

Configuration guide to NAT Destination

Version 1.0
ScreenOS 5.0.0 and higher.

NAT DESTINATION

The objective of the document is to describe step-by-step procedure on how to configure NAT-DST on the Netscreen firewall. This applies to any ScreenOS currently available.

INTRODUCTION:

You can define policies to translate the destination address from one IP address to another. Perhaps you need the NetScreen device to translate one or more public IP addresses to one or more private addresses. The relationship of the original destination address to the translated destination address can be any of the following.

One-to-one mapping maps a single public IP address (as defined in an Address Book entry) to a single private IP address.
- Many-to-one mapping translates a group of public addresses (as defined in an Address Book entry) to a single private IP address.
- Many-to-many mapping translates a group of public addresses (as defined in an Address Book entry) to a contiguous range of private IP addresses, using the address shifting mechanism.
- Port mapping allows you to add port translation to NAT-Dst configurations.

In this document we will be discussing about how to configure a One-to-One relation of a public IP with a private IP using NAT-DST. The same can be accomplished using a MIP on the untrust zone.
Note that when a MIP is configured, the private IP will be translated to the public IP for both incoming and outgoing traffic; whereas when NAT-Dst is configured in a policy, the translation is only restricted to incoming traffic
For more configuration examples with different NAT-DST options mentioned above, kindly refer the Concepts and Example guide.

http://www.juniper.net/techpubs/software/screenos/screenos5.2.0/CE_v7.pdf

REQUIREMENTS for NAT-DST:

1. In order for NAT-Dst to work, the public address needs to be “mapped” to the correct internal/private zone. You can accomplish this through either:

- Configuring the public address as a secondary address on one of the internal interfaces on which the server or computer is installed which is used for NAT-DST. (Refer step 4 (a) in the CLI configuration)

- By configuring a static route to the public address range with the Outbound interface being one of the internal interfaces as explained previously. (Refer step 4 in the WEBUI / CLI configuration)

2. Additionally, the addresses to be translated need to be configured as address book entries in the internal zone. It is not possible to use "any" as the pre-translation destination when using NAT-Dst.
   (Refer step 2 in the WEBUI / CLI configuration)

3. Ensure proper routing is configured from the ISP to direct traffic to the firewall for any Request coming in to the NAT-DST public address.

4. The original destination IP address and the translated destination IP address must be in the same security zone.

NAT-DST Configuration Procedure:

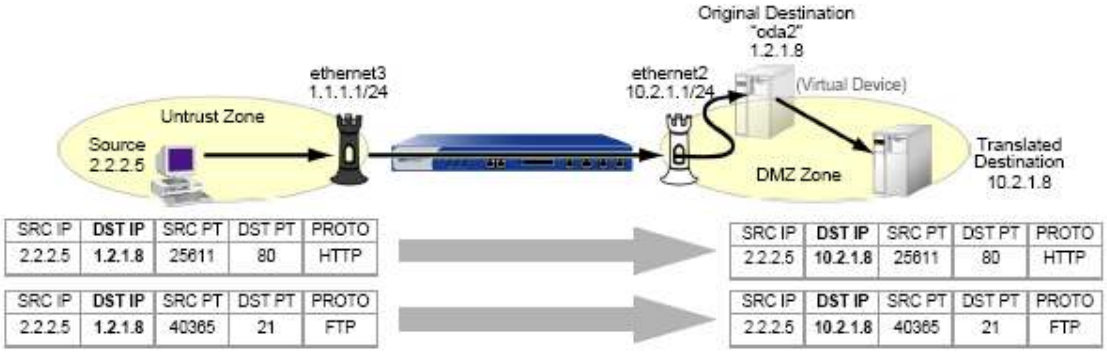
1. Configure Address book entry for public address (es).
2. Configure Route / reachability.
   a) Secondary Interface address
   b) Static Route.
3. Configure Policy.
   a) Single post-translation address (xxx to one)
   b) Multiple post-translation address (xxx to many)
   c) Port Mapping.

Example: One-to-One Destination Translation:

In this example, you set a policy to provide one-to-one destination network address translation (NAT-Dst) without changing the destination port addresses. The policy instructs the NetScreen device to perform the following tasks:

• Permit both FTP and HTTP traffic (defined as the service group "http-ftp") from any address in The Untrust zone to a the original destination address named "oda2" with address 1.2.1.8 in the DMZ zone
• Translate the destination IP address in the IP packet header from 1.2.1.8 to 10.2.1.8
• Leave the original destination port number in the TCP segment header as is (80 for HTTP, and 21 for FTP)
• Forward HTTP and FTP traffic to 10.2.1.8 in the DMZ zone

You bind ethernet3 to the Untrust zone, and assign it IP address 1.1.1.1/24. You bind ethernet2 to the DMZ, and assign it IP address 10.2.1.1/24. You also define a route to the original destination address 1.2.1.8 through ethernet2. Both the Untrust zone and the DMZ zone are in the trust-vr routing domain.



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:
Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:
Zone Name: DMZ
Static IP: (select this option when present)
IP Address/Netmask: 10.2.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following information, and then click **OK**:
Address Name: oda2
IP Address/Domain Name:
IP/Netmask: (select), 1.2.1.8/32
Zone: DMZ

3. Service Group

Objects > Services > Group: Enter the following group name, move the following services, and then click **OK**:
Group Name: HTTP-FTP
Select **HTTP** and use the **<<** button to move the service from the Available Members column to the Group Members column.
Select **FTP** and use the **<<** button to move the service from the Available Members column to the Group Members column.

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:
Network Address / Netmask: 1.2.1.8/32
Gateway: (select)
Interface: ethernet2
Gateway IP Address: 0.0.0.0

5. Policy

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:
Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), oda2
Service: HTTP-FTP
Action: Permit

> Advanced: Enter the following, and then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Destination Translation: (select)
Translate to IP: (select), 10.2.1.8
Map to Port: (clear)

CLI:

1. Interfaces

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. Address

```
set address dmz oda2 1.2.1.8/32
```

3. Service Group

```
set group service http-ftp
set group service http-ftp add http
set group service http-ftp add ftp
```

4. Route

```
set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
```

a) Secondary IP on the Interface

```
set interface ethernet2 ip 1.2.1.0/24 secondary
```

5. Policy

```
set policy from untrust to dmz any oda2 http-ftp nat dst ip 10.2.1.8
permit
save
```

Verifying Nat-DST-WEBUI

You can verify that translation has been added to the policy by looking at the action icon. A blue checkmark indicates that translation has been added via the advanced policy options.
The logging feature only captures source translation, so no destination translation will be visible via the WebUI

Verifying Nat-DST-CLI

Using the CLI, you can verify that translation has been added to the policy.

ns5gt-> get pol id 2
name:"none" (id 2), zone Untrust -> DMZ,action Permit, status "enabled"
src "Any", dst "oda2", serv "http-ftp"
Policies on this vpn tunnel: 0
nat dst map to 10.2.1.8, serv_timeout 0 (minute)
vpn unknown vpn, policy flag 00000000, session backup: on

traffic shapping off, scheduler n/a, serv flag 00
log no, log count 0, alert no, counter no(0) byte rate(sec/min) 0/0
total octets 0, counter(session/packet/octet) 0/0/0
priority 7, diffserv marking Off
tadapter: state off, gbw/mbw 0/-1
No Authentication
No User, User Group or Group expression set
ns5gt->

You can also view any currently established sessions and the associated translation with the **get session** command.
Note in this example that the destination IP address 1.2.1.8 is translated to the IP address 10.2.1.8:

ns5gt-> get session
alloc 3/max 2064, alloc failed 0, mcast alloc 0, di alloc failed 0
id 2061/s,vsys 0,flag 00000040/0080/21,policy 320000,time 180, dip 0**
3(0011):2.2.2.5/25611->1.2.1.8/80,6,000000000000,8,vlan 0,tun 0,vsd 0,route 2
2(100600):2.2.2.5/25611<-10.2.1.8/80,6,0003ba5ba68f,4,vlan 0,tun 0,vsd 0,route 1
Total 1 sessions shown

ns5gt-> get session
alloc 3/max 2064, alloc failed 0, mcast alloc 0, di alloc failed 0
id 2061/s,vsys 0,flag 00000040/0080/21,policy 320000,time 180, dip 0**
3(0011):2.2.2.5/40365->1.2.1.8/21,6,000000000000,8,vlan 0,tun 0,vsd 0,route 2
2(100600):2.2.2.5/40365<-10.2.1.8/21,6,0003ba5ba68f,4,vlan 0,tun 0,vsd 0,route 1
Total 1 sessions shown.