

# NAT Configure on IR900

## 1. Introduction

Network Address Translation (NAT) simplifies and conserves IP addresses. It enables private IP networks to connect to the Internet using unregistered IP addresses (in the private address space specified in RFC 1918). NAT operates on a router, usually connecting two networks together, and is used to translate the private addresses in the internal network into legal routable addresses, before packets are forwarded to another network, because ISPs will not route RFC 1918 addresses. NAT offers the dual functions of security and address conservation, and is typically implemented in remote-access environments at the edge of the network where an enterprise connects to its ISP.

## 2. Configure NAT on IR900

From navigation panel, select **Firewall>>NAT**, then enter “NAT” page, as shown below.

Firewall >> NAT

NAT

### Network Address Translation (NAT) Rules

Action	Source Network	Match Conditions	Translated Address
SNAT	Inside	ACL:100	cellular 1

Add Modify Delete

### Inside Network Interfaces

ID	Interface
1	fastethernet 0/1
2	fastethernet 0/2
3	

Add

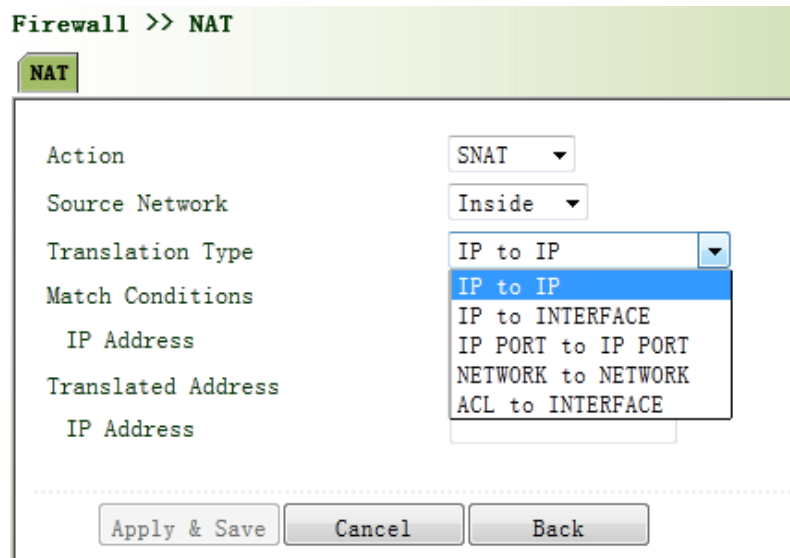
### Outside Network Interfaces

ID	Interface
1	cellular 1
2	

Add

Apply & Save Cancel

Click <Add> to add new NAT rules, as shown below.



Page description is shown below:

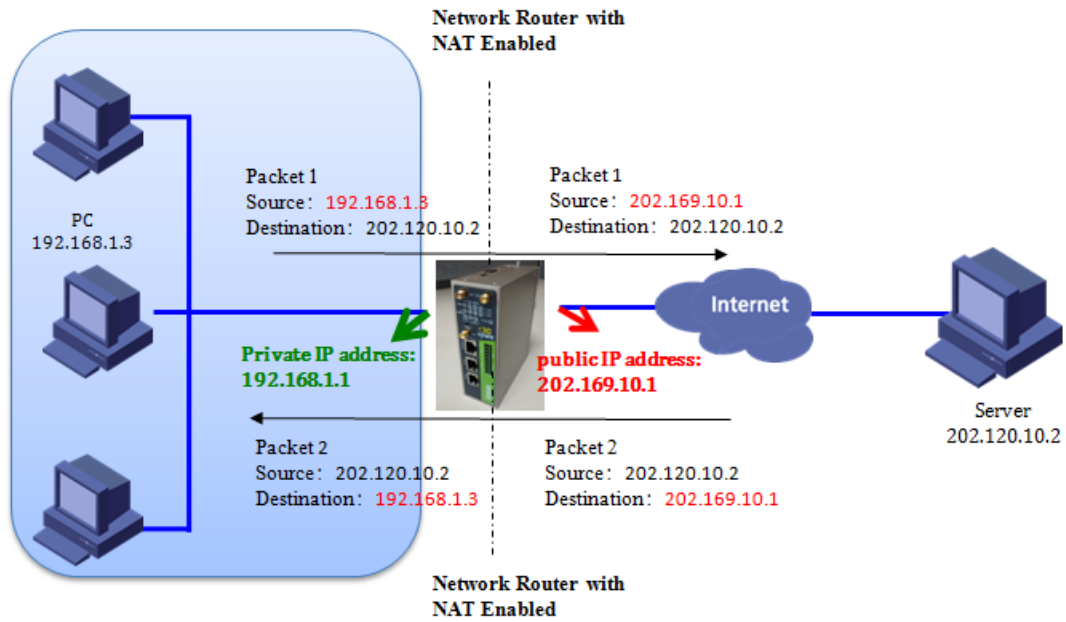
Parameters	Description	Default
Action	<p><b>SNAT:</b> Source NAT: Translate IP packet's source address into another address</p> <p><b>DNAT:</b> Destination NAT: Map a set of local internal addresses to a set of legal global addresses.</p> <p><b>1:1NAT:</b> Transfer IP address one to one.</p>	SNAT
Source Network	<p>Inside: Inside address</p> <p>Outside: Outside address</p>	Inside
Translation Type	<p>Select the Translation Type:</p> <p>IP to IP: Translate an IP address to another IP address</p> <p>IP to Interface: Translate an IP address to the IP address of one interface</p> <p>IP Port to IP Port: Translate an IP+Port group to another IP+Port group</p> <p>Network to Network: Translate network addresses to another network addresses.</p> <p>ACL to Interface: Translate the IP addresses that match the ACL to the IP address of one interface.</p>	IP to IP

### 3. Examples

Next we take two examples to explain the NAT function.

#### Application Case 1- SNAT:

SNAT allows IR900 to act as an Internet gateway for internal LAN clients by translating the clients' internal network IP Addresses into a public IP Address on IR900. Network topology as the following show. When the PCs in the LAN network (192.168.1.0/24) need to access internet, IR900 will translate their source IP address to the IP address of one interface on IR900.



### Configure on IR900:

Step 1: Configure ACL;

**ACL**

Type	standard ▼
ID	100
Action	permit ▼
Match Conditions	
Source IP	192.168.1.0
Source Wildcard	0.0.0.255
Log	<input type="checkbox"/>
Description	<input style="width: 100%;" type="text"/>

Step 2: Configure NAT;

**Firewall >> NAT**

**NAT**

Action: SNAT ▼

Source Network: Inside ▼

Translation Type: ACL to INTERFACE ▼

Match Conditions

Access Control List: 100

Translated Address

Interface: cellular 1 ▼

Apply & Save   Cancel   Back

Step 3: Define inside and outside interface;

### Inside Network Interfaces

ID	Interface
1	fastethernet 0/2
2	▼
Add	

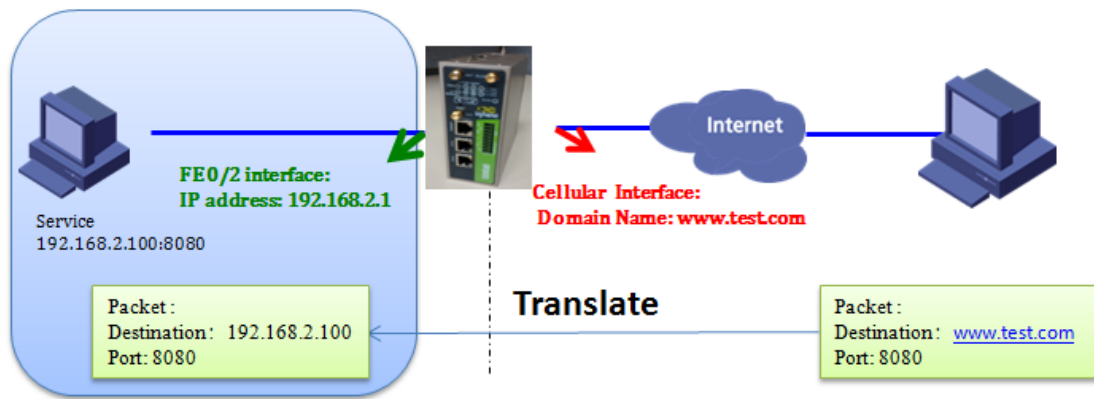
### Outside Network Interfaces

ID	Interface
1	cellular 1
2	fastethernet 0/1 ▼
Add	

### Application Case 2- DNAT(Port Mapping/Forwarding):

Port mapping/forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN).

As the following show, Any device which is capable of reaching internet can access remote service (192.168.2.100:8000) via port mapping .



**Configure on IR900:**

**Firewall >> NAT**

**NAT**

Action	DNAT ▼
Source Network	Outside ▼
Translation Type	INTERFACE PORT to IP PORT ▼
Protocol	TCP ▼
Match Conditions	
Interface	cellular 1 ▼
Port	8080
Translated Address	
IP Address	192.168.2.100
Port	8080
Description	PortMapping

## Firewall >> NAT

NAT

### Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address	Description
DNAT	Outside	cellular 1:TCP 8080	192.168.2.100:8080	PortMapping

### Inside Network Interfaces


ID	Interface
1	fastethernet 0/2
2	<input type="text"/>

### Outside Network Interfaces

ID	Interface
1	cellular 1
2	<input type="text"/>

### Application Case 3- 1:1NAT:

1:1 NAT, binds a specific internal address (or subnet) to a specific external address (or subnet). Incoming traffic from the Internet to the specified IP will be directed toward the associated internal IP. Outgoing traffic to the Internet from the specified internal IP will originate from the associated external IP



## Firewall >> NAT

NAT

Action	<input type="text" value="1:1NAT"/>
Translation Type	<input type="text" value="IP to IP"/>
Match Conditions	
IP Address	<input type="text" value="192.168.2.2"/>
Translated Address	
IP Address	<input type="text" value="218.16.16.35"/>
Description	<input type="text"/>
Log	<input type="checkbox"/>

## **Contact us**

Technical Support Engineer: Lily.Sun

Email: [sunll@inhand.com.cn](mailto:sunll@inhand.com.cn)