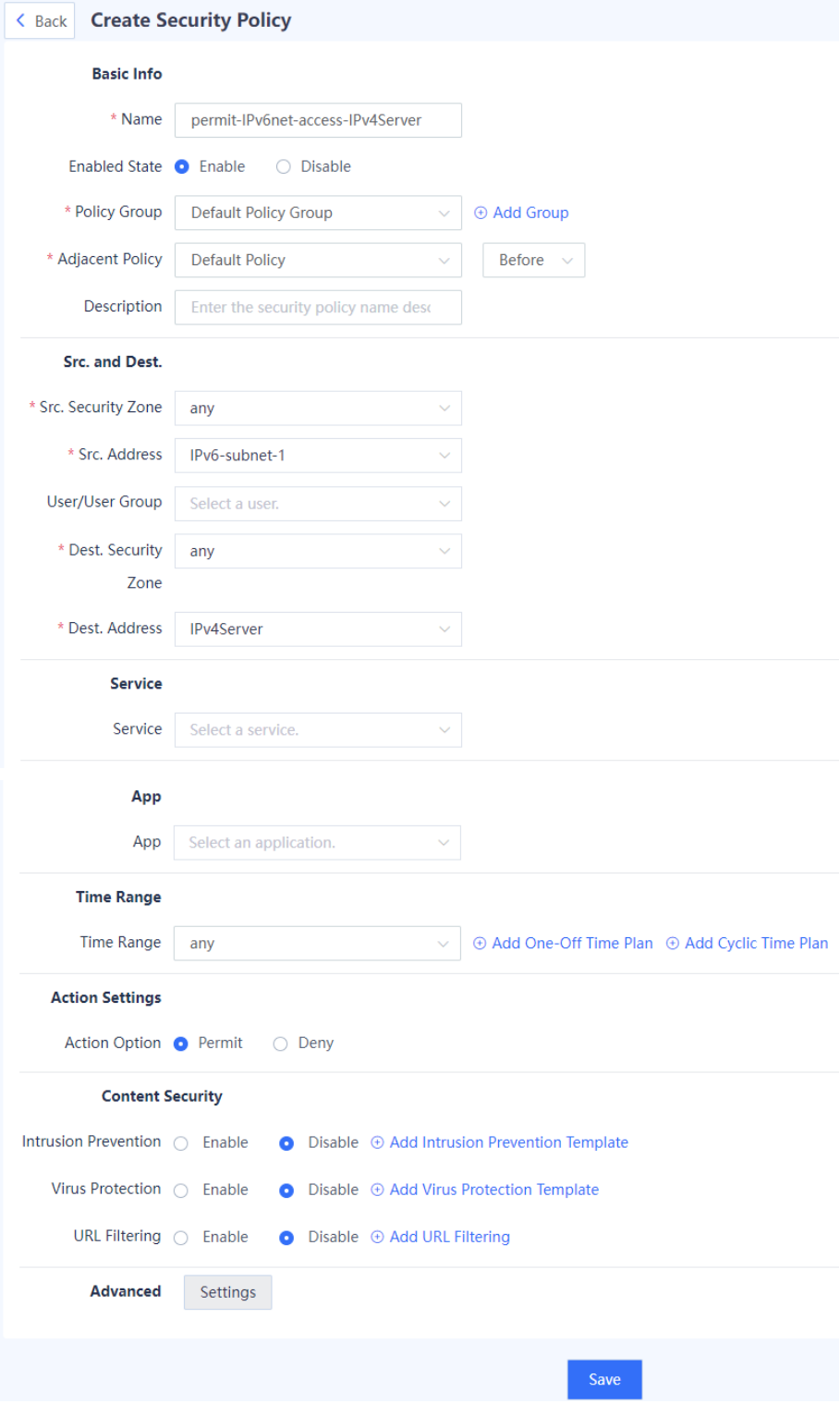
(5) Choose **NAT64** from the navigation pane. On the page that is displayed, click **Create** and configure a dynamic NAT64 rule according to the following figure. Configuration items with the asterisk (*) are mandatory.



(6) After verifying the configuration, click **Save**.

8.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT64 Rule

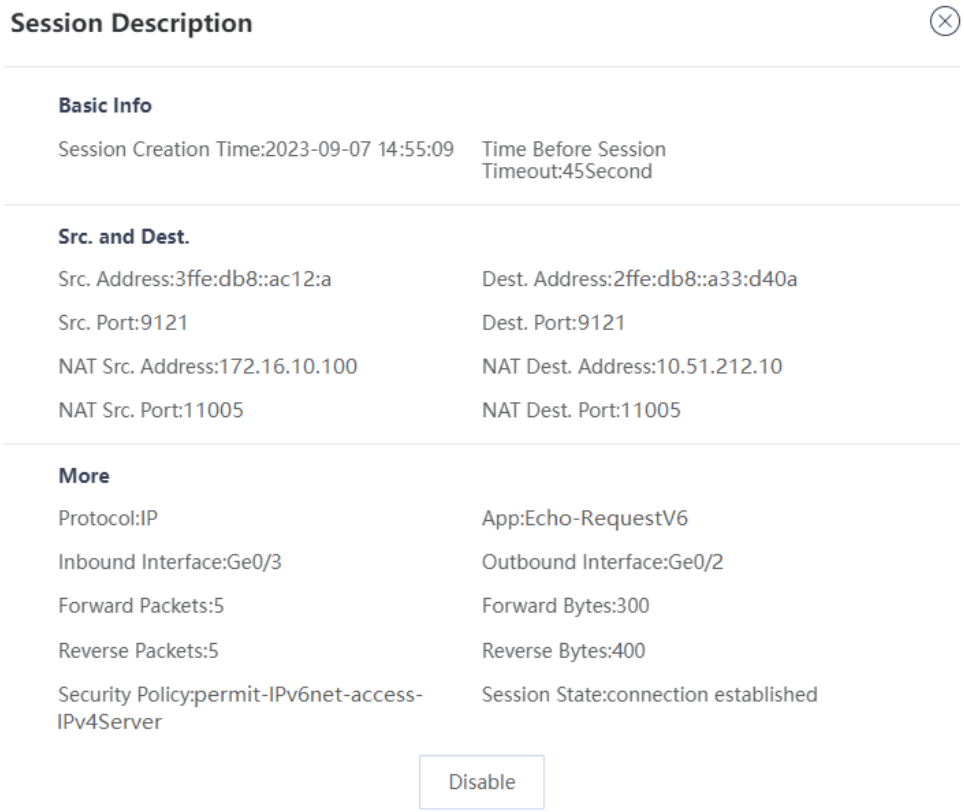
(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.



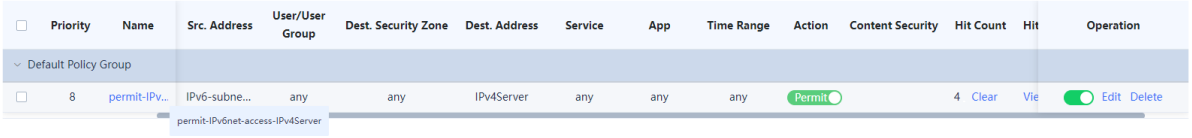
(2) After verifying the configuration, click **Save**.

8.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT64 session information.



- Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6net-access-IPv4Server** configured for the NAT64 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)



- Choose **Policy** > **NAT Policy** > **NAT64**. On the page that is displayed, check the hit count of the NAT64 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)

9 Configuration Example of NAT66-Source NPTv6 Networking

9.1 Applicable Products and Versions

Table 9-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

9.2 Service Demands

A company has deployed a firewall as a security gateway at the network boundary. A source NAT policy needs to be configured on the firewall to allow intranet users to access the Internet without exposing intranet IP addresses to extranets. In this way, network security of internal users can be enhanced.

The following figure shows the network diagram, in which the router is the access gateway provided by the ISP.

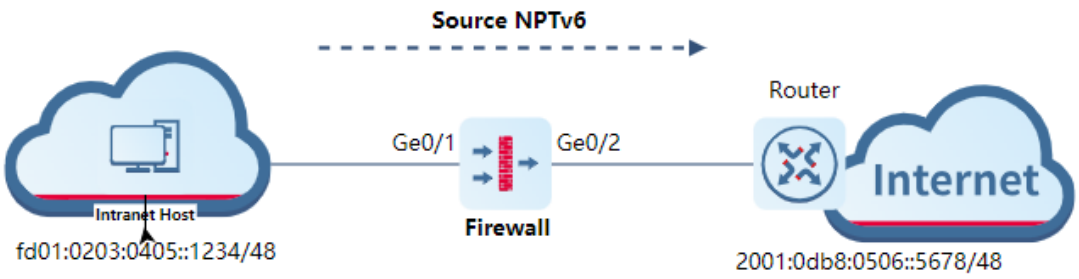


Table 9-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
IPv6 address object 1	fd01:0203:0405::/48, IPv6 prefix before source NAT
NPT information	2001:0db8:0001::/48, IPv6 prefix after source NPT

Item	Description
IPv6 address of Ge0/1	FD01:0203:0405::5678/48, trust zone
IPv6 address of Ge0/2	2001:0DB8:0506::1234/48, untrust zone
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

9.3 Restrictions and Guidelines

- The prefix lengths before and after NPT must be the same. For example, in a source NPTv6 rule, the IPv6 subnet prefix length in the matched source address object must be the same as the prefix length in the prefix information after NPT.
- If a NAT66 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- It is recommended that the IPv6 prefix information (IPv6 prefix and prefix length) after source NAT be different from the outbound interface IPv6 prefix information used by the NAT66 device for performing NAT66. For example, if the prefix after source NAT is 2001::/48, the IPv6 prefix of the outbound interface can be 2001::10/48.

9.4 Prerequisites

Destination addresses before and after destination NAT are reachable. Routing and related configurations have been completed in the early stage of network planning.

9.5 Procedure

9.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

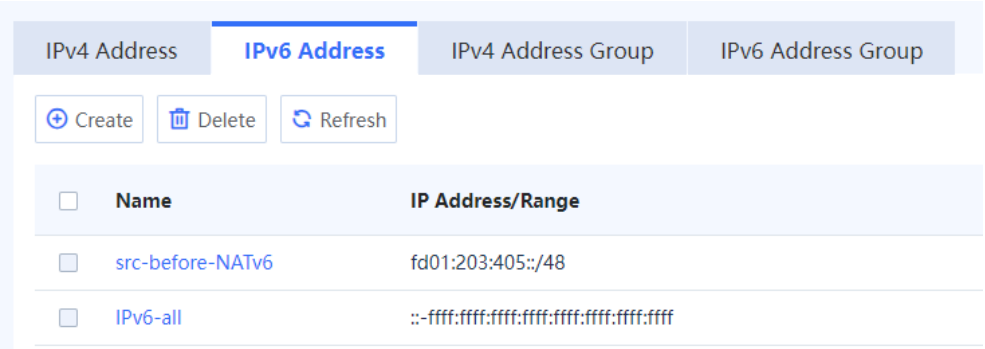
(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

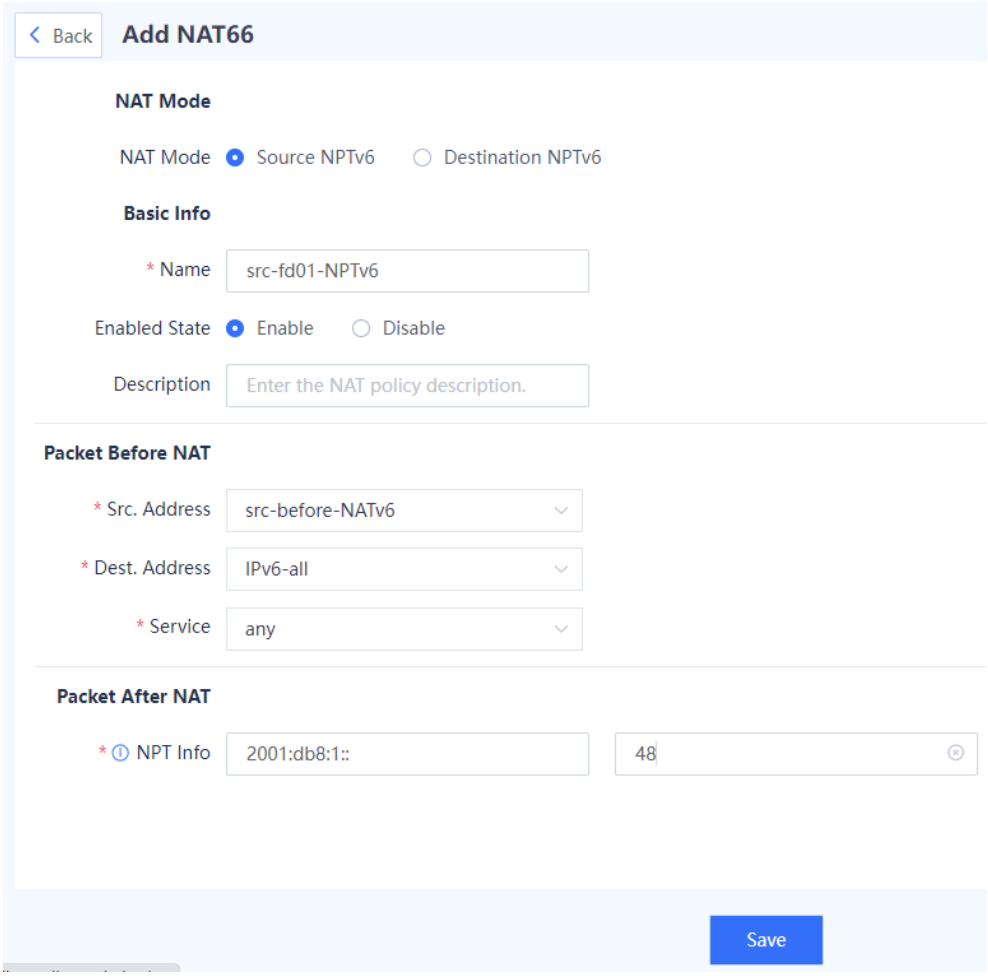
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

9.5.2 Configuring a NAT66-Source NPTv6 Rule

(1) Choose **Object** > **Address** > **IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.



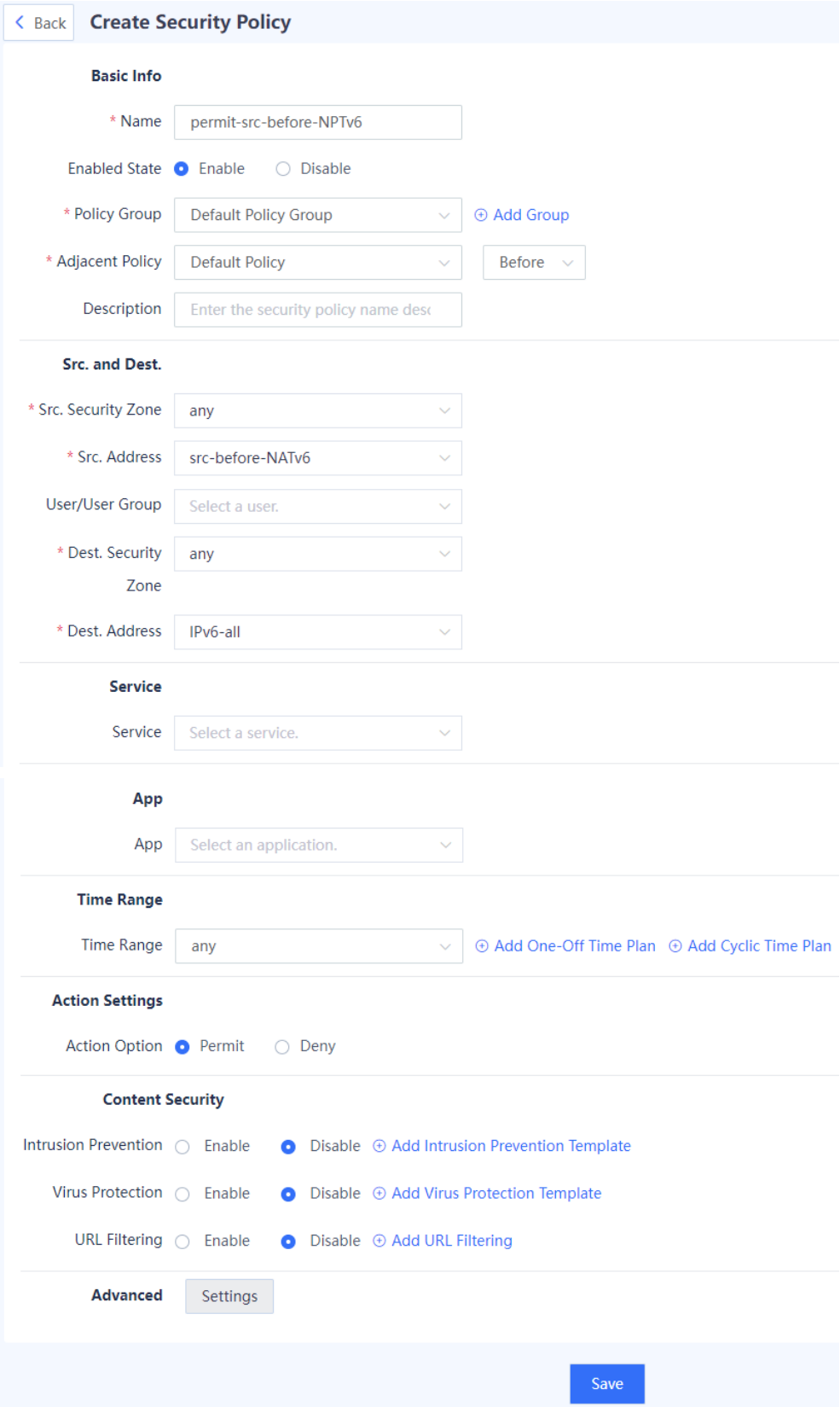
(2) Choose **Policy** > **NAT Policy** > **NAT66**. On the page that is displayed, click **Create** and configure a NAT66 rule according to the following figure. Set **NAT Mode** to **Source NPTv6**. Configuration items with the asterisk (*) are mandatory.



(3) After verifying the configuration, click **Save**.

9.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT66 Rule

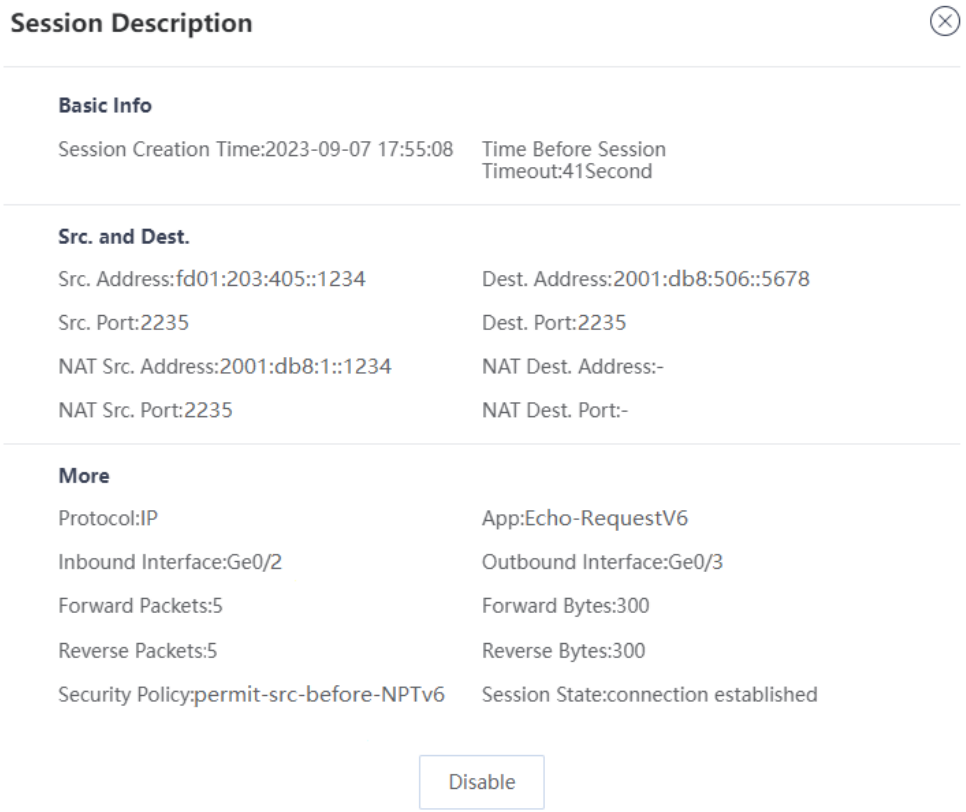
(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.



(2) After verifying the configuration, click **Save**.

9.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT66 session information.

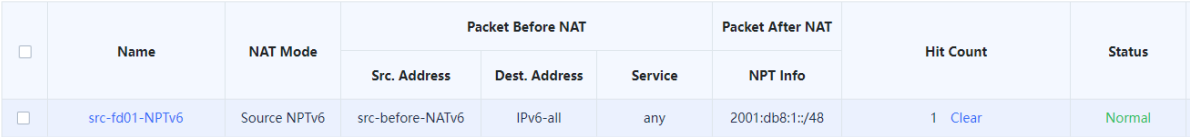


- Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-src-before-NPTv6** configured for the NAT66 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)

Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
Default Policy Group											
9	permit-src...	src-before-...	any	any	IPv6-all	any	any	any	Permit		1 Clear

permit-src-before-NPTv6

- Choose **Policy** > **NAT Policy** > **NAT66**. On the page that is displayed, check the hit count of the NAT66 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)



Name	NAT Mode	Packet Before NAT			Packet After NAT	Hit Count	Status
		Src. Address	Dest. Address	Service	NPT Info		
src-fd01-NPTv6	Source NPTv6	src-before-NATv6	IPv6-all	any	2001:db8:1::/48	1 Clear	Normal

10 Configuration Example of NAT66-Destination NPTv6 Networking

10.1 Applicable Products and Versions

Table 10-1 **Products and Versions**

Device Type	Device Model	Version
Firewall	RG-WALL 1600-Z-S series cloud-managed firewall	V5.2-NGFW_NTOS 1.0R5 or later

10.2 Service Demands

A company has deployed a firewall as a security gateway at the network boundary. To enable the intranet web server to provide services to extranets, a destination NAT policy needs to be configured on the firewall to provide the IP address of the web server for public network users to access. The following figure shows the network diagram, in which the router is the access gateway provided by the ISP.

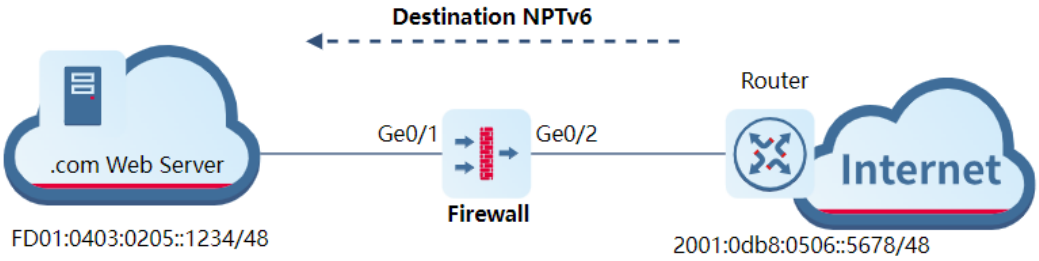


Table 10-2 **Key Configuration Points in the Network Diagram**

Item	Description
Firewall management port	Ge0/0, for accessing the firewall web UI and performing configurations
IP address of the firewall management port	192.168.1.200
IPv6 address object 1	2001:0DB8:0102::/48, IPv6 prefix before source NAT
NPT information	FD01:0403:0205::/48, IPv6 prefix after destination NPT
IPv6 address of Ge0/1	FD01:0403:0205::5678/48, trust zone

Item	Description
IPv6 address of Ge0/2	2001:0DB8:0506::1234/48, untrust zone
Any IPv6 address	::-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

10.3 Restrictions and Guidelines

- The prefix lengths before and after NPT must be the same. For example, in a source NPTv6 rule, the IPv6 subnet prefix length in the matched source address object must be the same as the prefix length in the prefix information after NPT.
- If a NAT66 rule needs to match any IPv6 address, you need to configure an any IPv6 address object. The default any object cannot be used, because it covers both any IPv4 address and any IPv6 address.
- The destination address after destination NPT must be the address of a physical device interface on the network.

10.4 Prerequisites

Destination addresses before and after destination NAT are reachable. Routing and related configurations have been completed in the early stage of network planning.

10.5 Procedure

10.5.1 Configuring Interface IP Addresses and Adding Interfaces to Security Zones

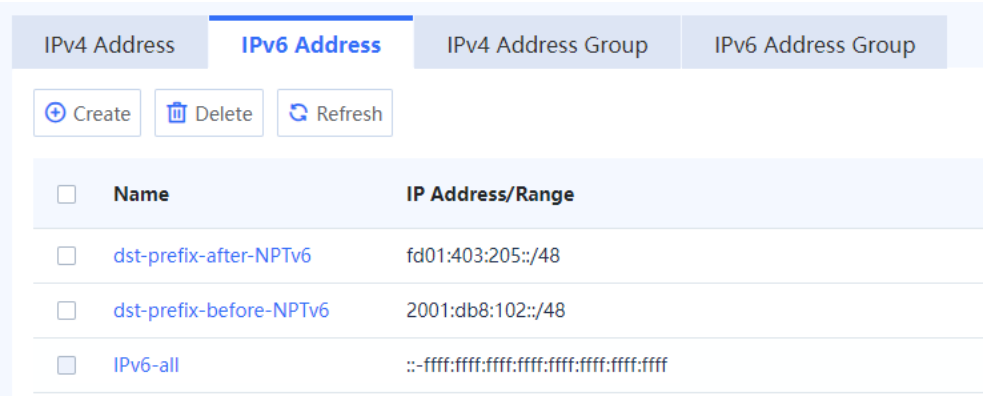
(1) Access the IP address of the firewall management port https://192.168.1.200 and log in to the firewall web UI.

(2) Choose **Network** > **Interface** > **Physical Interface**.

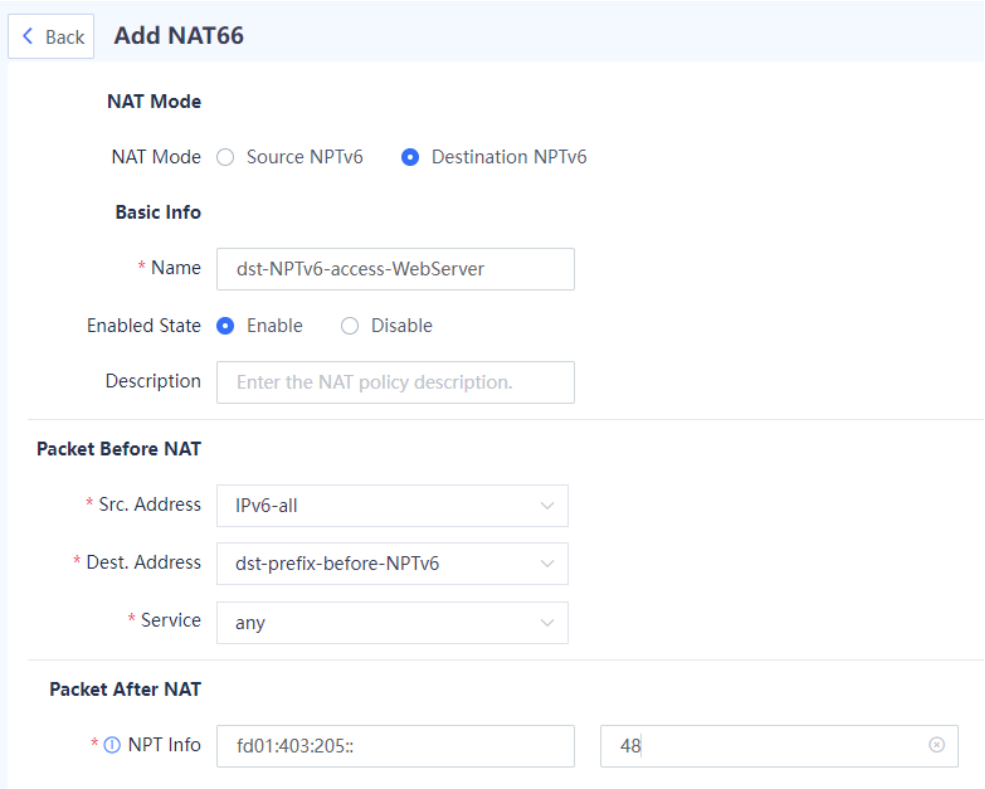
Click **Edit** in the **Operation** column of an interface. On the page that is displayed, configure an IP address and add the interface to a security zone.

10.5.2 Configuring a NAT66-Destination NPTv6 Rule

(1) Choose **Object** > **Address** > **IPv6 Address**. On the tab page that is displayed, click **Create** and create IPv6 address objects according to the following figure.



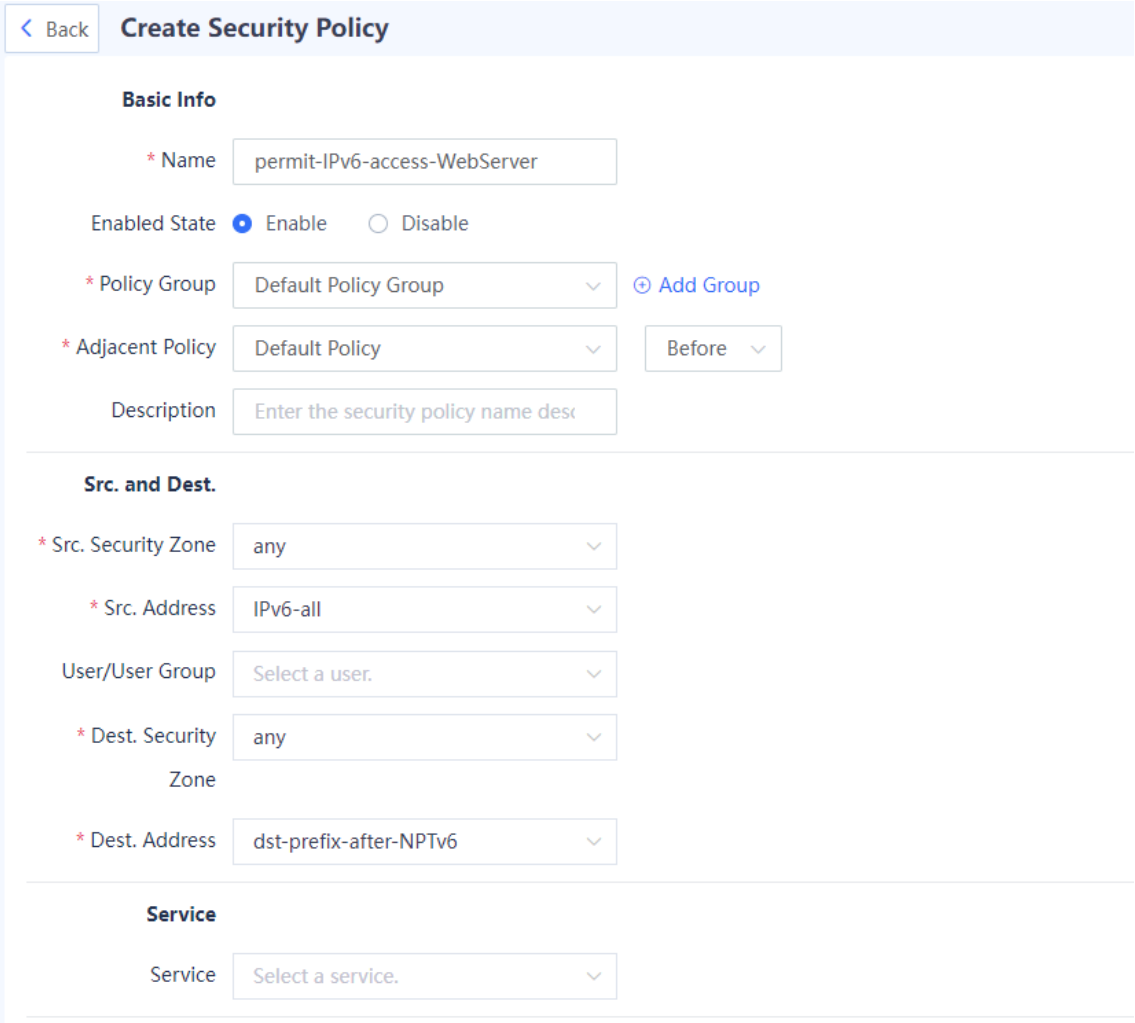
(2) Choose **Policy** > **NAT Policy** > **NAT66**. On the page that is displayed, click **Create** and configure a NAT66 rule according to the following figure. Set **NAT Mode** to **Destination NPTv6**. Configuration items with the asterisk (*) are mandatory.

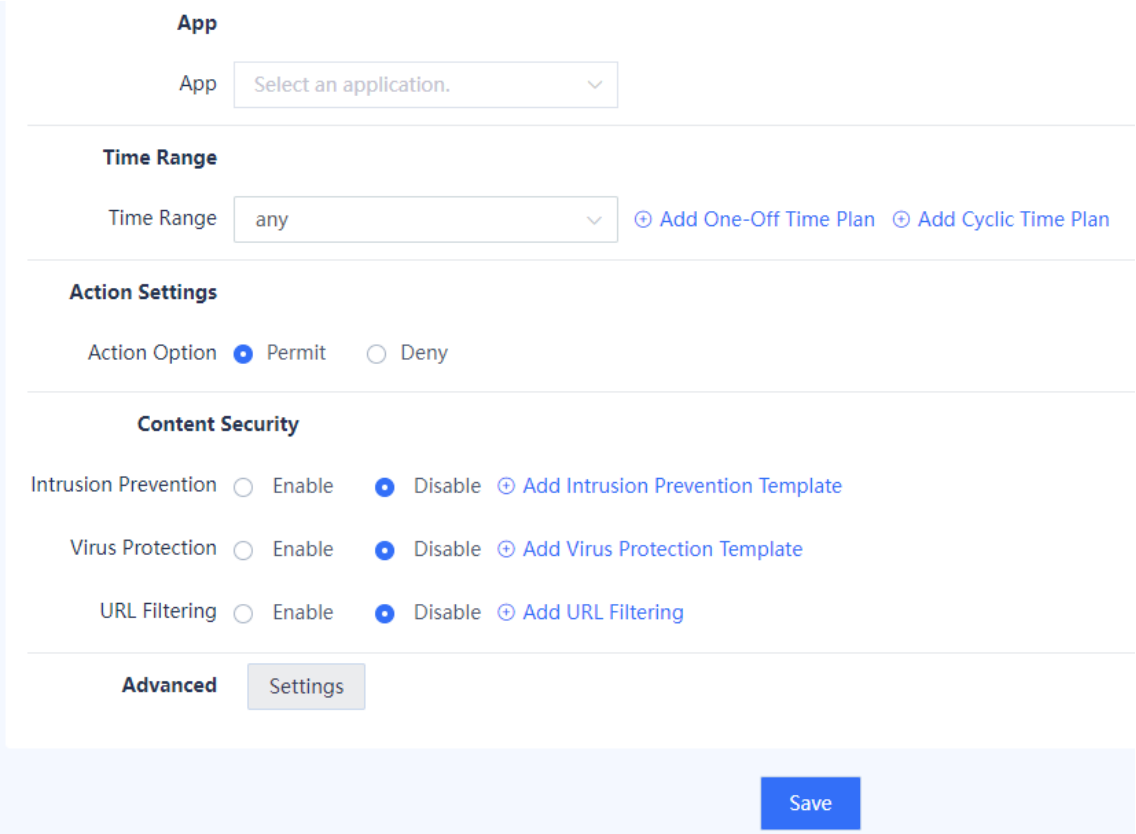


(3) After verifying the configuration, click **Save**.

10.5.3 Configuring a Security Policy to Permit Traffic That Matches the NAT66 Rule

(1) Choose **Policy** > **Security Policy** > **Security Policy**. On the page that is displayed, click **Create**. Configure a security policy according to the following figure. Configuration items with the asterisk (*) are mandatory.

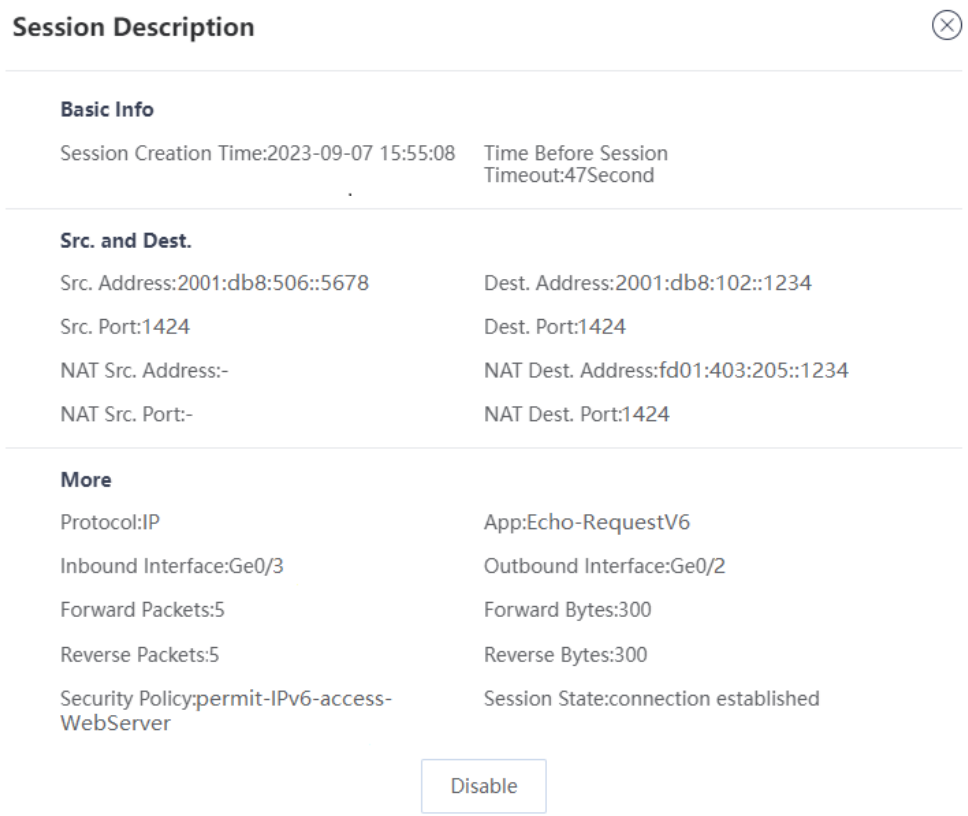

Back
Create Security Policy
Basic Info
* Name
permit-IPv6-access-WebServer
Enabled State
Enable
Disable
* Policy Group
Default Policy Group
Add Group
* Adjacent Policy
Default Policy
Before
Description
Enter the security policy name des
Src. and Dest.
* Src. Security Zone
any
* Src. Address
IPv6-all
User/User Group
Select a user.
* Dest. Security Zone
any
* Dest. Address
dst-prefix-after-NPTv6
Service
Service
Select a service.



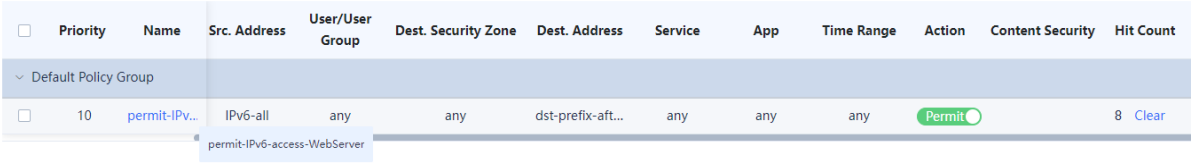
(2) After verifying the configuration, click **Save**.

10.6 Verification

- Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Session Statistics**. On the page that is displayed, locate the real-time session, and click **View Details** in the **Operation** column to view NAT66 session information.

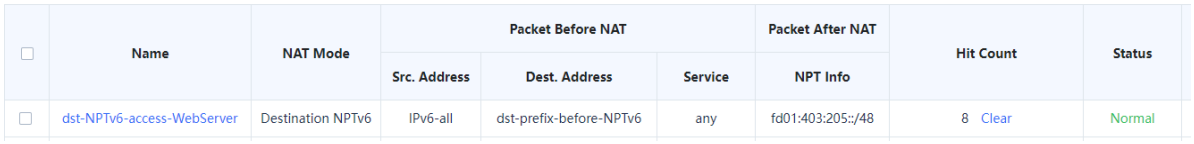


- Choose **Policy** > **Security Policy > Security Policy**. On the page that is displayed, check the hit count of the security policy **permit-IPv6-access-WebServer** configured for the NAT66 rule. (The policy hit count is incremented only for the first packet of a connection that matches a policy.)



Priority	Name	Src. Address	User/User Group	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count
Default Policy Group											
10	permit-IPv...	IPv6-all	any	any	dst-prefix-aft...	any	any	any	Permit		8 Clear
		permit-IPv6-access-WebServer									

- Choose **Policy** > **NAT Policy** > **NAT66**. On the page that is displayed, check the hit count of the NAT66 rule. (The rule hit count is incremented only for the first packet of a connection that matches a rule.)



Name	NAT Mode	Packet Before NAT			Packet After NAT	Hit Count	Status
		Src. Address	Dest. Address	Service	NPT Info		
dst-NPTv6-access-WebServer	Destination NPTv6	IPv6-all	dst-prefix-before-NPTv6	any	fd01:403:205::/48	8 Clear	Normal