

RG-WALL 1600 Next-Generation Firewall Function Configuration

Applicable to V5.2-R5.0

Contents

- **Preface**
- NAT
- Alternative-Line Load Balancing
- IPsec VPN Function Configuration

Preface

Audience

Ruijie business partners and customers who are responsible for configuring and maintaining Ruijie wireless devices.

Revision Record

Release Date	Change Contents	Reviser
2016.06	Initial publication V1.0	TAC Oversea

Note :

For more detail configuration , see configuration guide for each product . you can download configuration guide at <http://www.ruijienetworks.com>

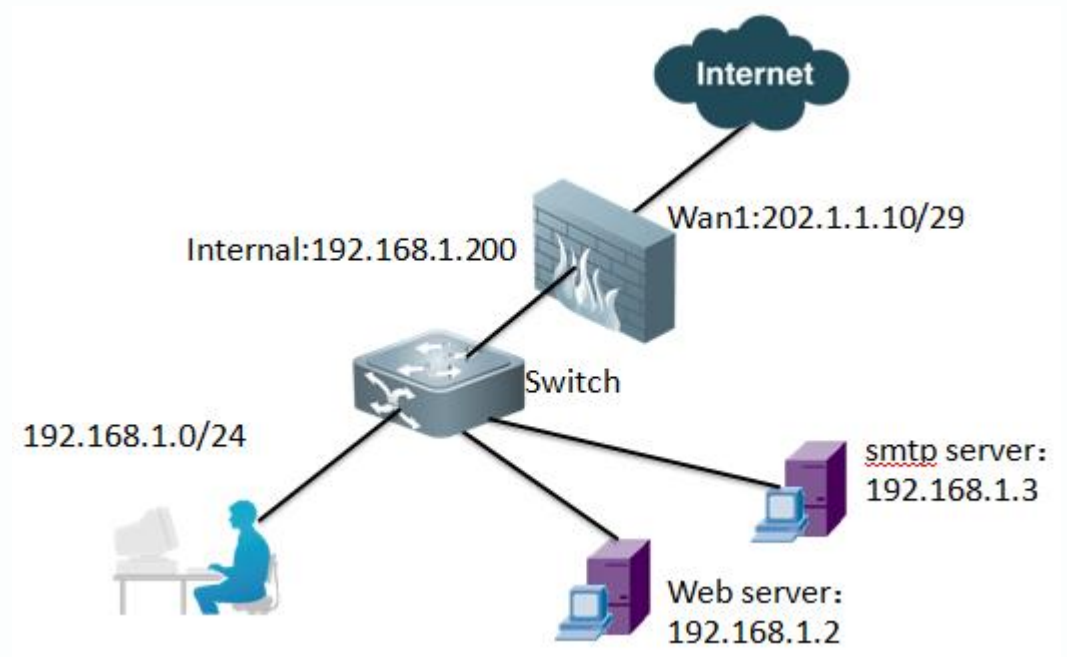
For more technical enquiry , you can visit Ruijie Service portal at <http://case.ruijienetworks.com> . You need to sign up before submit a case.

Contents

- Preface
- **NAT**
- Alternative-Line Load Balancing
- IPsec VPN Function Configuration

| NAT

Topology:



Background:

An enterprise is connected to the Internet through a line of Internet. Two public IP addresses exist. Employees need to access the Internet.

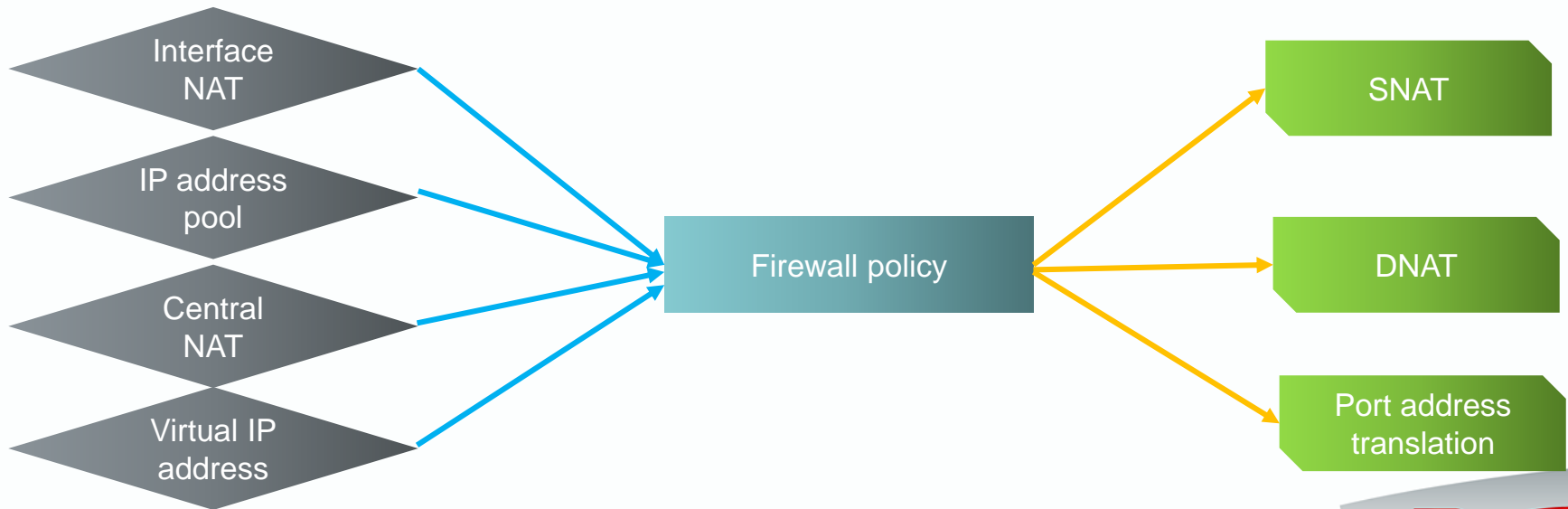
The Web server and SMTP server of the enterprise need to provide Internet access.

1. The IP addresses within the internal network segment 192.168.1.0/24 need to be converted into the IP address of the Wan1 interface before access to the Internet.
2. Port 80 with the IP address 192.168.1.2 on the Web server is mapped to Port 80 with the IP address 202.1.1.11.
3. Port 25 with the IP address 192.168.1.3 on the SMTP server is mapped to Port 25 with the IP address 202.1.1.11.

NAT Configuration

Principle:

Network address translation (NAT) is classified into source network address translation (SNAT), destination network address translation (DNAT), and port address translation. NAT and access control are implemented based on the same policy. A NAT policy does not need to be configured separately. In SNAT, an address is converted into the IP address of the outbound interface or an IP address in the address pool. In central NAT, IP addresses or source port addresses are converted in one-to-one mode. In DNAT, virtual IP addresses are used to realize one-to-one address mapping or many-to-many IP address mapping with equal quantities, including many-to-many port mapping.



NAT Configuration



Configure the IP addresses of interfaces. For details, see the courseware on installation and initialization.

Configure the IP addresses of the internal interface and Wan1 interface. See the figure below:

The figure displays two screenshots of the Ruijie network management interface, specifically the 'Edit Interface' configuration page. Both screenshots show a sidebar menu on the left with 'Interface' selected under the 'Network' section.

Top Screenshot (Interface: internal):

- Name: internal
- Alias: [Empty text box]
- Link Status: up (with green up arrow icon)
- Type: Physical Interface
- Addressing mode: Manual DHCP PPPoE
- IP/Netmask: 192.168.1.200/255.255.255.0 (highlighted with a red box)
- Administrative Access: HTTPS PING HTTP SSH SNMP TELNET

Bottom Screenshot (Interface: wan1):

- Name: wan1
- Alias: [Empty text box]
- Link Status: up (with green up arrow icon)
- Type: Physical Interface
- Addressing mode: Manual DHCP PPPoE
- IP/Netmask: 202.1.1.10/30
- Administrative Access: HTTPS PING HTTP SSH SNMP TELNET

NAT Configuration



Configure a route. For details, see the courseware on installation and initialization.

Configure the default route to the Internet. See the figure below:

Edit Static Route

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan1"/>
Gateway	<input type="text" value="202.1.1.9"/>
Distance	<input type="text" value="10"/> (1-255)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="To Office Room"/>

NAT Configuration



Configure virtual IP addresses used for DNAT.

The figure below shows how to configure the mapping between destination addresses and virtual IP addresses:

The screenshot shows the 'Add New Virtual IP Mapping' configuration window. The left sidebar contains a navigation menu with 'Virtual IP' selected. The main area displays two configuration examples:

- Example 1 (highlighted with a green box):**
 - External IP Address/Range: 202.1.1.11 - 202.1.1.15
 - Mapped IP Address/Range: 192.168.1.2 - 192.168.1.6
 - Port Forwarding:
 - Protocol: TCP UDP SCTP
 - External Service Port: 80 - 90
 - Map to Port: 80 - 90
- Example 2 (highlighted with a red box):**
 - Port Forwarding:
 - Protocol: TCP UDP SCTP
 - External Service Port: 25 - 25
 - Map to Port: 25 - 25

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

NAT Configuration



Configure the firewall policy whereby virtual IP address mapping (DNAT) is used to enable the Web server and SMTP server to provide services externally. See the figure below:

System

- Router
- Firewall**
- Policy
 - Policy**
 - Central NAT Table
 - DoS Policy
 - Protocol Options
 - SSL/SSH Inspection
 - NAT64 Policy
- + Address
- + Service
- + Schedule
- + Traffic Shaper

New Policy

Source Interface/Zone	wan1	
Source address	all	Multiple
Destination Interface/Zone	internal	
Destination address	smtpserver:25	Multiple
Schedule	always	
Service	HTTP	Multiple
Action	ACCEPT	

Log Allowed Traffic

NAT

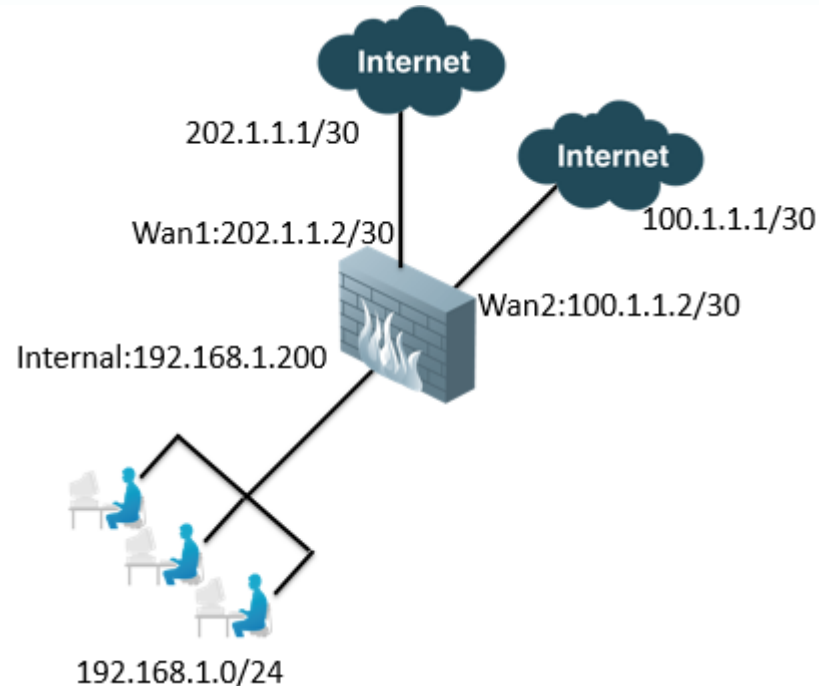
- No NAT
- Enable NAT
- Use Central NAT Table
- Dynamic IP Pool

Contents

- Preface
- NAT
- **Alternative-Line Load Balancing**
- IPsec VPN Function Configuration

Alternative-Line Load Balancing

Topology:



Background:

The egress of an enterprise network is deployed with two Internet lines, at 10 Mbps (Wan1) and 20 Mbps (Wan2) respectively. Users on the intranet need to access the Internet through the two lines in load balancing mode. That is, the line with higher bandwidth must carry more traffic, thereby increasing bandwidth utilization.

Alternative-Line Load Balancing

Principle:

When users on the intranet access the Internet, load may be unevenly distributed to external lines, which affects bandwidth utilization. To address this problem, you can configure the weight of each line based on the bandwidth ratio. The higher the bandwidth, the larger the weight, and the line must carry more traffic. This achieves load balancing between two lines. There is no strict requirement on weight configuration, as long as the weight is proportional to bandwidth.

Configuration procedure:

1. Add two default equal-cost routes.
2. Configure the weights of the routes which work in load balancing mode.
3. Add the SNAT firewall policy for the two routes.

NOTE:

Before you perform the preceding configuration, configure the IP addresses of interfaces by using the fast configuration feature.

Alternative-Line Load Balancing

Route configuration

Load balancing policy

Firewall policy

Route configuration: Configure two default equal-cost routes.

The screenshot shows the 'New Static Route' configuration window. The left sidebar is expanded to 'Router' > 'Static' > 'Static Route'. The main form contains the following fields:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan1
Gateway	202.1.1.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Buttons: OK, Cancel

The screenshot shows the 'New Static Route' configuration window for a second route. The left sidebar is expanded to 'Router' > 'Static' > 'Static Route'. The main form contains the following fields:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan2
Gateway	100.1.1.1
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Buttons: OK, Cancel

Alternative-Line Load Balancing

Route configuration

Load balancing policy

Firewall policy

Load balancing policy:

Configure a load balancing policy. Because the bandwidth ratio of the Wan1 line (10 Mbps) to the Wan2 line (20 Mbps) is 1:2, their weight ratio is also 1:2.

Therefore, set the weight of the Wan1 line to 10 and that of the Wan2 line to 20.

The screenshot shows the configuration interface for ECMP Load Balancing Method. The 'Weighted Load Balance' option is selected. A table lists interfaces and their weights:

Interface	Weight
lan	0
mesh.root	0
mgmt	0
modem	0
ssl.root	0
wan1	10
wan2	20

Alternative-Line Load Balancing

Route configuration

Load balancing policy

Firewall policy

Firewall policy:

Add two firewall policies for Internet access, which are used to convert source addresses into the IP addresses of the Wan1 and Wan2 outbound interfaces.

The screenshot displays the 'New Policy' configuration page in the Ruijie Network management interface. The left sidebar shows the navigation menu with 'Policy' selected. The main configuration area includes the following fields:

- Source Interface/Zone: internal
- Source address: all
- Destination Interface/Zone: wan2
- Destination address: all
- Schedule: always

Below these fields, a table lists the configured policies:

Policy Name	Source Interface/Zone	Source Address	Destination Interface/Zone	Destination Address	Schedule	Enable NAT	Dynamic IP Pool	Accept	Check
internal->wan2 (1)	internal	all	wan2	all	always	ALL		accept	<input checked="" type="checkbox"/>
internal->wan1 (1)	internal	all	wan1	all	always	ALL		accept	<input checked="" type="checkbox"/>

Additional configuration options include:

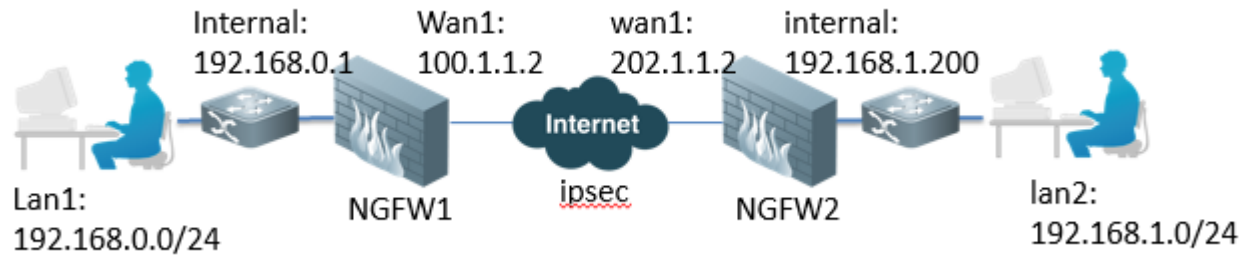
- Enable NAT
- Use Central NAT Table
- Dynamic IP Pool
- Session TTL: 0 (0 or 300-604800)
- Enable Identity Based Policy

Contents

- Preface
- NAT
- Alternative-Line Load Balancing
- IPsec VPN Function Configuration

IPsec VPN Function Configuration

Topology:



Background:

The headquarters of an enterprise and its branch office are located in different provinces, and they establish two intranets respectively. The two intranets need to be directly connected through IPsec VPN to form a VPN, where data is encrypted using the IPsec VPN encryption algorithm to ensure transmission security.

IPsec VPN Function Configuration

Principle:

IPsec is used to protect the security of sensitive data transmitted over the Internet. IP packets are encrypted and authenticated using IPsec at the network layer. IPsec provides the following network security services. Which service(s) to use is determined by the local security policy.

1. Data confidentiality: The IPsec sender encrypts the data to be sent.
2. The IPsec recipient verifies the received data to ensure that the data is not modified during transmission.
3. Data source verification: The IPsec recipient verifies the source of the received data.
4. Anti-rebroadcast: The IPsec recipient can detect that rebroadcast IP packets are discarded.

IPsec VPN can work in the following modes:

Interface mode (routing mode): Traffic is routed to the virtual IPsec interface.

Policy mode (tunnel mode): Only one firewall policy needs to be created for a bidirectional link. The firewall policy must be configured with IPsec VPN support.

| IPsec VPN Function Configuration

Configuration procedure:

The following procedure configures NGFW1 in interface mode. The configuration of NGFW2 is the same.

1. Perform the basic configuration of Internet access.
2. Perform IKE phase I configuration.
3. Perform IKE phase II configuration.
4. Configure a VPN route.
5. Configure firewall policies.

IPsec VPN Function Configuration - NGFW1



Basic configuration of Internet access

For details, see the courseware on installation and initialization.

Interface configuration:

Name	Type	IP/Netmask	Access	Administrative Status
dmz1	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,CAPWAP	🟢
dmz2	Physical Interface	0.0.0.0/0.0.0.0	PING	🟢
lan	Hardware Switch	192.168.0.1/255.255.255.0	PING,HTTPS	🟢
mgmt	Physical Interface	192.168.1.200/255.255.255.0	PING,HTTPS	🟢
wan1	Physical Interface	100.1.1.2/255.255.255.252	PING,HTTPS,TELNET	🟢
wan2	Physical Interface	172.29.1.1/255.255.255.252	PING,HTTPS,TELNET	🟢

Route configuration:

IP/Mask	Gateway	Device
172.29.0.0 255.255.0.0	172.29.1.2	wan2
0.0.0.0 0.0.0.0	100.1.1.1	wan1

IPsec VPN Function Configuration

Basic configuration of Internet access

IPsec VPN configuration

VPN route configuration

Policy configuration

IPsec VPN configuration: Perform IKE phase I configuration.

The screenshot displays the 'New Phase 1' configuration page in a web interface. The left sidebar shows a navigation menu with 'VPN' selected, and 'Auto Key (IKE)' highlighted. The main configuration area includes the following fields and options:

- Name:** vpn
- Comments:** (empty)
- Remote Gateway:** Static IP Address
- IP Address:** 202.1.1.2
- Local Interface:** wan1
- Mode:** Aggressive (selected), Main (ID protection)
- Authentication Method:** Preshared Key
- Pre-shared Key:** (masked with dots)
- Peer Options:** Accept any peer ID (selected)
- Enable IPsec Interface Mode:** (checked)
- IKE Version:** 1 (selected), 2
- Mode Config:** (unchecked)
- Local Gateway IP:** Main Interface IP (selected), Specify 0.0.0.0
- P1 Proposal:**
 - 1 - Encryption: 3DES
 - 2 - Encryption: AES128
 - Authentication: SHA1
- DH Group:** 1, 2, 5 (checked), 14
- Keylife:** 28800 (120-172800 seconds)
- Local ID:** (optional)
- XAUTH:** Disable (selected), Enable as Client, Enable as Server

IPsec VPN Function Configuration



IPsec VPN configuration: Perform IKE phase II configuration.

System Router Firewall UTM VPN IPsec Auto Key (IKE) Concentrator SSL monitor

New Phase 2

Name: vpn
Comments:
Phase 1: vpn

Advanced...

P2 Proposal

1-	Encryption: 3DES	Authentication: SHA1
2-	Encryption: AES128	Authentication: SHA1

Enable replay detection
 Enable perfect forward secrecy(PFS).
DH Group 1 2 5 14

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)
Autokey Keep Alive Enable
Auto_negotiate Enable

IPsec VPN Function Configuration



VPN route configuration:

Add a route to the destination private network segment. Select the VPN established at IKE phase I for the interface option.

The screenshot shows the 'New Static Route' configuration interface. The left sidebar contains a navigation menu with 'Router' selected, and 'Static Route' highlighted. The main configuration area includes the following fields:

- Destination IP/Mask: 192.168.1.0/24
- Device: vpn
- Gateway: 0.0.0.0
- Distance: 10 (1-255)
- Priority: 0 (0-4294967295)
- Comments: (empty text box)

At the bottom right, there are 'OK' and 'Cancel' buttons.

IPsec VPN Function Configuration



Firewall policy configuration:

Configure a firewall policy used to allow the local end to access the peer end.
Select the VPN interface as the destination interface.

Configure a firewall policy used to allow the peer end to access the local end.
Select the VPN interface as the source interface.

System Router **Firewall** Policy

- Policy
- Central NAT Table
- DoS Policy
- Protocol Options
- SSL/SSH Inspection
- NAT64 Policy

+ Address
+ Service
+ Schedule
+ Traffic Shaper
+ Virtual IP
+ Load Balance

Source Interface/Zone: VPN
Source address: 192.168.1.0/24
Destination Interface/Zone: internal
Destination address: 192.168.0.0/24
Schedule: always
Service: ALL
Action: ACCEPT

Log Allowed Traffic

NAT

- No NAT
- Enable NAT
- Use Central NAT Table
- Dynamic IP Pool

Session TTL: 0 (0 or 300-604800)

IPsec VPN Function Configuration - NGFW2



Basic configuration of Internet access

For details, see the courseware on installation and initialization.

Interface configuration:

Name	Type	IP/Netmask	Access	Administrative St
dmz1	Physical Interface	10.10.10.1/255.255.255.0	PING,HTTPS,CAPWAP	🟢
dmz2	Physical Interface	0.0.0.0/0.0.0.0	PING	🟢
lan	Hardware Switch	192.168.1.200/255.255.255.0	PING,HTTPS	🟢
mgmt	Physical Interface	192.168.110.1/255.255.255.0	PING,HTTPS	🟢
wan1	Physical Interface	202.1.1.2/255.255.255.252	PING,HTTPS,TELNET	🟢
wan2	Physical Interface	172.29.1.1/255.255.255.252	PING,HTTPS,TELNET	🟢

Route configuration:

IP/Mask	Gateway	Device
172.29.0.0 255.255.0.0	172.29.1.2	wan2
0.0.0.0 0.0.0.0	202.1.1.1	wan1

IPsec VPN Function Configuration



IPsec VPN configuration: Perform IKE phase I configuration.

The screenshot shows the configuration page for 'Edit Phase 1' in the Ruijie network device management interface. The left sidebar contains a navigation menu with 'VPN' selected, and sub-items for 'IPsec', 'Auto Key (IKE)', and 'Concentrator'. The main configuration area includes the following fields and options:

- Name:** vpn
- Comments:** (empty text area)
- Remote Gateway:** Static IP Address
- IP Address:** 100.1.1.2 (highlighted with a red box)
- Local Interface:** wan1
- Mode:** Aggressive (radio), Main (ID protection) (radio, selected)
- Authentication Method:** Preshared Key
- Pre-shared Key:** (password field with dots)
- Peer Options:** Accept any peer ID (radio, selected)
- Enable IPsec Interface Mode:** (checked)
- IKE Version:** 1 (radio, selected), 2 (radio)
- Mode Config:** (checkbox, unchecked)
- Local Gateway IP:** Main Interface IP (radio, selected), Specify 0.0.0.0 (radio, unchecked)
- P1 Proposal:**
 - 1 - Encryption: 3DES
 - 2 - Encryption: AES128
 - Authentication: SHA1
- DH Group:** 1 (checkbox, unchecked), 2 (checkbox, unchecked), 5 (checkbox, checked), 14 (checkbox, unchecked)

IPsec VPN Function Configuration



IPsec VPN configuration: Perform IKE phase II configuration.

System New Phase 2

Router

Firewall

UTM

VPN

IPsec

- Auto Key (IKE)
- Concentrator

SSL

monitor

Name: vpn2

Comments:

Phase 1: vpn

Advanced...

P2 Proposal

1-	Encryption: 3DES	Authentication: SHA1
2-	Encryption: AES128	Authentication: SHA1

Enable replay detection

Enable perfect forward secrecy(PFS).

DH Group 1 2 5 14

Keylife: SECONDS 1800 (seconds) 5120 (KBytes)

Autokey Keep Alive Enable

Auto_negotiate Enable

IPsec VPN Function Configuration



VPN route configuration:

Add a route to the destination private network segment. Select the VPN established at IKE phase I for the interface option.

The screenshot displays the 'New Static Route' configuration window. The left sidebar shows the navigation menu with 'Static Route' selected. The main configuration area includes the following fields:

Field	Value
Destination IP/Mask	192.168.0.0/24
Device	vpn
Gateway	0.0.0.0
Distance	10 (1-255)
Priority	0 (0-4294967295)
Comments	

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

IPsec VPN Function Configuration

Basic configuration of Internet access

IPsec VPN configuration

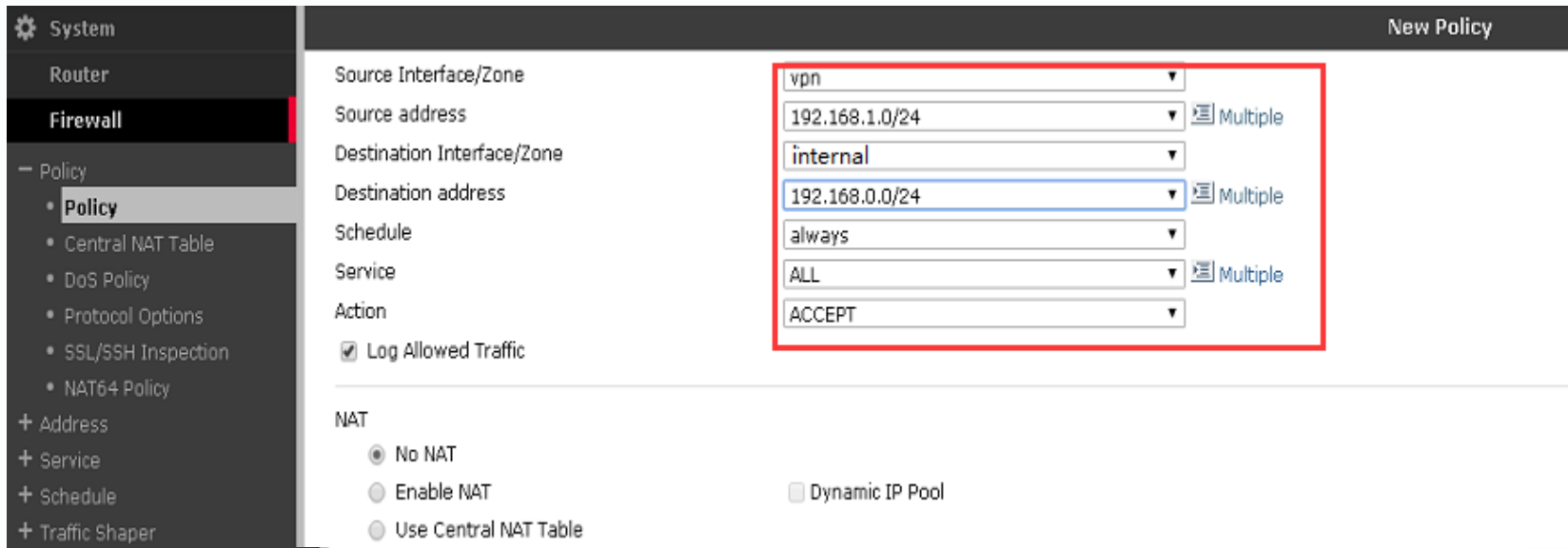
VPN route configuration

Policy configuration

Firewall policy configuration:

Configure a firewall policy used to allow the local end to access the peer end. Select the VPN interface as the destination interface.

Configure a firewall policy used to allow the peer end to access the local end. Select the VPN interface as the source interface.



The screenshot shows the 'New Policy' configuration page in the Ruijie management interface. The left sidebar contains a navigation menu with 'System', 'Router', 'Firewall', and 'Policy' sections. Under 'Policy', 'Policy' is selected, showing sub-items like 'Central NAT Table', 'DoS Policy', 'Protocol Options', 'SSL/SSH Inspection', and 'NAT64 Policy'. Below this are '+ Address', '+ Service', '+ Schedule', and '+ Traffic Shaper' options.

The main configuration area is titled 'New Policy' and contains the following fields:

- Source Interface/Zone: vpn
- Source address: 192.168.1.0/24 (Multiple)
- Destination Interface/Zone: internal
- Destination address: 192.168.0.0/24 (Multiple)
- Schedule: always
- Service: ALL (Multiple)
- Action: ACCEPT
- Log Allowed Traffic

Below these fields is the 'NAT' section with three radio button options: 'No NAT' (selected), 'Enable NAT', and 'Use Central NAT Table'. There is also an unchecked checkbox for 'Dynamic IP Pool'.