Contents

NAT commands

The following matrix shows the feature and hardware compatibility:

Hardware series	Model	NAT compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: • WX3010H • WX3010H-X • WX3024H No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	Yes

The WX1800H series, WX2500H series, and WX3000H series access controllers do not support the **slot** keyword or the *slot-number* argument.

address

Use **address** to add an address range to a NAT address group.

Use **undo address** to remove an address range from a NAT address group.

Syntax

address *start-address end-address*

undo address *start-address end-address*

Default

No address range exists.

Views

NAT address group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start and end IP addresses of the address range. The end address must not be lower than the start address. If they are the same, the address range has only one IP address.

Usage guidelines

A NAT address group is a set of address ranges. The source address in a packet destined for an external network is translated into an address in one of the group ranges.

Each address range can contain a maximum of 65535 addresses.

If you add multiple address ranges, make sure they do not overlap.

Examples

Add two group ranges to an address group.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-address-group-2] address 10.1.1.20 10.1.1.30
```

Related commands

nat address-group

block-size

Use **block-size** to set the port block size.

Use **undo block-size** to restore the default.

Syntax

block-size *block-size*

undo block-size

Default

The port block size is 256.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

block-size: Sets the number of ports for a port block. The value range for this argument is 1 to 65535.

Usage guidelines

When you set a port block size, make sure the port block size is not larger than the number of ports in the port range.

Examples

Set the port block size to 1024 for port block group **1**.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] block-size 1024
```

Related commands

nat port-block-group

display nat alg

Use **display nat alg** to display the NAT with ALG status for all supported protocols.

Syntax

display nat alg

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Display the NAT with ALG status for all supported protocols.

```
<Sysname> display nat alg
NAT ALG:
  DNS         : Enabled
  FTP         : Disabled
  H323        : Disabled
  ICMP-ERROR  : Disabled
  ILS         : Disabled
  MGCP        : Disabled
  NBT         : Disabled
  PPTP        : Disabled
  RTSP        : Disabled
  RSH         : Disabled
  SCCP        : Disabled
  SIP         : Disabled
  SQLNET      : Disabled
  TFTP        : Disabled
  XDMCP       : Disabled
```

Related commands

display nat all

display nat all

Use **display nat all** to display all NAT configuration information.

Syntax

display nat all

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display all NAT configuration information.

```
<Sysname> display nat all
NAT address group information:
  Totally 3 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15
  Address group 2:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65
  Address group 3:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---
NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP             Port        Weight
  1                   192.168.0.26          23          100
                      192.168.0.27          23          500
  2                   ---                   ---         ---
  3                   192.168.0.26          69          100
NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
   Address group ID: 2
   Add route: Y         NO-PAT:Y         Reversible: N
    Rule name: a
```

```
    Priority: 1000
    Config status: Active
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y    NO-PAT: N         Reversible: N
    Rule name: b
    Priority: 22
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: address group, and ACL.
  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: 1
    Port-preserved: N    NO-PAT: Y         Reversible: Y
    Rule name: c
    Priority: 100
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
NAT internal server information:
  Totally 5 internal servers.
  Interface: Vlan-interface30
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    Config status : Active
  Interface: Vlan-interface40
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    ACL           : 3000
    Rule name     : red
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
  Interface: Vlan-interface50
    Protocol: 17(UDP)
    Global IP/port: 50.1.1.2/23
    Local IP/port : server group 1
                    1.1.1.1/21           (Connections: 10)
                    192.168.100.200/80   (Connections: 20)
    Config status : Active
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
```

```
  Net-to-net:
    Global IP    : 2.2.2.1 – 2.2.2.255
    Local IP     : 1.1.1.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Rule name    : green
    Priority     : 4
    Config status: Active
  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 2001
    Reversible   : Y
    Rule name    : blue
    Priority     : 4
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
  Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Rule name    : yellow
    Priority     : 5
    Config status: Active
  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 2001
    Reversible   : Y
    Rule name    : pink
    Priority     : 6
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active
  Interface: Vlan-interface30
    Config status: Active
NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
```

```
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active
  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.
NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active
NAT ALG:
  DNS        : Enabled
  FTP        : Disabled
  H323       : Enabled
  ICMP-ERROR : Enabled
  ILS        : Enabled
  MGCP       : Enabled
  NBT        : Enabled
  PPTP       : Enabled
  RSH        : Enabled
  RTSP       : Enabled
  SCCP       : Enabled
  SIP        : Disabled
  SQLNET     : Enabled
  TFTP       : Enabled
  XDMCP      : Enabled
NAT port block group information:
  Totally 2 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
```

```
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    Port block group: 2
    Rule name       : red
    Priority        : 4
    Config status   : Active
  Interface: Vlan-interface20
    Port block group: 10
    Rule name       : tigger
    Priority        : 6
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

The output shows all NAT configuration information. Table 1 describes only the fields for the output of the **nat mapping-behavior** and **nat alg** commands.

Table 1 Command output

Field	Description
NAT address group information	Information about the NAT address group. See Table 2 for output description.
NAT server group information	Information about the internal server group. See Table 14 for output description.
NAT inbound information:	Inbound dynamic NAT configuration. See Table 5 for output description.
NAT outbound information	Outbound dynamic NAT configuration. See Table 8 for output description.
NAT internal server information	NAT Server configuration. See Table 13 for output description.
Static NAT mappings	Static NAT mappings. See Table 16 for output description.
NAT DNS mappings	NAT with DNS mappings. See Table 3 for output description.
NAT logging	NAT logging configuration. See Table 6 for output description.

Field	Description
NAT mapping behavior	Mapping behavior mode of PAT: **Endpoint-Independent** or **Address and Port-Dependent**.
ACL	ACL number or name. If no ACL is specified for NAT, this field displays hyphens (---).
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Config status	Status of NAT mapping behavior configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT mapping behavior configuration does not take effect. This field is available when the **Config status** is **Inactive**.
NAT ALG	NAT with ALG configuration for different protocols.
NAT port block group information	Configuration information about NAT port block groups. See Table 11 for output description.
NAT outbound port block group information	Information about port block group application. See Table 9 for output description.

display nat address-group

Use **display nat address-group** to display NAT address group information.

Syntax

display nat address-group [*group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-number: Specifies the ID of a NAT address group. The value range for this argument is 0 to 65535. If you do not specify the *group-number* argument, this command displays information about all NAT address groups.

Examples

Display information about all NAT address groups.

```
<Sysname> display nat address-group
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15

  Address group 2:
    Port range: 1-65535
```

```
    Address information:
      Start address         End address
      202.110.10.20         202.110.10.25
      202.110.10.30         202.110.10.35

  Address group 3:
    Port range: 1024-65535
    Address information:
      Start address         End address
      202.110.10.40         202.110.10.50

  Address group 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address         End address
      202.110.10.60         202.110.10.65

  Address group 6:
    Port range: 1-65535
    Address information:
      Start address         End address
      ---                   ---
```

Display information about NAT address group **1**.

```
<Sysname> display nat address-group 1
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address         End address
      202.110.10.10         202.110.10.15
```

Table 2 Command output

Field	Description
Address group	ID of the NAT address group.
Port range	Port range for public IP addresses.
Block size	Number of ports in a port block. This field is not displayed if the port block size is not set.
Extended block number	Number of extended port blocks. This field is not displayed if the number of extended port blocks is not set.
Address information	Information about the public IP addresses in the address group.
Start address	Start IP address of an address range. If you do not specify a start address for the range, this field displays hyphens (---).
End address	End IP address of an address range. If you do not specify an end address for the range, this field displays hyphens (---).

Related commands

nat address-group

display nat dns-map

Use **display nat dns-map** to display NAT with DNS mapping configuration.

Syntax

display nat dns-map

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NAT with DNS mapping configuration.

```
<Sysname> display nat dns-map
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name  : www.server.com
  Global IP    : 6.6.6.6
  Global port  : 23
  Protocol     : TCP(6)
  Config status: Active

  Domain name  : www.service.com
  Global IP    : ---
  Global port  : 12
  Protocol     : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.
```

Table 3 Command output

Field	Description
NAT DNS mapping information	Information about NAT with DNS mappings.
Domain-name	Domain name of the internal server.
Global IP	Public IP address of the internal server. • If Easy IP is configured, this field displays the IP address of the specified interface. • If you do not specify a public IP address, this field displays hyphens (---).
Global port	Public port number of the internal server.
Protocol	Protocol type and number of the internal server.

Field	Description
Config status	Status of the DNS mapping configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the DNS mapping configuration does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat dns-map

display nat eim

Use **display nat eim** to display information about NAT Endpoint-Independent Mapping (EIM) entries.

Syntax

display nat eim [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays EIM entry information for all member devices.

Usage guidelines

A NAT device with PAT EIM configured performs the following tasks:

1. Creates a NAT session entry.
2. Creates an EIM entry for recording the mapping between a private address/port and a public address/port.

The EIM entry ensures the following:

- The same EIM entry applies to subsequent connections originating from the same source IP and port.
- The EIM entries allow reverse translation for connections initiated by external hosts to internal hosts.

Examples

Display information about NAT EIM entries for IRF member device 1.

```
<Sysname> display nat eim slot 1
Slot 1:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)
```

```
Total entries found: 2
```

Table 4 Command output

Field	Description
Local IP/port	Private IP address and port number.
Global IP/port	Public IP address and port number.
Protocol	Protocol type and number.
Total entries found	Total number of EIM entries.

Related commands

- **nat mapping-behavior**
- **nat outbound**

display nat inbound

Use **display nat inbound** to display information about inbound dynamic NAT.

Syntax

display nat inbound

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about inbound dynamic NAT.

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2      Address group name: b
    Add route: Y    NO-PAT: Y         Reversible: N
    Rule name: abcd
    Priority: 1000
    Config status: Active

Interface: Vlan-interface30
    ACL: 2037
    Address group ID: 1      Address group name: a
    Add route: Y    NO-PAT: Y         Reversible: N
    Rule name: eif
    Priority: 1000
    Config status: Inactive
    Reasons for inactive status:
```

```
The following items don't exist or aren't effective: ACL.
```

Table 5 Command output

Field	Description
NAT inbound information	Information about inbound dynamic NAT.
Interface	Interface where inbound dynamic NAT is configured.
ACL	ACL number or name.
Address group	NAT address group used by inbound dynamic NAT rule.
Add route	Whether to add a route when a packet matches the inbound dynamic NAT rule.
NO-PAT	Whether NO-PAT or PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Config status	Status of the inbound dynamic NAT configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the inbound dynamic NAT configuration does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat inbound

display nat log

Use **display nat log** to display NAT logging configuration.

Syntax

display nat log

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NAT logging configuration.

```
<Sysname> display nat log
NAT logging:
  Log enable          : Enabled(ACL 2000)
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
```

```
  Alarm               : Disabled
```

Table 6 Command output

Field	Description
NAT logging	NAT logging configuration.
Log enable	Whether NAT logging is enabled. If an ACL is specified for NAT logging, this field also displays the ACL number or name.
Flow-begin	Whether logging is enabled for NAT session establishment events.
Flow-end	Whether logging is enabled for NAT session removal events.
Flow-active	Whether logging is enabled for active NAT flows. If it is, this field also displays the interval in minutes at which active flow logging is generated.
Port-block-assign	Whether logging is enabled for NAT444 port block assignment.
Port-block-withdraw	Whether logging is enabled for NAT444 port block withdrawal.
Alarm	Whether logging is enabled for NAT444 alarms.

Related commands

- **nat log enable**
- **nat log flow-active**
- **nat log flow-begin**

display nat no-pat

Use **display nat no-pat** command to display information about NAT NO-PAT entries.

Syntax

display nat no-pat [**slot** *slot-number*]

Views

Any view

Default user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NO-PAT entry information for all member devices.

Usage guidelines

If a NAT device has a NO-PAT translation method configured, the device creates the following items:

- A NAT session entry.
- A NO-PAT entry for recording the mapping between a private address and a public address.

A NO-PAT entry can also be created during the ALG process for NAT.

The NO-PAT entry ensures the following:

- The same entry applies to subsequent connections originating from the same source IP address.

- The NO-PAT entries allow reverse translation for connections initiated by external hosts to internal hosts.

Outbound and inbound NO-PAT address translations create their own NO-PAT tables. These two types of tables are displayed separately.

Examples

Display information about NO-PAT entries.

```
<Sysname> display nat no-pat
Slot 1:
Global  IP: 200.100.1.100
Local   IP: 192.168.100.100
Reversible: N
Type      : Inbound

Local   IP: 192.168.100.200
Global  IP: 200.100.1.200
Reversible: Y
Type      : Outbound

Total entries found: 2
```

Table 7 Command output

Field	Description
Local IP	Private IP address.
Global IP	Public IP address.
Reversible	Whether reverse address translation is allowed.
Type	Type of the NO-PAT entry: • **Inbound**—NO-PAT entries are created during inbound dynamic NAT. • **Outbound**—NO-PAT entries are created during outbound dynamic NAT.
Total entries found	Total number of NO-PAT entries.

Related commands

- **nat inbound**
- **nat outbound**

display nat outbound

Use **display nat outbound** to display information about outbound dynamic NAT.

Syntax

display nat outbound

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about outbound dynamic NAT.

```
<Sysname> display nat outbound
NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
    Address group ID: 1            Address group name: a
    Port-preserved: Y    NO-PAT: N         Reversible: N
    Rule name: abcd
    Priority: 1000
    Config status: Active

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: ---
    Port-preserved: N    NO-PAT: Y         Reversible: Y
    Rule name: abcd
    Priority: 1000
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL
```

Table 8 Command output

Field	Description
NAT outbound information	Information about outbound dynamic NAT.
Interface	Interface where outbound dynamic NAT is configured.
ACL	IPv4 ACL number or name. If no IPv4 ACL is specified for outbound dynamic NAT, this field displays hyphens (---).
Address group	Address group used by inbound dynamic NAT. If no address group is specified for address translation, the field displays hyphens (---).
Port-preserved	Whether to try to preserve the port numbers for PAT.
NO-PAT	Whether NO-PAT is used: • **Y**—NO-PAT is used. • **N**—PAT is used.
Reversible	Whether reverse address translation is allowed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Config status	Status of the outbound dynamic NAT configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the outbound dynamic NAT configuration does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat outbound

display nat outbound port-block-group

Use **display nat outbound port-block-group** to display information about port block group application for NAT444.

Syntax

display nat outbound port-block-group

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about port block group application for NAT444.

```
<Sysname> display nat outbound port-block-group
NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: Vlan-interface20
    Port block group: 2
    Rule name: abcdefg
    Config status   : Active

  Interface: Vlan-interface20
    Port block group: 10
    Rule name: abcfg
    Config status   : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

Table 9 Command output

Field	Description
Interface	Interface to which a port block group is applied.
Port block group	ID of the port block group.
Rule name	Name of the NAT rule.
Config status	Status of the port block group application: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the port block group application fails. This field is available when the **Config status** is **Inactive**.

Related commands

nat outbound port-block-group

display nat port-block

Use **display nat port-block** to display NAT444 mappings.

Syntax

display nat port-block { **dynamic** | **static** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays dynamic NAT444 mappings.

static: Displays static NAT444 mappings.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT444 mappings for all member devices.

Examples

Display static NAT444 mappings.

```
<Sysname> display nat port-block static
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           100.100.100.111  202.202.100.101  10001-10256  0
---           100.100.100.112  202.202.100.101  10257-10512  0
---           100.100.100.113  202.202.100.101  10513-10768  0
---           100.100.100.113  202.202.100.101  10769-11024  0
Total mappings found: 4
```

Display dynamic NAT444 mappings.

```
<Sysname> display nat port-block dynamic
Slot 1:
Local VPN     Local IP         Global IP        Port block   Connections
---           101.1.1.12       192.168.135.201  10001-11024  1
Total mappings found: 1
```

Table 10 Command output

Field	Description
Local VPN	VPN to which the private IP address belongs. The device does not support this field in the current software version.
Local IP	Private IP address.
Global IP	Public IP address.
Port block	Port block defined by a start port and an end port.
Connections	Number of connections established by using the ports in the port block.

display nat port-block-group

Use **display nat port-block-group** to display information about NAT port block groups.

Syntax

display nat port-block-group [*group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-number: Specifies the ID of a port block group. The value range for this argument is 0 to 65535. If you do not specify this argument, the command displays information about all port block groups.

Examples

Display information about all port block groups.

```
<Sysname> display nat port-block-group
NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        ---
      192.168.3.1          192.168.3.254        ---
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          ---
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      ---                  ---                  ---
    Global IP pool information:
      Start address        End address
```

```
      ---                 ---
```

Display information about port block group **1**.

```
<Sysname> display nat port-block-group 1
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address       End address         VPN instance
      172.16.1.1          172.16.1.254        ---
      192.168.1.1         192.168.1.254       ---
      192.168.3.1         192.168.3.254       ---
    Global IP pool information:
      Start address       End address
      201.1.1.1           201.1.1.10
      201.1.1.21          201.1.1.25
```

Table 11 Command output

Field	Description
Port block group	ID of the NAT port block group.
Port range	Port range for the public IP addresses.
Block size	Number of ports in a port block.
Local IP address information	Information about private IP addresses.
Global IP pool information	Information about public IP addresses.
Start address	Start IP address of a private or public IP address range. If no start IP address is specified for the address range, this field displays hyphens (---).
End address	End IP address of a private or public IP address range. If no end IP address is specified for the address range, this field displays hyphens (---).
VPN instance	VPN to which the private IP address range belongs. The device does not support this field in the current software version.

Related commands

nat port-block-group

display nat port-block-usage

Use **display nat port-block-usage** to display the port block usage for dynamic NAT444 address groups.

Syntax

display nat port-block-usage [**address-group** *group-id*] [**slot** *slot-number*]

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

address-group *group-id*: Specifies the ID of an address group. The value range is 0 to 65535. If you do not specify an address group, this command displays the port block usage for all address groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the port block usage for all member devices.

Examples

Display the port block usage for dynamic NAT444 address groups in slot 1.

```
<Sysname> display nat port-block-usage slot 1
Slot 1:
Total NAT address groups found: 1
```

Table 12 Command output

Field	Description
Total NAT address groups found	Number of address groups.

display nat server

Use **display nat server** to display NAT Server configuration.

Syntax

display nat server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NAT Server configuration.

```
<Sysname> display nat server
NAT internal server information:
  Totally 5 internal servers.
  Interface: Vlan-interface30
    Global ACL    : 2000
    Local IP/port : 192.168.10.1/23
    Rule name     : cdefgab
    Priority      : 1000
    Config status : Active

  Interface: Vlan-interface40
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Rule name     : abcg
    Config status : Inactive
```

```
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

Interface: Vlan-interface50
  Protocol: 17(UDP)
  Global IP/port: 50.1.1.2/23
  Local IP/port : server group 1
                  1.1.1.1/21            (Connections: 10)
                  192.168.100.200/80    (Connections: 20)
  Rule name     : cdefg
  Config status : Active
```

Table 13 Command output

Field	Description
NAT internal server information	Information about NAT Server configuration.
Interface	Interface where NAT Server is configured.
Protocol	Protocol number and type of the internal server.
Global IP/port	Public IP address and port number of the internal server. • **Global IP**—A single IP address or an address pool of consecutive addresses. If you use Easy IP, this field displays the address of the specified interface. If you do not specify an address for the interface, the **Global IP** field displays hyphens (---). • **port**—A single port number or a port pool of consecutive port numbers. If no port number is in the specified protocol, the **port** field displays hyphens (---).
Local IP/port	For common NAT Server, this field displays the private IP address and port number of the server. • **Local IP**—A single IP address or an address pool of consecutive addresses. • **port**—A single port number or a port pool of consecutive port numbers. If no port number is in the specified protocol, the **port** field displays hyphens (---). For load sharing NAT Server, this field displays the internal server group name, IP address, port number, and number of connections of each member.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Rule name	Name of the NAT rule.
Config status	Status of the NAT Server configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the NAT Server configuration does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

nat server

display nat server-group

Use **display nat server-group** to display internal server group configuration.

Syntax

display nat server-group [*group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-number: Specifies the ID of the internal server group. The value range for this argument is 0 to 65535. If you do not specify this argument, this command displays configuration about all internal server groups.

Examples

Display configuration about all internal server groups.

```
<Sysname> display nat server-group
NAT server group information:
  Totally 3 NAT server groups.
  Group Number        Inside IP            Port        Weight
  1                   192.168.0.26         23          100
                      192.168.0.27         23          500
  2                   ---                  ---         ---
  3                   192.168.0.26         69          100
```

Display configuration about the specified internal server group.

```
<Sysname> display nat server-group 1
  Group Number        Inside IP            Port        Weight
  1                   192.168.0.26         23          100
                      192.168.0.27         23          500
```

Table 14 Command output

Field	Description
Group Number	ID of the internal server group.
Inside IP	Private IP address of a member in an internal server group. If no address is specified, this field displays hyphens (---).
Port	Private port number of a member in an internal server group. If no port number is specified, this field displays hyphens (---).
Weight	Weight of a member in an internal server. If no weight value is specified, this field displays hyphens (---).

Related commands

nat server-group

display nat session

Use **display nat session** to display sessions that have been NATed.

Syntax

display nat session [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

source-ip *source-ip*: Displays NAT sessions for the source IP address specified by the *source-ip* argument. The IP address must be the real source IP address of the packet that triggers the session establishment.

destination-ip *destination-ip*: Displays NAT sessions for the destination IP address specified by the *destination-ip* argument. The IP address must be the destination IP address of the packet that triggers the session establishment.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT sessions for all member devices.

verbose: Display detailed information about NAT sessions. If you do not specify this keyword, this command displays brief information about NAT sessions.

Usage guidelines

If you do not specify any parameters, this command displays all NAT sessions.

Examples

Display detailed information about NAT sessions.

```
<Sysname> display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface20
State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:         1 packets         48 bytes
Responder->Initiator:         0 packets          0 bytes

Total sessions found: 1
```

Table 15 Command output

Field	Description
Initiator	Session information about an initiator.
Responder	Session information about a responder.
DS-Lite tunnel peer	Destination address of the DS-Lite tunnel interface. If the session does not belong to any DS-Lite tunnel, this field displays a hyphen (-). The device does not support this field in the current software version.
VPN instance/VLAN ID/Inline ID	MPLS L3VPN instance to which the session belongs. The device does not support this field in the current software version. VLAN ID to which the session belongs for Layer 2 forwarding. INLINE to which the session belongs for Layer 2 forwarding. If a setting is not specified, this field displays a hyphen (-).
Protocol	Transport layer protocol type, **DCCP**, **ICMP**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.
Inbound interface	Input interface.
State	NAT session status.
Application	Application layer protocol type, such as **FTP** and **DNS**. This field displays **OTHER** for the protocol types identified by non-well-known ports.
Start time	Time when the session starts.
TTL	NAT session lifetime in seconds.
Initiator->Responder	Number of packets and packet bytes from the initiator to the responder.
Responder->Initiator	Number of packets and packet bytes from the responder to the initiator.
Total sessions found	Total number of session tables.

Related commands

reset nat session

display nat static

Use **display nat static** to display static NAT mappings.

Syntax

display nat static

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display static NAT mappings.

```
<Sysname> display nat static
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
```

```
  Net-to-net:
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Rule name    : abcdefg
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL          : 3000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
   Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 3000
    Reversible   : Y
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:         : 3001
    Reversible   : Y
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

  Interface: Vlan-interface30
    Config status: Active
```

Table 16 Command output

Field	Description
Net-to-net	Net-to-net static NAT mapping.
IP-to-IP	One-to-one static NAT mapping.
Local IP	Private IP address or address pool.
Global IP	Public IP address or address pool.
Netmask	Network mask.
ACL	ACL number or name. If no ACL is specified, this field is not displayed.
Reversible	Whether reverse address translation is allowed. If this feature is not configured, this field is not displayed.
Rule name	Name of the NAT rule.
Priority	Priority of the NAT rule.
Config status	Status of the static NAT mapping configuration: **Active** or **Inactive**.
Reasons for inactive status	Reasons why the static NAT mapping configuration does not take effect. This field is available when the **Config status** is **Inactive**.

Related commands

- **nat static**
- **nat static net-to-net**
- **nat static enable**

display nat statistics

Use **display nat statistics** to display NAT statistics.

Syntax

display nat statistics [**summary**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays NAT statistics summary. If you do not specify this keyword, this command displays detailed NAT statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT statistics for all member devices.

Examples

Display detailed information about all NAT statistics.

```
<Sysname> display nat statistics
Slot 1:
  Total session entries: 100
  Total EIM entries: 1
```

```
Total inbound NO-PAT entries: 0
Total outbound NO-PAT entries: 0
Total static port block entries: 10
Total dynamic port block entries: 15
Active static port block entries: 0
Active dynamic port block entries: 0
```

Table 17 Command output

Field	Description
Total session entries	Number of NAT session entries.
Total EIM entries	Number of EIM entries.
Total inbound NO-PAT entries	Number of inbound NO-PAT entries.
Total outbound NO-PAT entries	Number of outbound NO-PAT entries.
Total static port block entries	Number of static NAT444 mappings.
Total dynamic port block entries	Number of dynamic NAT444 mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
Active static port block entries	Number of static NAT444 mappings that are in use.
Active dynamic port block entries	Number of dynamic NAT444 mappings that have been created. It equals the number of dynamically assigned port blocks.

Display summary information about all NAT statistics.

```
<Sysname> display nat statistics summary
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM       SPB       DPB       ASPB      ADPB
1    0         0         0         1572720   0         0
```

Table 18 Command output

Field	Description
Slot	Member ID of the IRF member device.
Sessions	Number of NAT session entries.
EIM	Number of EIM entries.
SPB	Number of static NAT444 mappings.
DPB	Number of dynamic NAT444 mappings that can be created. It equals the number of port blocks for dynamic assignment, including the assigned and unassigned port blocks.
ASPB	Number of static NAT444 mappings in use.
ADPB	Number of dynamic NAT444 mappings that have been created. It equals the number of dynamically assigned port blocks.

global-ip-pool

Use **global-ip-pool** to add a public IP address range to a NAT port block group.

Use **undo global-ip-pool** to delete a public IP address range from a NAT port block group.

Syntax

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address*

Default

No public IP address range exists in the NAT port block group.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a public IP address range. The end IP address cannot be smaller than the start IP address. If the start and end IP addresses are the same, only one public IP address is specified.

Usage guidelines

You can add multiple public IP address ranges to a port block group, but they cannot overlap.

Public IP address ranges in different port block groups can overlap. But the port ranges for overlapped ranges in different port block groups cannot overlap.

The number of port blocks that a public IP address can assign is determined by dividing the number of ports in the port range by the port block size.

Examples

Add a public IP address range to the port block group **1**. The public IP address range consists of IP addresses from 202.10.1.1 to 202.10.1.10.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10
```

Related commands

nat port-block-group

inside ip

Use **inside ip** to add a member to an internal server group.

Use **undo inside ip** to remove a member from an internal server group.

Syntax

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

Default

An internal server group does not contain any member.

Views

Internal server group view

Predefined user roles

network-admin

Parameters

inside-ip: Specifies the IP address of an internal server.

port *port-number*: Specifies the port number of an internal server, in the range of 1 to 65535, excluding FTP port 20.

weight *weight-value*: Specifies the weight of the internal server. The value range is 1 to 1000, and the default value is 100. An internal server with a larger weight receives a larger percentage of connections in the internal server group.

Examples

Add a member with IP address 10.1.1.2 and port number 30 to internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
[Sysname-nat-server-group-1] inside ip 10.1.1.2 port 30
```

Related commands

nat server-group

local-ip-address

Use **local-ip-address** to add a private IP address range to a NAT port block group.

Use **undo local-ip-address** to delete a private IP address range from a NAT port block group.

Syntax

local-ip-address *start-address end-address*

undo local-ip-address *start-address*

Default

No private IP address range exists in a NAT port block group.

Views

NAT port block group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start IP address and end IP address of a private IP address range. The end IP address cannot be smaller than the start IP address. If the start and end IP addresses are the same, only one private IP address is specified.

Usage guidelines

You can add multiple private IP address ranges to a port block group, but they cannot overlap.

Private IP address ranges in different port block groups can overlap.

For static NAT444 mappings in one port block group, the number of private IP addresses cannot be larger than the number of assignable port blocks. Otherwise, some private IP addresses cannot obtain port blocks.

Examples

Add a private IP address range to the port block group 1. The private IP address range consists of IP addresses from 172.16.1.1 to 172.16.1.255.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255
```

Related commands

nat port-block-group

nat address-group

Use **nat address-group** to create a NAT address group and enter its view.

Use **undo nat address-group** to remove a NAT address group.

Syntax

nat address-group *group-number* [**name** *group-name*]

undo nat address-group *group-number*

Default

No NAT address group exists.

Views

System view

Predefined user roles

network-admin

Parameters

group-number: Assigns an ID to the NAT address group. The value range for this argument is 0 to 65535.

name *group-name*: Assigns a name to the NAT address group. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

A NAT address group consists of multiple address ranges. Use the **address** command to specify an address range.

Examples

Create a NAT address group numbered 1 and named **abc**.

```
<Sysname> system-view
[Sysname] nat address-group 1 name abc
```

Related commands

- **address**
- **display nat address-group**
- **display nat all**
- **nat inbound**
- **nat outbound**

nat alg

Use **nat alg** to enable NAT with ALG for the specified or all supported protocols.

Use **undo nat alg** to disable NAT with ALG for the specified or all supported protocols.

Syntax

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** |**tftp** | **xdmcp** }

Default

NAT with ALG is enabled for DNS, FTP, ICMP error messages, RTSP, and PPTP, and is disabled for the other supported protocols.

Views

System view

Predefined user roles

network-admin

Parameters

all: Enables NAT with ALG for all supported protocols.

dns: Enables NAT with ALG for DNS.

ftp: Enables NAT with ALG for FTP.

h323: Enables NAT with ALG for H.323.

icmp-error: Enables NAT with ALG for ICMP error packets.

ils: Enables NAT with ALG for ILS.

mgcp: Enables NAT with ALG for MGCP.

nbt: Enables NAT with ALG for NBT.

pptp: Enables NAT with ALG for PPTP.

rsh: Enables NAT with ALG for RSH.

rtsp: Enables NAT with ALG for RTSP.

sccp: Enables NAT with ALG for SCCP.

sip: Enables NAT with ALG for SIP.

sqlnet: Enables NAT with ALG for SQLNET.

tftp: Enables NAT with ALG for TFTP.

xdmcp: Enables NAT with ALG for XDMCP.

Usage guidelines

NAT with ALG translates address or port information in the application layer payload to ensure connection establishment.

For example, an FTP application includes a data connection and a control connection. The IP address and port number for the data connection depend on the payload information of the control connection. This requires NAT with ALG to translate the address and port information to establish data connection.

Examples

Enable NAT with ALG for FTP.

```
<Sysname> system-view
[Sysname] nat alg ftp
```

Related commands

display nat all

nat dns-map

Use **nat dns-map** to configure a DNS mapping for NAT. The mapping maps the domain name of an internal server to the public IP address, public port number, and protocol type of the internal server.

Use **undo nat dns-map** to remove a DNS mapping for NAT.

Syntax

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

Default

No DNS mapping for NAT exists.

Views

System view

Predefined user roles

network-admin

Parameters

domain *domain-name*: Specifies the domain name of an internal server. A domain name is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.) (for example, aabbcc.com). The domain name suffix can contain a maximum of 253 characters, and each separated string contains no more than 63 characters.

protocol *pro*-type: Specifies the type of the protocol used by the internal server, **tcp** or **udp**.

interface *interface-type interface-number*: Enables Easy IP to use the IP address of the interface specified by its type and number as the public address of the internal server.

ip *global-ip*: Specifies the public IP address used by the internal server to provide services for the external network.

port *global-port*: Specifies the public port number used by the internal server to provide services for the external network. The port number format can be one of the following:

- A number in the range of 1 to 65535.
- A protocol name, a string of 1 to 15 characters. For example, **ftp** and **telnet**.

Usage guidelines

NAT with DNS mapping must operate with the NAT Server feature. NAT with DNS mapping maps the domain name of the internal server to the public IP address, public port number, and protocol type of the server. NAT Server maps the public IP and port to the private IP and port of the internal server. This allows an internal host to access an internal server on the same private network by using the domain name of the internal server when the DNS server is on the public network.

You can configure multiple NAT with DNS mappings.

Examples

Configure a NAT with DNS mapping between the domain name **www.server.com**, the public IP address **202.112.0.1**, and the public port number **12345**. Specify the protocol type as TCP.

```
<Sysname> system-view
[Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345
```

Related commands

- **display nat all**
- **display nat dns-map**
- **nat server**

nat icmp-error reply

Use **nat icmp-error reply** to enable sending ICMP error messages for NAT failures.

Use **undo nat icmp-error reply** to restore the default.

Syntax

nat icmp-error reply

undo nat icmp-error reply

Default

No ICMP error messages are sent for NAT failures.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Disabling sending ICMP error messages for NAT failures reduces useless packets, saves bandwidth, and avoids exposing the firewall IP address to the public network.

This command is required for traceroute.

Examples

Enable sending ICMP error messages for NAT failures.

```
<Sysname> system-view
[Sysname] nat icmp-error reply
```

nat inbound

Use **nat inbound** to configure an inbound dynamic NAT rule on an interface.

Use **undo nat inbound** to remove the specified inbound dynamic NAT rule on an interface.

Syntax

nat inbound { *acl-number* | **name** *acl-name* } **address-group** { *group-number* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat inbound { *acl-number* | **name** *acl-name* }

Default

No inbound dynamic NAT rule is configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

address-group *group-number*: Specifies an address group for address translation. The value for the *group-number* argument is 0 to 65535.

group-name: Specifies the name of a NAT address group. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

no-pat: Uses NO-PAT for inbound NAT. If you do not specify this keyword, PAT is used. PAT supports only TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal hosts to external hosts. It uses existing NO-PAT entries to translate destination addresses for packets of these connections if the packets are permitted by ACL reverse matching.

add-route: Automatically adds a route to the private address when address translation is performed for a packet. The output interface is the NAT interface and the next-hop is the source address before translation. If you do not specify this keyword, you must manually add the route. Because automatic route adding is slow, H3C recommends that you add routes manually.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the inbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

description *text*: Specifies a description for the inbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Inbound dynamic NAT translates the source IP addresses of incoming packets permitted by the ACL into IP addresses in the address group.

Inbound dynamic NAT supports the PAT and NO-PAT modes.

- **PAT**—Performs port translation in addition to IP address translation.
- **NO-PAT**—Performs only IP address translation.

The NO-PAT mode supports reverse address translation. Reverse address translation uses ACL reverse matching to identify packets to be translated. ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.

- Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Inbound dynamic NAT typically operates with one of the following to implement bidirectional NAT:

- Outbound dynamic NAT (the **nat outbound** command).
- The NAT Server feature (the **nat server** command).
- Outbound static NAT (the **nat static** command).

An address group cannot be used by both the **nat inbound** and **nat outbound** commands. It cannot be used by the **nat inbound** command in both PAT and NO-PAT modes.

Do not specify the **add-route** keyword if the internal and external networks are on the same subnet.

An ACL can be used by only one inbound dynamic NAT rule on an interface.

You can configure multiple inbound dynamic NAT rules on an interface.

The **vpn-instance** parameter is required if you deploy inbound dynamic NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure ACL 2001, and create a rule to permit packets only from subnet 10.110.10.0/24 to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Create address group 1 and add an address range to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an inbound NO-PAT rule on interface VLAN-interface 10, and specify the name and the priority of the rule as **abc** and 0, respectively. NAT translates the source addresses of incoming packets into the addresses in address group 1, and automatically adds a route for translated packets.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc
priority 0
```

Related commands

- **display nat all**
- **display nat inbound**
- **display nat no-pat**

nat inbound rule move

Use **nat inbound rule move** to modify the priority of an inbound dynamic NAT rule.

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of a NAT rule to be moved.

after: Moves NAT rule *nat-rule-name1* to appear behind NAT rule *nat-rule-name2*.

before: Moves NAT rule *nat-rule-name1* to appear in front of NAT rule *nat-rule-name2*.

nat-rule-name2: Specifies the name of a NAT rule to be moved.

Usage guidelines

This command takes effect only on an inbound dynamic NAT rule that has a name.

After you change the order of the inbound dynamic NAT rules by executing this command, the priorities of these NAT rules also changes.

- If you execute the **nat inbound rule move** *nat-rule-name1* **after** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. The priority value of NAT rule *nat-rule-name1* changes to be greater than that of NAT rule *nat-rule-name2* by 1.
- If you execute the **nat inbound rule move** *nat-rule-name1* **before** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. The priority value of NAT rule *nat-rule-name1* changes to be smaller than that of NAT rule *nat-rule-name2* by 1.

A rule with a high priority takes precedence over a rule with a low priority for packet matching.

Examples

Move inbound dynamic NAT rule **abc** to appear in front of inbound dynamic NAT rule **def**.

```
<Sysname> nat inbound rule move abc before def
```

Related commands

nat inbound

nat log alarm

Use **nat log alarm** to enable NAT444 alarm logging.

Use **undo nat log alarm** to disable NAT444 alarm logging.

Syntax

nat log alarm

undo nat log alarm

Default

NAT alarm logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable NAT logging before you enable NAT444 alarm logging. The alarm logs are informational.

The NAT444 gateway generates alarm logs in the following situations:

- The ports in the selected port block of a static NAT444 mapping are all occupied.

- The ports in the selected port blocks (including extended ones) of a dynamic NAT444 mapping are all occupied.
- The public IP addresses and port blocks for dynamic NAT444 are all assigned.

Examples

Enable NAT444 alarm logging.

```
<Sysname> system-view
[Sysname] nat log alarm
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat log enable

Use **nat log enable** to enable NAT logging.

Use **undo nat log enable** to disable NAT logging.

Syntax

nat log enable [**acl** { *acl-number* | **name** *acl-name* }]

undo nat log enable

Default

NAT logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

acl: Specifies an ACL.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You must enable NAT logging before you enable NAT session logging, NAT444 user logging, or NAT444 alarm logging.

The **acl** keyword takes effect only for NAT session logging. If an ACL is specified, flows matching the permit rule might trigger NAT session logs. If you do not specify an ACL, all flows processed by NAT might trigger NAT session logs.

Examples

Enable NAT logging.

```
<Sysname> system-view
[Sysname] nat log enable
```

Related commands

- **display nat all**
- **display nat log**

- **nat log alarm**
- **nat log flow-active**
- **nat log flow-begin**
- **nat log flow-end**
- **nat log port-block-assign**
- **nat log port-block-withdraw**

nat log flow-active

Use **nat log flow-active** to log active NAT flows and set the logging interval.

Use **undo nat log flow-active** to disable the logging feature for active NAT flows.

Syntax

nat log flow-active *time-value*

undo nat log flow-active

Default

Logging for active NAT flows is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the interval for logging active NAT flows, in the range of 10 to 120 minutes.

Usage guidelines

This feature helps track active NAT flows.

Logging for active flows takes effect only after you enable NAT logging.

Examples

Enable logging for active NAT flows and set the logging interval to 10 minutes.

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat log flow-begin

Use **nat log flow-begin** to enable logging for NAT session establishment events.

Use **undo nat log flow-begin** to disable logging for NAT session establishment events.

Syntax

nat log flow-begin

undo nat log flow-begin

Default

Logging for NAT session establishment events is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Logging for NAT session establishment events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session establishment events.

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat log flow-end

Use **nat log flow-end** to enable logging for NAT session removal events.

Use **undo nat log flow-end** to disable logging for NAT session removal events.

Syntax

nat log flow-end

undo nat log flow-end

Default

Logging for NAT session removal events is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Logging for NAT session removal events takes effect only after you enable NAT logging.

Examples

Enable logging for NAT session removal events.

```
<Sysname> system-view
[Sysname] nat log flow-end
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat log port-block-assign

Use **nat log port-block-assign** to enable NAT444 user logging for port block assignment.

Use **undo nat log port-block-assign** to disable NAT444 user logging for port block assignment.

Syntax

nat log port-block-assign

undo nat log port-block-assign

Default

NAT444 user logging is disabled for port block assignment.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable NAT logging before you enable NAT444 user logging for port block assignment.

For static NAT444, the NAT444 gateway generates a user log when it translates the first connection from a private IP address.

For dynamic NAT444, the NAT444 gateway generates a user log when it assigns or extends a port block for a private IP address.

Examples

Enable NAT444 user logging for port block assignment.

```
<Sysname> system-view
[Sysname] nat log port-block-assign
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat log port-block-withdraw

Use **nat log port-block-withdraw** to enable NAT444 user logging for port block withdrawal.

Use **undo nat log port-block-withdraw** to disable NAT444 user logging for port block withdrawal.

Syntax

nat log port-block-withdraw

undo nat log port-block-withdraw

Default

NAT444 user logging is disabled for port block withdrawal.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable NAT logging before you enable NAT444 user logging for port block withdrawal.

For static NAT444, the NAT444 gateway generates a user log when all connections from a private IP address are disconnected.

For dynamic NAT444, the NAT444 gateway generates a user log when all the following conditions are met:

- All connections from a private IP address are disconnected.
- The port blocks (including the extended ones) assigned to the private IP address are withdrawn.
- The corresponding mapping entry is deleted.

Examples

Enable NAT444 user logging for port block withdrawal.

```
<Sysname> system-view
[Sysname] nat log port-block-withdraw
```

Related commands

- **display nat all**
- **display nat log**
- **nat log enable**

nat mapping-behavior

Use **nat mapping-behavior** to configure the mapping behavior mode for PAT.

Use **undo nat mapping-behavior** to restore the default.

Syntax

nat mapping-behavior endpoint-independent [**acl** { *acl-number* | **name** *acl-name* }]

undo nat mapping-behavior endpoint-independent

Default

Address and Port-Dependent Mapping applies.

Views

System view

Predefined user roles

network-admin

Parameters

acl: Specifies an ACL to apply the NAT mapping behavior to packets that are permitted by the ACL. If you do not specify an ACL, the Endpoint-Independent Mapping applies to all packets.

acl *acl-number*: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

PAT supports the following types of NAT mappings:

- **Endpoint-Independent Mapping**—Uses the same IP and port mapping (EIM entry) for packets from the same source and port to any destination. EIM allows external hosts to access the internal hosts by using the translated IP address and port. It allows internal hosts behind different NAT gateways to access each other.

- **Address and Port-Dependent Mapping**—Uses different IP and port mappings for packets with the same source IP and port to different destination IP addresses and ports. APDM allows an external host to access an internal host only under the condition that the internal host has previously accessed the external host. It is secure, but it does not allow internal hosts behind different NAT gateways to access each other.

This command takes effect only on outbound PAT. Address and Port-Dependent Mapping always applies to inbound PAT.

Examples

Apply the Endpoint-Independent Mapping mode to all packets for address translation.

```
<Sysname> system-view
[Sysname] nat mapping-behavior endpoint-independent
```

Apply the Endpoint-Independent Mapping to FTP and HTTP packets, and the Address and Port-Dependent Mapping to other packets for address translation.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] nat mapping-behavior endpoint-independent acl 3000
```

Related commands

- **nat outbound**
- **display nat eim**

nat outbound

Use **nat outbound** to configure an outbound dynamic NAT rule on an interface.

Use **undo nat outbound** to remove the specified outbound dynamic NAT rule.

Syntax

NO-PAT:

nat outbound [*acl-number* | **name** *acl-name*] **address-group** { *group-number* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat outbound [*acl-number* | **name** *acl-name*]

PAT:

nat outbound [*acl-number* | **name** *acl-name*] [**address-group** { *group-number* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*]

undo nat outbound [*acl-number* | **name** *acl-name*]

Default

No outbound dynamic NAT rule is configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

address-group *group-number*: Specifies an address group for NAT. The value range for the *group-number* argument is 0 to 65535. If you do not specify an address group, the IP address of the interface is used as the NAT address. Easy IP is used.

group-name: Specifies the name of a NAT address group. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

no-pat: Uses NO-PAT for outbound NAT. If you do not specify this keyword, PAT is used. PAT only supports TCP, UDP, and ICMP query packets. For an ICMP packet, the ICMP ID is used as its source port number.

reversible: Allows reverse address translation. Reverse address translation uses existing NO-PAT entries to translate destination addresses for packets of connections actively initiated by external hosts to internal hosts.

port-preserved: Tries to preserve port number for PAT.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the outbound dynamic NAT rule. If you do not specify this keyword, the rule is enabled.

description *text*: Specifies a description for the outbound dynamic NAT rule. The *text* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Outbound dynamic NAT is typically configured on the interface connected to the external network. NAT translates the source IP addresses of outgoing packets permitted by the ACL into IP addresses in the address group. If you do not specify an ACL, NAT translates all packets.

Outbound dynamic NAT supports the following modes:

- **PAT**—Performs port translation in addition to IP address translation.
- **NO-PAT**—Performs only IP address translation.

The NO-PAT mode supports reverse address translation. If an ACL is specified, reverse address translation only applies to packets permitted by ACL reverse matching. ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the matching NO-PAT entry, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Dynamic NAT444 does not support the **NO-PAT** mode.

An address group cannot be used by both the **nat inbound** and **nat outbound** commands. It cannot be used by the **nat outbound** command in both PAT and NO-PAT modes.

An ACL can be used by only one outbound dynamic NAT rule an interface.

You can configure multiple outbound dynamic NAT rules on an interface.

Outbound dynamic NAT rules with ACLs configured on an interface takes precedence over those without ACLs. The priority for the ACL-based dynamic NAT rules depends on ACL number. A higher ACL number represents a higher priority.

When a port range and port block parameters are specified in the NAT address group, this command configures a dynamic NAT444 rule. Packets matching the ACL permit rule are processed by dynamic NAT444.

The **port-preserved** keyword does not take effect on dynamic NAT444.

The **vpn-instance** parameter is required if you deploy outbound dynamic NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure ACL 2001, and create a rule to permit packets only from segment 10.110.10.0/24 to pass through.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

Create address group 1 and add an address range to the group.

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

Configure an outbound dynamic PAT rule on interface VLAN-interface 10 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address group 1.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1
[Sysname-Vlan-interface10] quit
```

Or

Configure an outbound NO-PAT rule on interface VLAN-interface 10 to translate the source addresses of outgoing packets permitted by ACL 2001 into the addresses in address pool 1.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1 no-pat
[Sysname-Vlan-interface10] quit
```

Or

Enable Easy IP to use the IP address of VLAN-interface 10 as translated address.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001
[Sysname-Vlan-interface10] quit
```

Or

Enable reverse address translation and use addresses in address pool 1 as NAT addresses.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible
```

Related commands

- **display nat eim**
- **display nat outbound**
- **nat mapping-behavior**

nat outbound port-block-group

Use **nat outbound port-block-group** to apply a port block group to the outbound direction of an interface.

Use **undo nat outbound port-block-group** to remove a port block group application.

Syntax

nat outbound port-block-group *group-number* [**rule** *rule-name*]

undo nat outbound port-block-group *group-number*

Default

No port block group is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-number: Specifies a port block group by its ID. The value range for this argument is 0 to 65535.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

Usage guidelines

You can apply multiple port block groups to one interface.

After you apply a port block group to an interface, the system automatically computes the NAT444 mappings and creates entries for them. When a private IP address accesses the public network, the private IP address is translated to the mapped public IP address, and the ports are translated to ports in the selected port block.

Examples

Apply port block group 1 to the outbound direction of VLAN-interface 10, and specify the name of the port block group mapping rule as **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat outbound port-block-group 1 rule abc
```

Related commands

- **display nat all**
- **display nat outbound port-block-group**
- **display nat port-block**
- **nat port-block-group**

nat outbound rule move

Use **nat outbound rule move** to modify the priority of an outbound dynamic NAT rule.

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of a NAT rule to be moved.

after: Moves NAT rule *nat-rule-name1* to appear behind NAT rule *nat-rule-name2*.

before: Moves NAT rule *nat-rule-name1* to appear in front of NAT rule *nat-rule-name2*.

nat-rule-name2: Specifies the name of a NAT rule to be moved.

Usage guidelines

This command takes effect only on an outbound dynamic NAT rule that has a name.

After you change the order of the outbound dynamic NAT rules by executing this command, the priorities of these NAT rules also changes.

- If you execute the **nat outbound rule move** *nat-rule-name1* **after** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. The priority value of NAT rule *nat-rule-name1* changes to be greater than that of NAT rule *nat-rule-name2* by 1.
- If you execute the **nat outbound rule move** *nat-rule-name1* **before** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. The priority value of NAT rule *nat-rule-name1* changes to be smaller than that of NAT rule *nat-rule-name2* by 1.

A rule with a high priority takes precedence over a rule with a low priority for packet matching.

Examples

Move outbound dynamic NAT rule **abc** to appear in front of outbound dynamic NAT rule **def**.

```
<Sysname> nat outbound rule move abc before def
```

Related commands

nat outbound

nat port-block global-share enable

Use **nat port-block global-share enable** to enable global mapping sharing for dynamic NAT444.

Use **undo nat port-block global-share enable** to disable global mapping sharing for dynamic NAT444.

Syntax

nat port-block global-share enable

undo nat port-block global-share enable

Default

Global mapping sharing is disabled for Dynamic NAT444.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When multiple interfaces have dynamic NAT444 configured, the interfaces might create different NAT444 mappings for packets from the same IP address. You can use this command to configure the interfaces to share the same NAT444 mapping for translating packets from the same IP address.

Examples

Enable global mapping sharing for dynamic NAT444.

```
<Sysname> system-view
[Sysname] nat port-block global-share enable
```

Related commands

port-block

nat port-block-group

Use **nat port-block-group** to create a port block group and enter its view.

Use **undo nat port-block-group** to delete a port block group.

Syntax

nat port-block-group *group-number*

undo nat port-block-group *group-number*

Default

No port block group exists.

Views

System view

Predefined user roles

network-admin

Parameters

group-number: Assigns an ID to the NAT port block group. The value range for this argument is 0 to 65535.

Usage guidelines

A port block group is configured to implement static NAT444.

You must configure the following items for a port block group:

- A minimum of one private IP address range (see the **local-ip-address** command).
- A minimum of one public IP address range (see the **global-ip-address** command).
- A port range (see the **port-range** command).
- A port block size (see the **block-size** command).

The system computes static NAT444 mappings according to the port block group configuration, and creates entries for the mappings.

Examples

Create NAT port block group **1**.

```
<Sysname>system-view
[Sysname]nat port-block-group 1
[Sysname-port-block-group-1]
```

Related commands

- **block-size**
- **display nat all**
- **display nat port-block-group**
- **global-ip-pool**
- **local-ip-address**
- **nat outbound port-block-group**
- **port-range**

nat log port-block usage threshold

Use **nat log port-block usage threshold** to set the port block usage threshold for dynamic NAT444.

Use **undo nat log port-block usage threshold** to restore the default.

Syntax

nat log port-block usage threshold *threshold-value*

undo nat log port-block usage threshold

Default

The port block usage threshold for dynamic NAT444 is 90%.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the port block usage threshold in percentage, in the range of 40 to 100.

Usage guidelines

The system generates alarm logs if the port block usage exceeds the threshold.

Examples

Set the port block usage threshold for dynamic NAT444 to 60%.

```
<Sysname> system-view
[Sysname] nat log port-block usage threshold 60
```

nat server

Use **nat server** to create a mapping from the private IP address and port of an internal server to a public address and port for an internal server.

Use **undo nat server** to remove a mapping.

Syntax

Common NAT Server:

- A single public address with no or a single public port:

  nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] **inside** *local-address* [*local-port*] [**acl** { *acl-number* | **name** *acl-name* }] [**reversible**] [**rule** *rule-name*] [**disable**]

undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*]

- A single public address with consecutive public ports:

  nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port1 local-port2* } [**acl** { *acl-number* | **name** *acl-name* }] [**rule** *rule-name*] [**disable**]

  undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2*

- Consecutive public addresses with no or a single public port:

  nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**acl** { *acl-number* | **name** *acl-name* }] [**rule** *rule-name*] [**disable**]

  undo nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*]

- Consecutive public addresses with a single public port:

  nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* **inside** *local-address local-port1 local-port2* [**acl** { *acl-number* | **name** *acl-name* }] [**rule** *rule-name*] [**disable**]

  undo nat server protocol *pro-type* **global** *global-address1 global-address2 global-port*

Load sharing NAT Server:

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* } **inside server-group** *group-number* [**acl** { *acl-number* | **name** *acl-name* }] [**rule** *rule-name*] [**disable**]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* }

ACL-based NAT Server:

nat server global { *global-acl-number* | **name** *global-acl-name* } **inside** *local-address* [*local-port*] [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat server global { *global-acl-number* | **name** *global-acl-name* } **inside** *local-address* [*local-port*]

Default

The NAT Server feature is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

protocol *pro-type*: Specifies a protocol type. When the protocol is TCP or UDP, NAT Server can be configured with port information. If you do not specify a protocol type, the command applies to packets of all protocols. The protocol type format can be one of the following:

- A number in the range of 1 to 255.
- A protocol name of **icmp**, **tcp**, or **udp**.

global-address: Specifies the public address of an internal server.

global-address*1 global address2*: Specifies a public IP address range, which can include a maximum number of 65535 addresses. The *global-address1* argument specifies the start address, and *global address2* specifies the end address that must be greater than the start address.

global: Specifies an ACL. The destination IP addresses of packets permitted by the ACL can be translated.

global-acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *global-acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

current-interface: Enables Easy IP on the current interface. The IP address of the interface is used as the public address for the internal server.

interface *interface-type interface-number*: Enables Easy IP on the interface specified by its type and number. The IP address of the interface is used as the public address for the internal server. Only loopback interfaces are supported.

global-port1 global-port2: Specifies a public port number range, which can include a maximum of 256 ports. The *global-port1* argument specifies the start port, and *global-port2* specifies the end port that must be greater than the start port. The public port number format can be one of the following:

- A number in the range of 1 to 65535. Both the start port and the end port support this format.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**. Only the start port supports this format.

local-address1 local-address2: Specifies a private IP address range. The *local-address1* argument specifies the start address, and *local-address2* specifies the end address that must be greater than the start address. The number of addresses in the range must equal the number of ports in the public port number range.

local-port: Specifies the private port number. The private port number format can be one of the following:

- A number in the range of 1 to 65535, excluding FTP port 20. Both the start port and the end port support this format.
- A protocol name, a string of 1 to 15 characters. For example, **http** and **telnet**.

global-port: Specifies the public port number. The default value and value range are the same as those for the *local-port* argument.

local-address: Specifies the private IP address.

server-group *group-number*: Specifies the internal server group to which the internal server belongs. With this parameter, the load sharing NAT Server feature is configured. The *group-number* argument specifies the internal server group number. The value range for this argument is 0 to 65535.

acl: Specifies an ACL to identify packets that can be translated by using the mapping.

acl-number: Specifies an ACL by its number in the range of 2000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal servers to the external network. It translates the private IP addresses of the internal servers to their public IP addresses.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the NAT Server mapping. If you do not specify this keyword, the mapping is enabled.

Usage guidelines

You can configure the NAT Server feature to allow internal servers (such as Web, FTP, Telnet, POP3, and DNS servers) in the internal network to provide services for external users.

NAT Server is usually configured on the interface connected to the external network on a NAT device. By using the *global-address* and *global-port* arguments, external users can access the internal server at *local-address* and *local-port*. The following table describes the address-port mappings between an external network and an internal network for NAT Server.

Table 19 Address-port mappings for NAT Server

External network	Internal network
One public address	One private address
One public address and one public port number	One private address and one private port number
One public address and *N* consecutive public port numbers	One private address and one private port number
	N consecutive private addresses and one private port number
	One private address and *N* consecutive private port numbers
N consecutive public addresses	One private address
	N consecutive private addresses
N consecutive public addresses and one public port number	One private address and one private port number
	N consecutive private addresses and one private port number
	One private address and *N* consecutive private port numbers
One public address and one public port number	One private server group
One public address and *N* consecutive public port numbers	
N consecutive public addresses and one public port number	
Public addresses matching an ACL	One private address
	One private address and one private port

The number of internal servers that each command can define equals the number of public ports in the specified public port range.

When the protocol type is not **udp** (protocol number 17) or **tcp** (protocol number 6), you can configure only one-to-one IP address mapping.

The mapping of the protocol type, public address, and public port number must be unique for an internal server on an interface.

If the IP address of an interface used by Easy IP changes and conflicts with the IP address of an internal server not using Easy IP, the Easy IP configuration becomes invalid. If the conflicted address is modified to an unconflicted address or the internal server configuration without Easy IP is removed, the Easy IP configuration takes effect.

The **vpn-instance** parameter is required if you deploy NAT Server for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Allow external users to access the internal Web server at 10.110.10.10 on the LAN through http://202.110.10.10:8080.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http
[Sysname-Vlan-interface10] quit
```

Allow external users to access the internal FTP server at 10.110.10.11 through ftp://202.110.10.10.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server protocol tcp global 202.110.10.10 21 inside 10.110.10.11
[Sysname-Vlan-interface10] quit
```

Allow external hosts to ping the host at 10.110.10.12 by using the **ping 202.110.10.11** command.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server protocol icmp global 202.110.10.11 inside 10.110.10.12
[Sysname-Vlan-interface10] quit
```

Allow external hosts to access the Telnet services of internal servers at 10.110.10.1 to 10.110.10.100 through the public address 202.110.10.10 and port numbers from 1001 to 1100. As a result, a user can Telnet to 202.110.10.10:1001 to access 10.110.10.1, Telnet to 202.110.10.10:1002 to access 10.110.10.2, and so on.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server protocol tcp global 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet
```

Configure ACL-based NAT Server to allow users to use IP addresses in subnet 192.168.0.0/24 to access the internal server at 10.0.0.172.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat server global 3000 inside 10.0.0.172
```

Related commands

- **display nat all**
- **display nat server**
- **nat server-group**

nat server-group

Use **nat server-group** to create an internal server group.

Use **undo nat server-group** to remove an internal server group.

Syntax

nat server-group *group-number*

undo nat server-group *group-number*

Default

No internal server group exists.

Views

System view

Predefined user roles

network-admin

Parameters

group-number: Assigns an ID to the internal server group. The value range for this argument is 0 to 65535.

Usage guidelines

An internal server group can contain multiple members configured by the **inside ip** command.

Examples

Create internal server group 1.

```
<Sysname> system-view
[Sysname] nat server-group 1
```

Related commands

- **display nat all**
- **display nat server-group**
- **inside ip**
- **nat server**

nat server rule move

Use **nat server rule move** to modify the priority of an ACL-based NAT server rule.

Syntax

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

Interface view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of a NAT rule to be moved.

after: Moves NAT rule *nat-rule-name1* to appear behind NAT rule *nat-rule-name2*.

before: Moves NAT rule *nat-rule-name1* to appear in front of NAT rule *nat-rule-name2*.

nat-rule-name2: Specifies the name of a NAT rule to be moved.

Usage guidelines

This command takes effect only on an ACL-based NAT server rule that has a name.

After you change the order of the ACL-based NAT server rules by executing this command, the priorities of these NAT rules also changes.

- If you execute the **nat server rule move** *nat-rule-name1* **after** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes to be greater than that of NAT rule *nat-rule-name2* by 1.
- If you execute the **nat server rule move** *nat-rule-name1* **before** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes to be smaller than that of NAT rule *nat-rule-name2* by 1.

A rule with a high priority takes precedence over a rule with a low priority for packet matching.

Examples

Move ACL-based NAT server rule **abc** to appear in front of ACL-based NAT server rule **def**.

```
<Sysname> nat server rule move abc before def
```

Related commands

nat server

nat static enable

Use **nat static enable** to enable static NAT on an interface.

Use **undo nat static enable** to disable static NAT on an interface.

Syntax

nat static enable

undo nat static enable

Default

Static NAT is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Static NAT mappings take effect on an interface only after static NAT is enabled on the interface.

Examples

Configure an outbound static NAT mapping between private IP address 192.168.1.1 and public IP address 2.2.2.2, and enable static NAT on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] nat static enable
```

Related commands

- **display nat all**
- **display nat static**
- **nat static**
- **nat static net-to-net**

nat static inbound

Use **nat static inbound** to configure a one-to-one mapping for inbound static NAT.

Use **undo nat static inbound** to remove a one-to-one mapping for inbound static NAT.

Syntax

nat static inbound *global-ip* [**acl** { *acl-number* | **name** *acl-name* } [**reversible**]] *local-ip* [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static inbound *global-ip* [**acl** { *acl-number* | **name** *acl-name* }]

Default

No NAT mapping exists.

Views

System view

Predefined user roles

network-admin

Parameters

global-ip: Specifies a public IP address.

acl: Specifies an ACL to identify packets that can be translated by using the mapping.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal hosts to the external host. It uses the mapping to translate the destination address for packets of these connections if the packets are permitted by ACL reverse matching.

local-ip: Specifies a private IP address.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the one-to-one inbound static mapping. If you do not specify this keyword, the mapping is enabled.

Usage guidelines

When the source IP address of a packet from the public network to the private network matches the *global-ip*, the source IP address is translated into the *local-ip*. When the destination IP address of a packet from the private network to the public network matches the *local-ip*, the destination IP address is translated into the *global-ip*.

- If you do not specify an ACL, the source address of all incoming packets and the destination address of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. The destination address of packets is not translated for connections actively initiated by internal hosts to the external host.
- If you specify both an ACL and the **reversible** keyword, the source address of incoming packets permitted by the ACL is translated. If packets of connections actively initiated by internal hosts to the external host are permitted by ACL reverse matching, the destination address is translated.

ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP address/port in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy inbound static NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure an inbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1
```

Related commands

- **display nat all**
- **display nat static**
- **nat static enable**

nat static inbound net-to-net

Use **nat static inbound net-to-net** to configure a net-to-net mapping for inbound static NAT.

Use **undo nat static inbound net-to-net** to remove a net-to-net mapping for inbound static NAT.

Syntax

nat static inbound net-to-net *global-start-address global-end-address* [**acl** { *acl-number* | **name** *acl-name* } [**reversible**]] **local** *local-network* { *mask-length* | *mask* } [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static inbound net-to-net *global-start-address global-end-address* [**acl** { *acl-number* | **name** *acl-name* }]

Default

No NAT mapping exists.

Views

System view

Predefined user roles

network-admin

Parameters

global-start-address global-end-address: Specifies a public address range which can contain a maximum of 255 addresses. The *global-end-address* must not be lower than *global-start-address*. If they are the same, only one public address is specified.

acl: Specifies an ACL to identify packets that can use NAT rules for address translation.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by internal hosts to the external hosts. It uses the mapping to translate destination addresses for packets of these connections if the packets are permitted by ACL reverse matching.

local-network: Specifies a private network address.

mask-length: Specifies the mask length of the private network address, in the range of 8 to 31.

mask: Specifies the mask of the private network address.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the net-to-net inbound static mapping. If you do not specify this keyword, the mapping is enabled.

Usage guidelines

Specify a public network through a start address and an end address, and a private network through a private address and a mask.

The public end address cannot be greater than the greatest IP address in the subnet determined by the public start address and the private network mask. For example, if the private address is 2.2.2.0 with a mask 255.255.255.0 and the public start address is 1.1.1.100, the public end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When the source IP address of an incoming packet matches the public address range, the source IP address is translated into a private address in the private address range. When the destination IP address of a packet from the private network matches the private address range, the destination IP address is translated into a public address in the public address range.

- If you do not specify an ACL, the source addresses of all incoming packets and the destination addresses of all outgoing packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source addresses of incoming packets permitted by the ACL are translated. The destination addresses of packets are not translated for connections actively initiated by internal hosts to the external hosts.
- If you specify both an ACL and the **reversible** keyword, the source addresses of incoming packets permitted by the ACL are translated. If packets of connections actively initiated by internal hosts to the external hosts are permitted by ACL reverse matching, the destination addresses are translated.

ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple inbound static NAT mappings by using the **nat static inbound** command and the **nat static inbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy inbound static NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure an inbound static NAT between public network address 202.100.1.0/24 and private network address 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24
```

Related commands

- **display nat all**
- **display nat static**
- **nat static enable**

nat static inbound rule move

Use **nat static inbound rule move** to modify the priority of a one-to-one static inbound NAT rule.

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of a NAT rule to be moved.

after: Moves NAT rule *nat-rule-name1* to appear behind NAT rule *nat-rule-name2*.

before: Moves NAT rule *nat-rule-name1* to appear in front of NAT rule *nat-rule-name2*.

nat-rule-name2: Specifies the name of a NAT rule to be moved.

Usage guidelines

This command takes effect only on a one-to-one static inbound NAT rule that has a name.

After you change the order of the one-to-one static inbound NAT rules by executing this command, the priorities of these NAT rules also changes.

- If you execute the **nat static inbound rule move** *nat-rule-name1* **after** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes to be greater than that of NAT rule *nat-rule-name2* by 1.
- If you execute the **nat static inbound rule move** *nat-rule-name1* **before** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes to be smaller than that of NAT rule *nat-rule-name2* by 1.

A rule with a high priority takes precedence over a rule with a low priority for packet matching.

Examples

Move one-to-one static inbound NAT rule **abc** to appear in front of one-to-one static inbound NAT rule **def**.

```
<Sysname> nat static inbound rule move abc before def
```

Related commands

nat static inbound

nat static outbound

Use **nat static outbound** to configure a one-to-one mapping for outbound static NAT.

Use **undo nat static outbound** to remove a one-to-one mapping for outbound static NAT.

Syntax

nat static outbound *local-ip* [**acl** { *acl-number* | **name** *acl-name* } [**reversible**]] *global-ip* [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static outbound *local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

Default

No NAT mapping exists.

Views

System view

Predefined user roles

network-admin

Parameters

local-ip: Specifies a private IP address.

acl: Specifies an ACL to identify packets that can use NAT rules for address translation.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by external hosts to the internal host. It uses the mapping to translate the destination address for packets of these connections if the packets are permitted by ACL reverse matching.

global-ip: Specifies a public IP address.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the one-to-one outbound static mapping. If you do not specify this keyword, the mapping is enabled.

Usage guidelines

When the source IP address of an outgoing packet matches the *local-ip*, the IP address is translated into the *global-ip*. When the destination IP address of an incoming packet matches the *global-ip*, the destination IP address is translated into the *local-ip*.

- If you do not specify an ACL, the source address of all outgoing packets and the destination address of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. The destination address of packets is not translated for connections actively initiated by external hosts to the internal host.
- If you specify both an ACL and the **reversible** keyword, the source address of outgoing packets permitted by the ACL is translated. If packets of connections actively initiated by external hosts to the internal host are permitted by ACL reverse matching, the destination address is translated.

ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP address/port in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy outbound static NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure an inbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1
```

Configure outbound static NAT, and allow the internal user 192.168.1.1 to access the external network 3.3.3.0/24 by using the public IP address 2.2.2.2.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound 192.168.1.1 acl 3001 2.2.2.2
```

Related commands

- **display nat all**
- **display nat static**
- **nat static enable**

nat static outbound net-to-net

Use **nat static outbound net-to-net** to configure a net-to-net outbound static NAT mapping.

Use **undo nat static outbound net-to-net** to remove the specified net-to-net outbound static NAT mapping.

Syntax

nat static outbound net-to-net *local-start-address local-end-address* [**acl** { *acl-number* | **name** *acl-name* } [**reversible**]] **global** *global-network* { *mask-length* | *mask* } [**rule** *rule-name*] [**priority** *priority*] [**disable**]

undo nat static outbound net-to-net *local-start-address local-end-address* [**acl** { *acl-number* | **name** *acl-name* }

Default

No NAT mapping exists.

Views

System view

Predefined user roles

network-admin

Parameters

local-start-address local-end-address: Specifies a private address range which can contain a maximum of 255 addresses. The *local-end-address* must not be lower than *local-start-address*. If they are the same, only one private address is specified.

acl: Specifies an ACL to identify packets that can use NAT rules for address translation.

acl-number: Specifies an ACL number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

reversible: Allows reverse address translation. Reverse address translation applies to connections actively initiated by external hosts to the internal hosts. It uses the mapping to translate destination addresses for packets of these connections if the packets are permitted by ACL reverse matching.

global-network: Specifies a public network address.

mask-length: Specifies the mask length of the public network address, in the range of 8 to 31.

mask: Specifies the mask of the public network address.

rule *rule-name*: Specifies the name of a NAT rule. The rule name is a case-insensitive string of 1 to 63 characters. If you do not specify a rule name, the specified NAT rule does not have a name.

priority *priority*: Specifies the priority of a NAT rule. The value range for the *priority* argument is 0 to 65535. The smaller the priority value, the higher the priority. If you do not specify a priority, the priority value is 65535, which is the lowest. For NAT rules of the same type and the same priority, the device uses them to match packets in the order as they are configured.

disable: Disables the net-to-net outbound static mapping. If you do not specify this keyword, the mapping is enabled.

Usage guidelines

Specify a private network through a start address and an end address, and a public network through a public address and a mask.

The private end address cannot be greater than the greatest IP address in the subnet determined by the private start address and the public network mask. For example, the public address is 2.2.2.0 with a mask 255.255.255.0, and the private start address is 1.1.1.100. The private end address cannot be greater than 1.1.1.255, the greatest IP address in the subnet 1.1.1.0/24.

When the source IP address of a packet from the private network matches the private address range, the source IP address is translated into a public address in the public address range. When the destination IP address of a packet from the public network matches the public address range, the destination IP address is translated into a private address in the private address range.

- If you do not specify an ACL, the source addresses of all outgoing packets and the destination addresses of all incoming packets are translated.
- If you specify an ACL and do not specify the **reversible** keyword, the source addresses of outgoing packets permitted by the ACL are translated. The destination addresses of packets are not translated for connections actively initiated by external hosts to the internal hosts.
- If you specify both an ACL and the **reversible** keyword, the source addresses of outgoing packets permitted by the ACL are translated. If packets of connections actively initiated by external hosts to the internal hosts are permitted by ACL reverse matching, the destination addresses are translated.

ACL reverse matching works as follows:

- Compares the source IP address/port of a packet with the destination IP addresses/ports in the ACL.
- Translates the destination IP address of the packet according to the mapping, and then compares the translated destination IP address/port with the source IP addresses/ports in the ACL.

Static NAT takes precedence over dynamic NAT when both are configured on an interface.

You can configure multiple outbound static NAT mappings by using the **nat static outbound** command and the **nat static outbound net-to-net** command.

The **vpn-instance** parameter is required if you deploy outbound static NAT for VPNs. The specified VPN instance must be the VPN instance to which the NAT interface belongs.

Examples

Configure an outbound static NAT mapping between private network address 192.168.1.0/24 and public network address 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24
```

Configure outbound static NAT. Allow internal users on subnet 192.168.1.0/24 to access the external subnet 3.3.3.0/24 by using public IP addresses on subnet 2.2.2.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 acl 3001 global 2.2.2.0
24
```

Related commands

- **display nat all**
- **display nat static**
- **nat static enable**

nat static outbound rule move

Use **nat static outbound rule move** to modify the priority of a one-to-one static outbound NAT rule.

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

Views

System view

Predefined user roles

network-admin

Parameters

nat-rule-name1: Specifies the name of a NAT rule to be moved.

after: Moves NAT rule *nat-rule-name1* to appear behind NAT rule *nat-rule-name2*.

before: Moves NAT rule *nat-rule-name1* to appear in front of NAT rule *nat-rule-name2*.

nat-rule-name2: Specifies the name of a NAT rule to be moved.

Usage guidelines

This command takes effect only on a one-to-one static outbound NAT rule that has a name.

After you change the order of the one-to-one static outbound NAT rules by executing this command, the priorities of these NAT rules also changes.

- If you execute the **nat static outbound rule move** *nat-rule-name1* **after** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes be greater than that of NAT rule *nat-rule-name2* by 1.
- If you execute the **nat static outbound rule move** *nat-rule-name1* **before** *nat-rule-name2* command, the priority value of NAT rule *nat-rule-name2* does not change. And the priority value of NAT rule *nat-rule-name1* changes to be smaller than that of NAT rule *nat-rule-name2* by 1.

A rule with a high priority takes precedence over a rule with a low priority for packet matching.

Examples

Move one-to-one static outbound NAT rule **abc** to appear in front of one-to-one static outbound NAT rule **def**.

```
<Sysname> nat static outbound rule move abc before def
```

Related commands

nat static outbound

port-block

Use **port block** to configure port block parameters for a NAT address group.

Use **undo port block** to remove port block configuration from a NAT address group.

Syntax

port block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port block

Default

Port block parameters are not configured for a NAT address group.

Views

NAT address group view

Predefined user roles

network-admin

Parameters

block-size *block-size*: Sets the port block size. The value range for this argument is 1 to 65535. In a NAT address group, the port block size cannot be larger than the number of ports in the port range.

extended-block-number *extended-block-number*: Specifies the number of extended port blocks, in the range of 1 to 5. When a private IP address accesses the public network, but the ports in the selected port block are all occupied, the NAT444 gateway extends port blocks one by one for the private IP address.

Usage guidelines

With dynamic NAT444 configured, when a private IP address initiates a connection to the public network, the NAT444 gateway assigns it a public IP address and a port block, and creates an entry for the mapping. For subsequent connections from the private IP address, the NAT444 gateway translates the private IP address to the mapped public IP address and the ports to ports in the selected port block.

Examples

Set the port block size to 256 and the number of extended port blocks to 1 for NAT address group 2.

```
<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1
```

Related commands

nat address-group

port-range

Use **port-range** to specify a port range for public IP addresses.

Use **undo port-range** to restore the default.

Syntax

port-range *start-port-number end-port-number*

undo port-range

Default

The port range for public IP addresses is 1 to 65535.

Views

NAT address group view

NAT port block group view

Predefined user roles

network-admin

Parameters

start-port-number end-port-number: Specifies the start port number and end port number for the port range. The end port number cannot be smaller than the start port number.

Usage guidelines

The port range must include all ports that a public IP address uses for address translation.

The number of ports in a port range cannot be smaller than the port block size.

Examples

Specify the port range as 1024 to 65535 for NAT address group 1.

```
<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-range 1024 65535
```

Specify the port range as 30001 to 65535 for NAT port block group 1.

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-range 30001 65535
```

Related commands

- **nat address-group**
- **nat port-block-group**

reset nat session

Use **reset nat session** to clear NAT sessions.

Syntax

reset nat session [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears NAT sessions for all member devices.

Usage guidelines

After you remove the NAT session, the corresponding NAT EIM table and NO-PAT table are removed at the same time.

Examples

Clear all NAT sessions.

```
<Sysname> reset nat session
```

Related commands

display nat session