



Understanding and Configuring NAT

Tech Note

PAN-OS 4.1

Contents

Overview	3
Scope	3
Design Consideration.....	3
Software requirement	3
Hardware requirement	3
NAT with PAN-OS	3
Life of a packet	4
Address Pools.....	5
Proxy-ARP for NAT Pools	5
Source NAT	5
Dynamic-ip-and-port.....	5
Dynamic-ip.....	5
Source NAT examples	6
Case 1: Source NAT IP Address and Port Translation.....	6
<i>Case 1a: Using the Interface IP Address for Translation</i>	<i>6</i>
<i>Case 1b: Using an Address Object for Translation.....</i>	<i>8</i>
Case 2: Source NAT IP Address Translation	9
Reserving IP Addresses	11
Static NAT: Bi-directional Translation	11
Destination NAT	15
Case1: One-to-one mapping.....	15
Case 2: Destination IP and Port Translation	19
Case 3: One-to-Many Mapping.....	20
Case 4: Server Access for Internal Users or U-turn NAT	22
Case 5: Server in the Same Zone as the Clients	23
Translating source and destination IP address	24
Virtual Wire NAT	26
Source NAT	26
Static NAT	27
Destination NAT.....	28
NAT with IPSec VPN	29
Verifying NAT rules	29
NAT Exemptions.....	29
NAT interaction with applications	30
Summary.....	30
Revision History.....	30

Overview

Network address translation (NAT) was designed to address the depletion of the IPv4 address space. Since then NAT is not only used to conserve available IP addresses, but also as a security feature to hide the real IP addresses of hosts, securely providing private LAN users access to the public addresses. NAT is also sometimes used to solve network design challenges, enabling networks with identical IP subnets communicate with each other.

Scope

The purpose of this application note is to explain Palo Alto Networks PAN-OS NAT architecture, and to provide several common configuration examples. This paper assumes that the reader is familiar with NAT and how it is used in both service provider and enterprise networks.

Design Consideration

Software requirement

Virtual wire NAT requires PAN-OS 4.1

Hardware requirement

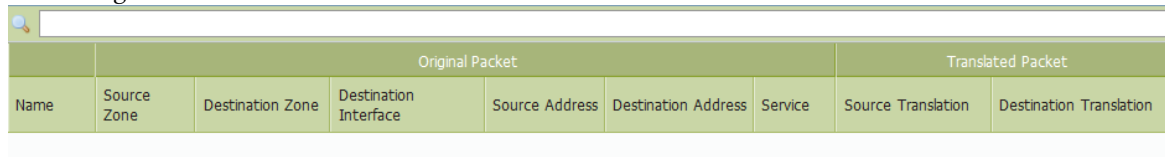
PA-5000, PA-4000, PA-2000 and PA-500 series of firewalls

NAT with PAN-OS

PAN-OS provides a mechanism for translating both the source IP addresses/port numbers and destination IP addresses/port numbers. PAN-OS uses rules to configure NAT. These rules are separate entities, and not configured as part of the allow/drop security rules. NAT rules are configured to match on:

- Source and destination zone
- Destination interface (optional)
- Source and destination addresses
- Service

The configurable fields in the NAT rule are as follows:

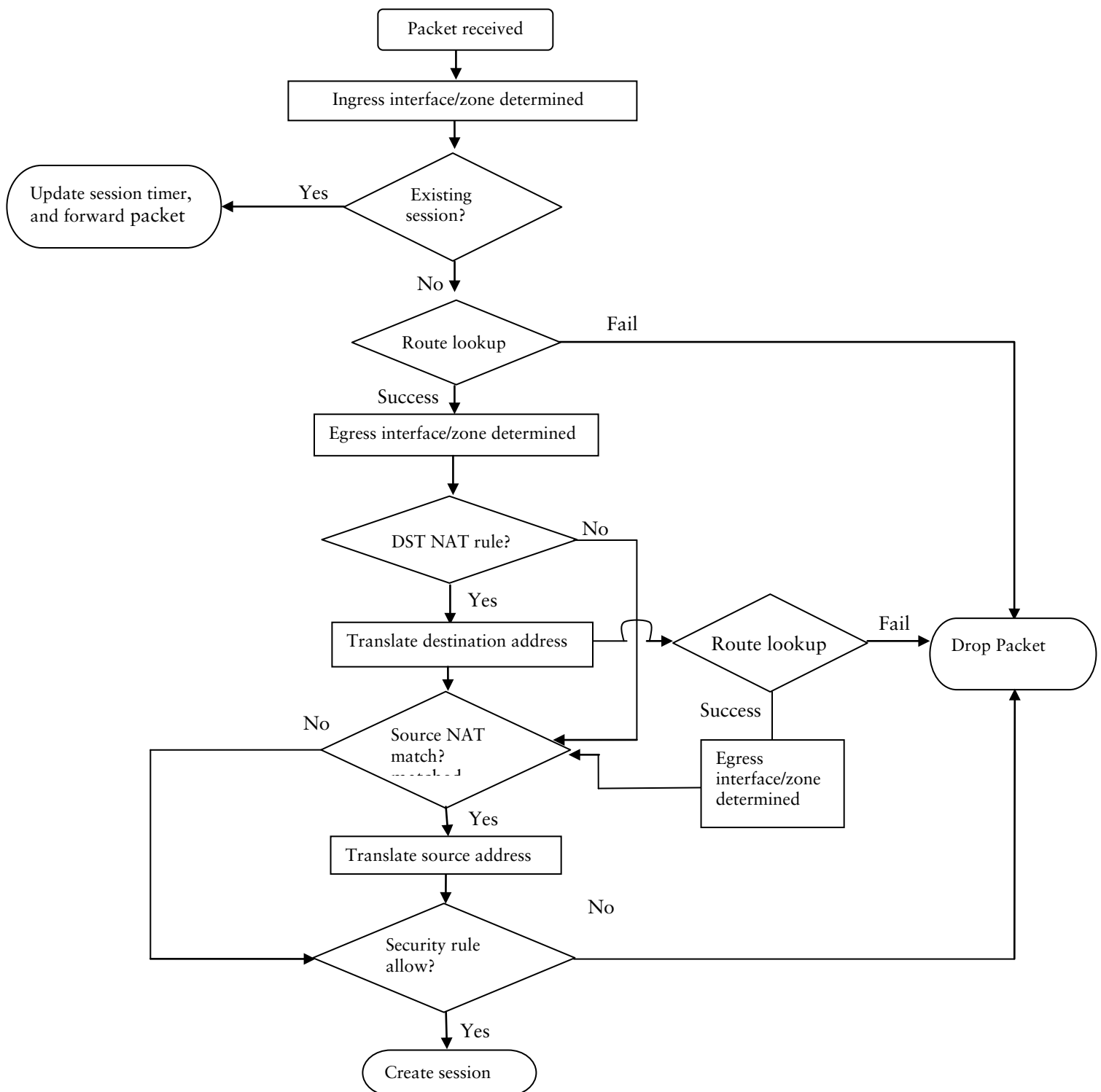


	Original Packet						Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation

There can be multiple NAT rules configured on a PAN-OS device. NAT rules are evaluated top down like security rules. Once a packet matches a NAT rule, any other NAT rules configured are skipped for processing. Therefore, more specific NAT rules must be at the top to the rule list.

Life of a packet

The following diagram captures the packet processing sequence when NAT is involved. For the sake of simplicity the APP-ID, Content- ID and User- ID processing is not shown in the flow chart.



The translated addresses are determined after a packet matches the NAT rule. It is very important to note that the IP address and port translation happens only when the packet egresses the firewall. Hence the NAT rules and security rules always refer to the original IP addresses in the packet (i.e. the pre-NAT addresses).

Address Pools

In PAN-OS, the IP address (also commonly referred to as IP address pools) used for address translation is configured as an address object. The address object can be a host IP address, IP subnet or IP address range. Because the address objects are used both in the security policies and NAT rules, it is recommended to use names that identify the address objects specifically used as NAT address pools. For example the names of address objects used in NAT rules begin with prefix “NAT-<name>”.

Proxy-ARP for NAT Pools

The address pools are not bound to any interfaces. If the address pool is in the same subnet as the egress/ingress interface IP address, the firewall will respond to ARP requests received on that interface for the IP addresses configured in the pool. If the address pool is not in the same subnet as the egress interface IP address, you must configure the necessary routes on the upstream devices in order to ensure the response traffic after address translation is routed back to the firewall.

Source NAT

PAN-OS supports the following options for source translation:

- Dynamic-ip-and-port
- Dynamic-ip
- Static IP

Dynamic-ip-and-port

This method allows for translation of the source IP address and port numbers to:

- Interface IP address
- IP address
- IP subnet
- Range of IP addresses

Dynamic-ip

This method allows for translation of only the source IP address to:

- IP address
- IP subnet, or
- Range of IP addresses

The size of the dynamic-ip pool defines the number of the hosts that can be translated. If all the IP addresses in the dynamic-ip pool are used, any new connections that require address translation will be dropped. As sessions terminate, and IP addresses in the pool become available, these addresses can be used to translate new connections.

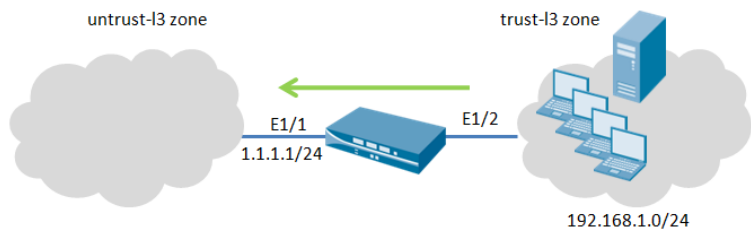
Note: Dynamic-IP does not guarantee IP addresses reservation by default.

Source NAT examples

We shall discuss different scenarios where source NAT can be used to translate the source IP address and/or port numbers. Because the security policies always match the original IP address in the IP packet, for the sake of simplicity a generic security policy between the zones trust-l3 and untrust-l3 is applied to the device for all NAT configuration used in this document unless otherwise noted.

Source					Destination							
Name	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options	
rule1	trust-l3	any	any	any	untrust-l3	any	any	any		none		

Topology



Case 1: Source NAT IP Address and Port Translation

For translating both the source IP address and port numbers “dynamic-ip-and-port” type of translation must be used. This form of NAT is also commonly referred to as interface-based NAT or network address port translation (NAPT).

Case 1a: Using the Interface IP Address for Translation

In this example all the traffic from the subnet 192.168.1.0/24 is translated to the egress interface ethernet1/1 IP address 1.1.1.1/24:

Configuration

The NAT rule for this configuration would look as follows:

Original Packet							Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Int Source NAT	trust-l3	untrust-l3	none	Net-192-1	any	any	dynamic-ip-and-port ethernet1/1 1.1.1.1/24	none

Source Translation

IP Type

Dynamic IP and Port

Address Type

Interface Address

Interface

ethernet1/1

IP Type

IP

1.1.1.1/24

OK

Cancel

Verification

The `show session` command can be used to view the session table. Notice that the source IP address and port of the hosts 192.168.1.250 and 192.168.1.100 are both translated to the interface IP 1.1.1.1 and to unique port numbers:

```
admin@PA-5060> show session all
```

ID	Application	State	Type	Flag	Src[Sport]/Zone/Proto (translated IP[Port])	Dst[Dport]/Zone (translated IP[Port])
2359304	ssh	ACTIVE	FLOW	NS	192.168.1.250[59534]/trust-l3/6	(1.1.1.1[50219])
vsys1					1.1.1.10[22]/untrust-l3	(1.1.1.10[22])
2359303	ssh	ACTIVE	FLOW	NS	192.168.1.100[50034]/trust-l3/6	(1.1.1.1[51650])
vsys1					1.1.1.10[22]/untrust-l3	(1.1.1.10[22])

```
admin@PA-5060>
```

The `show session id` command can be used to view more details about the session. Note in the server to client flow, the response is to the IP address 1.1.1.1 on port 50219, which is the translated address of the host 192.168.1.250:

```
admin@PA-5060> show session id 2359304
```

```
Session          2359304
```

```
  c2s flow:
```

```
    source:      192.168.1.250 [trust-l3]
    dst:         1.1.1.10
    proto:       6
    sport:       59534           dport:      22
    state:       ACTIVE         type:        FLOW
    src user:    unknown
    dst user:    unknown
```

```
  s2c flow:
```

```
    source:      1.1.1.10 [untrust-l3]
    dst:         1.1.1.1
    proto:       6
    sport:       22             dport:      50219
    state:       ACTIVE         type:        FLOW
    src user:    unknown
    dst user:    unknown
```

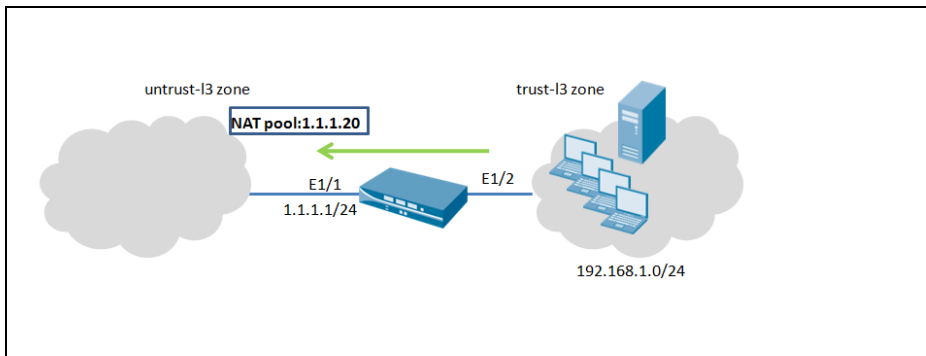
```
  start time      : Fri Apr  8 10:26:33 2011
  timeout         : 432000 sec
  time to live    : 431845 sec
  total byte count : 5686
```

```
_____ output truncated _____
```

Case 1b: Using an Address Object for Translation

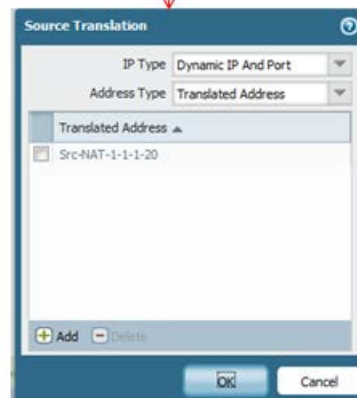
You can also translate the source IP address and port numbers to a single IP address instead of using the egress interface IP address. In this example all the traffic from the subnet 192.168.1.0/24 will be translated to the IP address 1.1.1.20.

Configuration:



An address object referring to the NAT IP address of 1.1.1.20 must be created as shown in the following rule:

Original Packet							Translated Packet	
Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Int Source NAT	trust-l3	untrust-l3	none	Net-192-	any	any	dynamic-ip-and-port Src-NAT-1-1-1-20	none

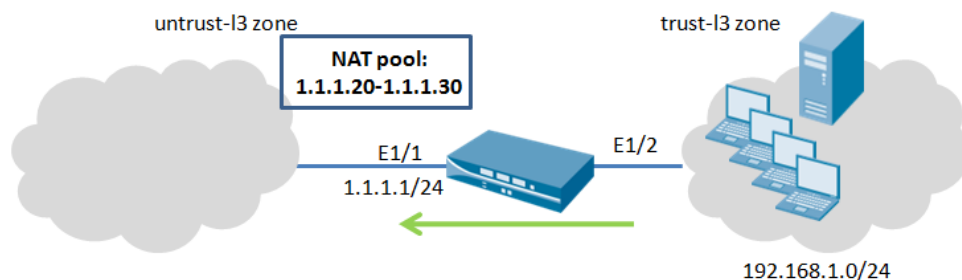


```
admin@PA-5060> show session all
```

```
-----
ID      Application  State  Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys
-----
2359306 ssh          ACTIVE FLOW  NS    192.168.1.250[50964]/trust-l3/6  (1.1.1.20[7987])
vsys1
2359305 ssh          ACTIVE FLOW  NS    192.168.1.100[50426]/trust-l3/6  (1.1.1.20[43853])
vsys1
admin@PA-5060>
```

Note: You can also use a pool of IP addresses for dynamic-ip-and-port source translation.

Case 2: Source NAT IP Address Translation



For translating only the source IP address, the “dynamic-ip” type of source translation must be used. In this form of NAT, the original source port number is left intact. Only the source IP address will be translated.

Note: When using the dynamic-ip type of source NAT, the size of the NAT pool must be equal to the number of the internal hosts that require address translation. If all the IP addresses in the pool are in use, any connections from new hosts cannot be address translated and hence will be dropped. New sessions from hosts with established sessions with NAT will be allowed.

Configuration:

In this example an address pool of eleven IP addresses is created. The address pool is defined as an address object as follows:

Network>address

The NAT rule would look as follows:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Int Source NAT	trust-l3	untrust-l3	none	Net-192.168.1.0/24	any	any	dynamic-ip Src-NAT-pool	none

Verification

Run the `show session` command; note that the source port is not translated:

```
admin@PA-5060> show session all
```

ID	Application	State	Type	Flag	Src[Sport]/Zone/Proto (translated IP[Port])	Dst[Dport]/Zone (translated IP[Port])
2359311	ssh	ACTIVE	FLOW	NS	192.168.1.100[51298]/trust-13/6	(1.1.1.21[51298])
vsys1					1.1.1.10[22]/untrust-13	(1.1.1.10[22])
2359310	ssh	ACTIVE	FLOW	NS	192.168.1.250[43409]/trust-13/6	(1.1.1.20[43409])
vsys1					1.1.1.10[22]/untrust-13	(1.1.1.10[22])

Troubleshooting tip:

If all the addresses in the pool are in use, any new connections will not be translated and instead the packets will be dropped. Use the following command to see if any sessions have failed due to NAT IP allocation:

```
show counter global filter aspect session severity drop | match nat
```

Debug output from a NAT allocation failure is shown below:

```
Packet received at slowpath stage
Packet info: len 74 port 17 interface 1
  wqe index 229345 packet 0x0x8000000416fef0e6
Packet decoded dump:
L2:    00:15:17:dd:9f:bb->00:1b:17:2c:c2:01, type 0x0800
IP:    192.168.1.250->1.1.1.10, protocol 6
      version 4, ihl 5, tos 0x00, len 60,
      id 49401, frag_off 0x4000, ttl 64, checksum 46357
TCP:   sport 49099, dport 22, seq 3586889157, ack 0,
      reserved 0, offset 10, window 5840, checksum 61035,
      flags 0x0002 ( SYN), urgent data 0
TCP option:
00000000: 02 04 05 b4 04 02 08 0a  fd 67 55 3c 00 00 00 00  ....
.gU<....
00000010: 01 03 03 07                ....
Session setup: vsys 1
PBF lookup (vsys 1) with application ssh
Session setup: ingress interface vlan egress interface ethernet1/1 (zone 5)
NAT policy lookup, matched rule index 0
Policy lookup, matched rule index 0
```

DP2 is selected to process this session.

Allocated new session 203.

Packet dropped, source NAT IP/port allocation failed

Packet dropped, Session setup failed

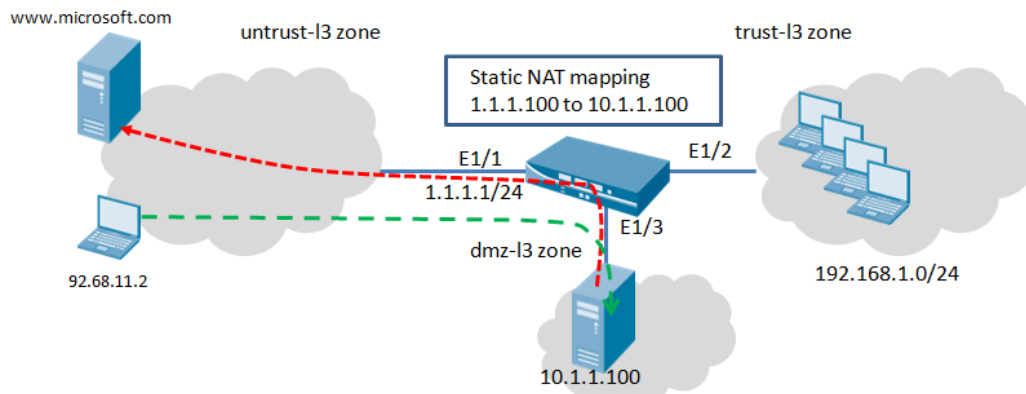
Reserving IP Addresses

Dynamic-IP address pools can be configured to reserve IP addresses for translation. By default, the IP reservation setting, `reserve-ip`, is disabled. If `reserve-ip` is set to yes, `reserve-time` must also be set to a value between 1-604800 seconds (30 days). If set, the dynamic IP rules will support reserving an IP address up to the user specified reserve-time after all sessions of that original source IP address translation expire. For example, if `reserve-time` is set to 8 hours, when the last session of the original source IP expires, the translated IP will be reserved for another 8 hours. During this time the IP address is “reserved” for the original source IP address. This means that other hosts will not be able to get a translated IP address from the pool even if there are active sessions because all translated IP addresses are reserved. IP reservation is configured from the CLI as follows:

```
set setting nat reserve-ip <yes/no>
set setting nat reserve-time < 1-604800 secs>
```

Static NAT: Bi-directional Translation

Static NAT is used for translating a range of IP addresses or a subnet to another IP address range or subnet. The size of the static NAT pool must be same as the size of the source addresses to be translated. Static NAT also offers the benefit of bi-directional translation, where the destination IP can also be translated for inbound connections. Static NAT is commonly used to access servers behind a firewall from the outside. The following diagram shows static NAT use case.



The server 10.1.1.100 is mapped to IP 1.1.1.100. With a static NAT configuration, all connections initiated from the server will be translated to 1.1.1.100 as follows:

Src IP	Dst IP	Src Port	Dst Port	Data
1.1.1.100	updates.microsoft.com	2020	443	



Src IP	Dst IP	Src Port	Dst Port	Data
10.1.1.100	updates.microsoft.com	2020	443	

If the bi-directional setting is configured for static NAT, then all connections to the IP address of 1.1.1.100 will be translated to the real IP address of the server 10.1.1.100:

Src IP	Dst IP	Src Port	Dst Port	Data
92.68.11.2	1.1.1.100	4200	443	



Src IP	Dst IP	Src Port	Dst Port	Data
92.68.11.2	10.1.1.100	4200	443	

Configuration:

In this example, the server 10.1.1.100 is mapped to IP 1.1.1.100. Static NAT is configured for bi-directional NAT. The following address objects are required for this setup:

- Address object for the real IP address of the server
- Address object for the translated IP address of the server

The following shows the configured address objects on the firewall:

	Name	Type	Address
<input checked="" type="checkbox"/>	Internal-Server-1	IP Netmask	10.1.1.100
<input type="checkbox"/>	Net-192-168-1-0	IP Netmask	192.168.1.0/24
<input type="checkbox"/>	static-nat-server	IP Netmask	1.1.1.100

The NAT rules would look as follows. Note that the NAT rule “Int Source NAT” is required for translating hosts other than 10.1.1.100:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Static NAT	dmz-l3	untrust-l3	none	Internal-Serv	any	any	static-ip static-nat-server bi-directional: yes	none
Int Source NAT	trust-l3	untrust-l3	none	Net-192-168-	any	any	dynamic-ip-and-port ethernet1/1	none

Source Translation

IP Type: Static IP

Translated Address: static-nat-server

Bi-directional: yes

OK Cancel

Configuration Tip: Static NAT does not have precedence over other forms of NAT. Therefore the order of the NAT rules is very important. For static NAT to work, the static NAT rules must be above all configured NAT rules

Security Policy configuration

For outbound access from the host 10.1.1.100, the generic security policy to permit any from the dmz-l3 zone to the untrust-l3 zone is required. In order to allow inbound access from outside hosts, the security policy must match the following:

1. Source and destination IP address as seen in the original packet
2. Source zone: Incoming zone of the packet to the server
3. Destination zone: zone where the server is physically connected

The configured security policy to provide access to the server from the untrust-l3 zone would look as follows:

Name	Source				Destination		Applicatio	Service	Action
	Zone	Address	User	HIP Profile	Zone	Address			
Internet acc	trust-l3	any	any	any	untrust-l3	any	any	any	✓
Server Acces	untrust-l3	any	any	any	dmz-l3	static-nat-server	any	any	✓

Configuration Tip: The destination address in the policy is 1.1.1.100 and NOT 10.1.1.100.

Verification

The connection initiated from host 10.1.1.100 is translated to 1.1.1.100. The port numbers remain unchanged.

```
admin@PA-5060> show session all
```

```
-----  
ID      Application  State  Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])  
Vsys                                         Dst[Dport]/Zone (translated IP[Port])  
-----  
2359314 ssh          ACTIVE  FLOW  NS    10.1.1.100[54121]/dmz-13/6 (1.1.1.100[54121])  
vsys1                                         1.1.1.10[22]/untrust-13 (1.1.1.10[22])  
admin@PA-5060>
```

In the following connection from host 1.1.1.10 to 1.1.1.100, the destination IP address is translated to 10.1.1.100.

```
admin@PA-5060> show session all
```

```
-----  
ID      Application  State  Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])  
Vsys                                         Dst[Dport]/Zone (translated IP[Port])  
-----  
524291  ssh          ACTIVE  FLOW  ND    1.1.1.10[60616]/untrust-13/6 (1.1.1.10[60616])  
vsys1                                         1.1.1.100[22]/dmz-13 (10.1.1.100[22])
```

Note: The bi-directional option in the static NAT configuration must be enabled for the outside host 1.1.1.10 to access the server. This function creates a hidden NAT rule, allowing the destination translation to the static NAT host.

```
admin@PA-5060> show running nat-policy
```

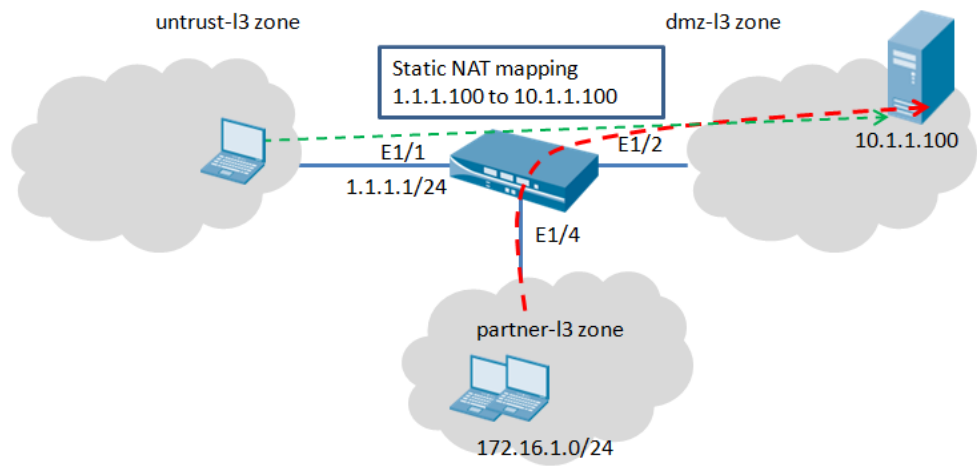
```
"Static NAT" {  
    from dmz-13;  
    source 10.1.1.100;  
    to untrust-13;  
    to-interface ;  
    destination any;  
    service any/any;  
    translate-to "src: 1.1.1.100 (static-ip) (pool idx: 2)";  
}
```

```
"Static NAT" {  
    from any;  
    source any;  
    to untrust-13;  
    to-interface ;  
    destination 1.1.1.100;  
    service any/any;  
    translate-to "dst: 10.1.1.100";  
}
```

System generated NAT rule

With these settings, connections from any zone to the server are permitted. This requires creating the security policy to allow traffic to the destination zone where the server is connected.

In the following topology, in order to allow hosts from “partner-l3” zone to access the server, the security policy in the previous configuration is modified to allow connections from any host in the “partner-l3” zone.



The modified security policy would look as follows:

Name	Source				Destination		Applicatio	Service	Action
	Zone	Address	User	HIP Profile	Zone	Address			
Internet acc	trust-l3	any	any	any	untrust-l3	any	any	any	✓
Server Acces	partner-l3	any	any	any	dmz-l3	static-nat-server	any	any	✓
	untrust-l3								

Verification

```
admin@PA-5060> show session all

-----
ID      Application  State  Type  Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                         Dst[Dport]/Zone (translated IP[Port])
-----
524297  ssh           ACTIVE FLOW  ND    172.16.1.10[56970]/partner-13/6 (172.16.1.10[56970])
vsys1                                     1.1.1.100[22]/dmz-13 (10.1.1.100[22])
524298  ssh           ACTIVE FLOW  ND    1.1.1.10[46504]/untrust-13/6 (1.1.1.10[46504])
vsys1                                     1.1.1.100[22]/dmz-13 (10.1.1.100[22])
admin@PA-5060>
```

Destination NAT

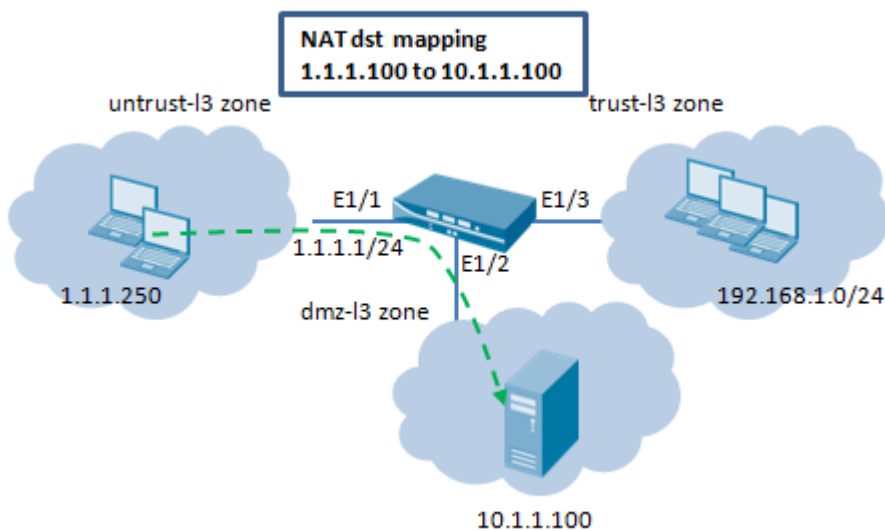
Destination NAT is used to translate the destination IP address and/or the destination IP address and port number of packet. This form of NAT can also be used to map one IP address to multiple internal host IP addresses. In this case, the destination port numbers are used to identify the destination host.

NAT and Security Rule Interaction with Destination NAT

The most common mistake in configuring the NAT and security rules are the references to the zones and address objects. The addresses used in destination NAT rules always refer to the original IP address in the packet (i.e. the pre-translated address). The destination zone in the NAT rule is determined after the route lookup of the destination IP address on the original packet (i.e. the pre-NAT destination IP address).

The addresses in the security policy also refer to the IP address in the original packet (i.e. the pre-NAT address). However, the destination zone is the zone where the end host is physically connected. The other way to look at it is the destination zone in the security rule is determined after the route lookup of the post NAT destination IP address.

Case1: One-to-one mapping



Configuration

In this example, users from zone untrust-l3 access the server 10.1.1.100 in zone dmz-l3 using the IP address 1.1.1.100.

Before configuring the NAT rules, let us walk through the sequence of the events for this flow:



1. Host 1.1.1.250, sends an ARP request for the address 1.1.1.100.
2. The firewall receives the ARP request packet for destination 1.1.1.100 on the interface ethernet1/1 and processes the request. The firewall responds to the ARP request with its own MAC address because of the destination NAT rule configured.
3. The NAT rule is evaluated for a match. For the destination IP address to be translated, a destination NAT rule from zone untrust-l3 to zone untrust-l3 must be created to translate the destination IP of 1.1.1.100 to 10.1.1.100.
4. After the translated address is determined, a route lookup for destination 10.1.1.100 is performed to determine the egress interface. In this example the egress interface will be ethernet1/2 in zone dmz-l3.
5. A security policy lookup is performed to see if the traffic is permitted from zone untrust-l3 to dmz-l3. It is important to note, the direction of the policy matches the ingress zone and the zone where the server is physically located. Also note that the security policy refers to the IP addresses in the original packet, which has a destination address of 1.1.1.100.
6. The packet is then forwarded out to the server via the egress interface ethernet1/2. The destination address is changed to 10.1.1.100 as the packet leaves the firewall.

Configuration




The following address objects are required for this setup:

- Address object for the real IP address of the server
- Address object for the translated IP address of the server

The configured address objects would look like this:

	Name	Type	Address
	webserver-private	IP Netmask	10.1.1.100
	Webserver-public	IP Netmask	1.1.1.100

And the configured NAT rules would look like this:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-webse	 untrust-I3	 untrust-I3	none	any	 Webserver-public	any	none	address: webserver-private

Configuration tip: The direction of the NAT rules is based on the result of route lookup. Also note that the security policy refers to the IP addresses in the original packet, which has a destination address of 1.1.1.100.

The configured security policy to provide access to the server from the untrust-I3 zone would look as follows:

Name	Source		Destination		Application	Service	Action	Profile	Options
	Zone	Address	Zone	Address					
Webserver acces	 untrust-I3	any	 dmz-I3	 Webserver-pul	 web-browsing	any		none	

Configuration tip: The direction of the security policy matches the ingress zone and the zone where the server is physically located. Also note that the security policy refers to the IP addresses in the original packet, which has a destination address of 1.1.1.100.

Verification

Verify the sender IP address and target IP address in the ARP request packet:

```
Packet received at ingress stage
Packet info: len 60 port 16 interface 16
  wqe index 229341 packet 0x0x8000000416ffe0e0
Packet decoded dump:
L2:    a4:ba:db:ba:3f:07->ff:ff:ff:ff:ff:ff, type 0x0806
ARP:   hardware type 0x0001
       protocol type 0x0800
       hardware size 6
       protocol size 4
       opcode REQUEST
       sender mac address a4:ba:db:ba:3f:07
       sender ip address 1.1.1.250
       target mac address 00:00:00:00:00:00
       target ip address 1.1.1.100
No flow lookup for packet, continue with forwarding
Forwarding lookup, ingress interface 16
L3 mode, virtual-router 1
Enqueue packet to ARP process
```


Flow debug

```
Packet received at fastpath stage
Packet info: len 477 port 16 interface 16
  wqe index 229320 packet 0x0x8000000416fe70e6
Packet decoded dump:
L2:      a4:ba:db:ba:3f:07->00:1b:17:01:4a:10, type 0x0800
IP:      1.1.1.250->1.1.1.100, protocol 6
        version 4, ihl 5, tos 0x00, len 463,
        id 699, frag_off 0x4000, ttl 128, checksum 61710
TCP:     sport 52288, dport 80, seq 3878305383, ack 933869295,
        reserved 0, offset 5, window 63537, checksum 28577,
        flags 0x0018 ( ACK PSH), urgent data 0
TCP option:
Flow fastpath, session 15
NAT session, run address/port translation
session 15 packet sequeunce old 13 new 14

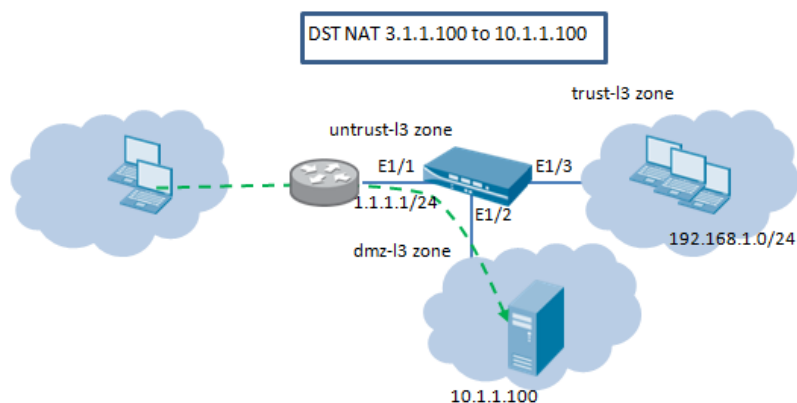
== Jun 07 10:43:07 ==
Packet received at forwarding stage
Packet info: len 477 port 16 interface 16
  wqe index 229333 packet 0x0x8000000416fe70e6
Packet decoded dump:
L2:      a4:ba:db:ba:3f:07->00:1b:17:01:4a:10, type 0x0800
IP:      1.1.1.250->10.1.1.100, protocol 6
        version 4, ihl 5, tos 0x00, len 463,
        id 699, frag_off 0x4000, ttl 128, checksum 59406
TCP:     sport 52288, dport 80, seq 3878305383, ack 933869295,
        reserved 0, offset 5, window 63537, checksum 26273,
        flags 0x0018 ( ACK PSH), urgent data 0
TCP option:
Forwarding lookup, ingress interface 16
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 10.1.1.100
Route found, interface ethernet1/2, zone 19
Resolve ARP for IP 10.1.1.100 on interface ethernet1/2
ARP entry found on interface 17
Transmit packet on port 17
```

```
admin@PA-2050# run show session all
```

ID	Application	State	Type	Flag	Src[Sport]/Zone/Proto (translated IP[Port])	Dst[Dport]/Zone (translated IP[Port])
30	web-browsing	ACTIVE	FLOW	ND	1.1.1.250[53079]/untrust-l3/6 (1.1.1.250[53079])	1.1.1.100[80]/dmz-13 (10.1.1.100[80])

Case 1a:

In this example, the firewall is configured to use a destination NAT IP address that does not belong to any of its connected interfaces. The upstream router must be configured to route the traffic to the destination NAT address to the firewall. In this example, the traffic to destination 3.1.1.100 must be routed to the firewall for address translation.



The following is a snapshot of the routing table on the firewall:

```
admin@PA-2050> show routing fib

total virtual-router shown :          1

-----
virtual-router name: VR1
interfaces:
  ethernet1/1 ethernet1/2 ethernet1/3 tunnel.1
```

```
route table:
flags: u - up, h - host, g - gateway
```

```
maximum of fib entries for device:      5000
number of fib entries for device:        5
maximum of fib entries for this fib:     5000
number of fib entries for this fib:      5
number of fib entries shown:             5
```

id	destination	nexthop	flags	interface	mtu
113	0.0.0.0/0	0.0.0.0	ug	ethernet1/1	1500
112	1.1.1.0/24	0.0.0.0	u	ethernet1/1	1500
111	1.1.1.1/32	0.0.0.0	uh	ethernet1/1	1500
38	10.1.1.0/24	0.0.0.0	u	ethernet1/2	1500
37	10.1.1.1/32	0.0.0.0	uh	ethernet1/2	1500

Before configuring the NAT rules, let us walk through the sequence of the events for this flow:

1. The router forwards the packet with destination IP address 3.1.1.100 to the firewall. The ingress interface for this packet is ethernet1/1, which is in the zone untrust-l3.
2. The firewall does a route lookup to determine the egress interface. The best route match is the default route, route id 113.
3. The packet is then forwarded back on to the interface ethernet1/1. The egress zone for this packet is same as ingress zone: untrust-l3.
4. The NAT rule is evaluated for a match. In order for the destination IP address to be translated, a destination NAT rule from zone untrust-l3 to zone untrust-l3 must be created to translate the destination IP of 3.1.1.100 to 10.1.1.100.

- After the translated address is determined, a route lookup for destination 10.1.1.100 is performed to determine the egress interface. In this example the egress interface will be ethernet1/2 in zone dmz-l3.
- A security policy lookup is performed to see if the traffic is permitted from zone untrust-l3 to dmz-l3. It is important to note, the direction of the policy matches the ingress zone and the zone where the server is physically located. Also note that the security policy refers to the IP addresses in the original packet, which has a destination address of 3.1.1.100.
- The packet is then forwarded out to the server via the egress interface ethernet1/2. The destination address is changed to 10.1.1.100 as the packet leaves the firewall.

Configuration:

This configuration requires the following address objects:

Name	Type	Address
web server public	IP Netmask	3.1.1.100
webserver-private	IP Netmask	10.1.1.100

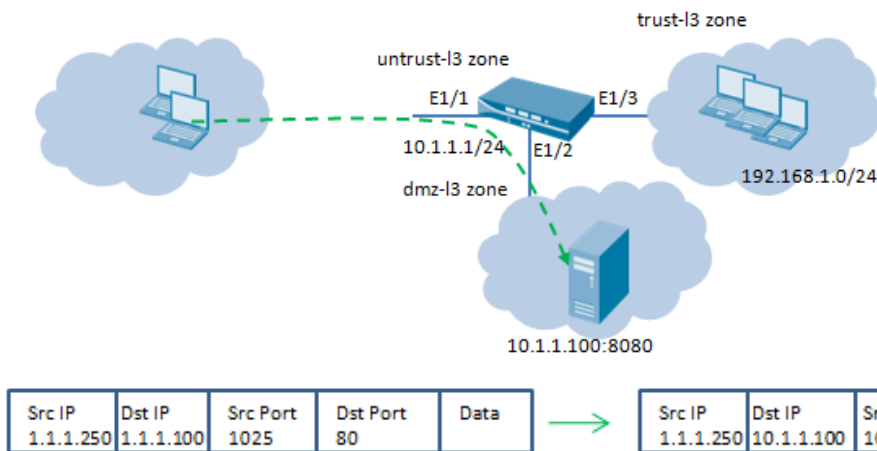
The NAT rules and the security policies are configured similar to Case1:

```
admin@PA-2050> show session all
```

ID	Application	State	Type	Flag	Src[Sport]/Zone/Proto (translated IP[Port])	Dst[Dport]/Zone (translated IP[Port])
146	web-browsing	ACTIVE	FLOW	ND	5.1.1.250[58820]/untrust-l3/6 (5.1.1.250[58820])	3.1.1.100[80]/dmz-l3 (10.1.1.100[80])
vsys1						

Case 2: Destination IP and Port Translation

In this example, the web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 and TCP port 80. The destination NAT rule is configured to translate both IP and port to 10.1.1.100 and TCP port 8080.



Configuration:

The following NAT and security rules must be configured on the firewall:

NAT rule

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-webserver	untrust-l3	untrust-l3	none	any	Servers-public	service-http	none	address: webserver-private port: 8080

Security rule

Name	Source		Destination		Application	Service
	Zone	Address	Zone	Address		
Webserver access	untrust-l3	any	dmz-l3	Servers-public	web-browsing	any

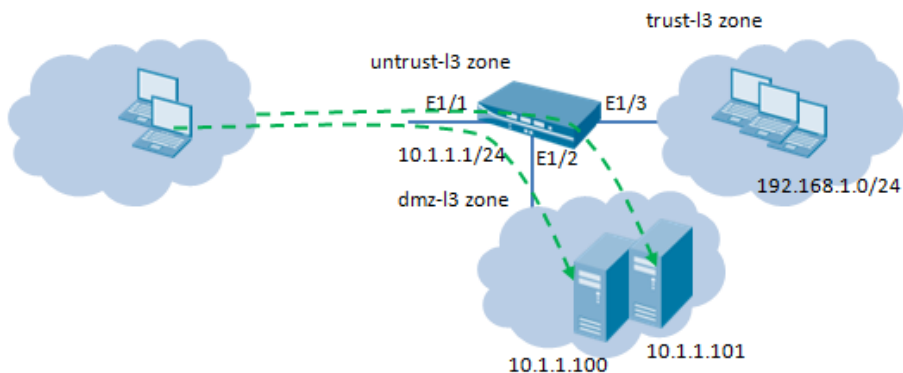
Verification

```
admin@PA-2050> show session all
```

```
-----
ID      Application  State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys
-----
80      web-browsing    ACTIVE  FLOW  ND      1.1.1.250[55077]/untrust-l3/6 (1.1.1.250[55077])
vsys1
                               1.1.1.100[80]/dmz-l3 (10.1.1.100[8080])
-----
```

Case 3: One-to-Many Mapping

In this example, one IP address maps to two different internal hosts. The application is used to identify the internal host to which the firewall will forward the traffic.



All HTTP traffic is sent to the host 10.1.1.100 and SSH traffic is sent to the server 10.1.1.101 as follows:




Src IP 1.1.1.250	Dst IP 1.1.1.100	Src Port 1025	Dst Port 80	Data	→	Src IP 1.1.1.250	Dst IP 10.1.1.100	Src Port 1025	Dst Port 80	Data
Src IP 1.1.1.250	Dst IP 1.1.1.100	Src Port 1026	Dst Port 22	Data	→	Src IP 1.1.1.250	Dst IP 10.1.1.101	Src Port 1026	Dst Port 22	Data

Configuration









The following address objects are required for this setup:

- Address object for the real IP address of the web server
- Address object for real IP address of the SSH server
- Address object for the translated IP address of the server













The configured address objects would look like this:

	Name	Type	Address
	Servers-public	IP Netmask	1.1.1.100
	SSH-server	IP Netmask	10.1.1.101
	webserver-private	IP Netmask	10.1.1.100

The NAT rules would look like this:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-websevr	 untrust-l3	 untrust-l3	none	any	 Servers-public	 service-http	none	address: webserver-private
Dst NAT-SSH	 untrust-l3	 untrust-l3	none	any	 Servers-public	 custom-ssh	none	address: SSH-server

And the security rules would look like this:

Name	Source		Destination		Application	Service	Action
	Zone	Address	Zone	Address			
Webserver acces	 untrust-l3	any	 dmz-l3	 Servers-public	 web-browsing	 application-default	
SSH access	 untrust-l3	any	 dmz-l3	 Servers-public	 ssh	 application-default	

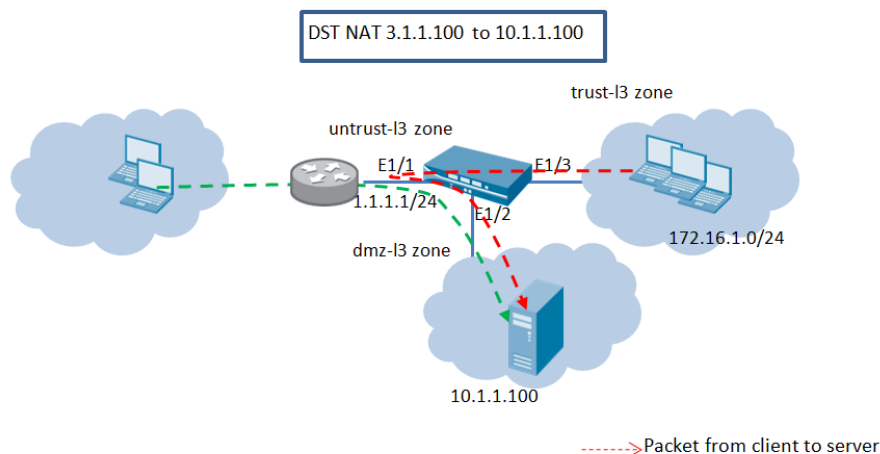
Verification

```
admin@PA-2050> show session all
```

```
-----
ID      Application  State  Type  Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys
-----
75      web-browsing   ACTIVE FLOW  ND    1.1.1.250[54863]/untrust-l3/6 (1.1.1.250[54863])
vsys1   1.1.1.100[80]/dmz-l3 (10.1.1.100[80])
74      ssh            ACTIVE FLOW  ND    1.1.1.250[54862]/untrust-l3/6 (1.1.1.250[54862])
vsys1   1.1.1.100[22]/dmz-l3 (10.1.1.101[22])
-----
```

Case 4: Server Access for Internal Users or U-turn NAT

In the scenario, destination NAT is configured for outside users to access the server in the dmz-l3 zone using the address 3.1.1.100. This example shows the configuration to allow the internal users to access the same server using the IP address 3.1.1.100.



The routing configuration on the firewall:

```
admin@PA-2050> show routing fib

total virtual-router shown :          1

-----
virtual-router name: VR1
interfaces:
  ethernet1/1 ethernet1/2 ethernet1/3 tunnel.1

route table:
flags: u - up, h - host, g - gateway

maximum of fib entries for device:      5000
number of fib entries for device:       5
maximum of fib entries for this fib:    5000
number of fib entries for this fib:     5
number of fib entries shown:            5
```

id	destination	nexthop	flags	interface	mtu
113	0.0.0.0/0	0.0.0.0	ug	ethernet1/1	1500
112	1.1.1.0/24	0.0.0.0	u	ethernet1/1	1500
111	1.1.1.1/32	0.0.0.0	uh	ethernet1/1	1500
38	10.1.1.0/24	0.0.0.0	u	ethernet1/2	1500
37	10.1.1.1/32	0.0.0.0	uh	ethernet1/2	1500

Packet flow sequence:

1. The firewall receives the packet for destination 3.1.1.100 on the interface ethernet1/15 and does a route lookup to determine the egress interface.
2. The packet is forwarded on to the interface ethernet1/1.
3. The NAT rule is evaluated for a match. In order for the destination IP address to be translated, a destination NAT rule from zone trust-l3 to zone untrust-l3 must be created to translate the destination IP of 3.1.1.100 to 10.1.1.100.

- After the translated address is determined, a route lookup for destination 10.1.1.100 is performed to determine the egress interface. In this example the egress interface will be ethernet1/2 in zone dmz-l3.
- A security policy lookup is performed to see if the traffic is permitted from zone trust-l3 to dmz-l3. It is important to note, the direction of the policy matches the ingress zone and the zone where the server is physically located. Also note that the security policy refers to the IP address in the original packet, which has a destination address of 3.1.1.100.
- The packet is then forwarded out to the server via the egress interface ethernet1/2. The destination address is changed to 10.1.1.100 as the packet leaves the firewall.

Configuration:

NAT rule

Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Web server internal	trust-l3	untrust-l3	none	any	web server public	any	none	address: webserver-private

Security rule

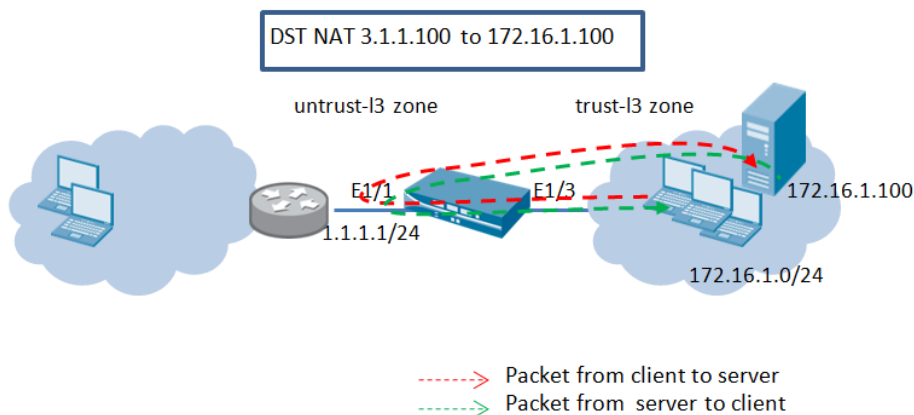
Source		Destination					
Name	Zone	Address	Zone	Address	Application	Service	Action
Webserver access	trust-l3	any	dmz-l3	web server public	web-browsing	any	✓
Outside access	trust-l3	any	untrust-l3	any	any	any	✓

Verification

```
admin@PA-2050> show session all
```

ID	Application	State	Type	Flag	Src[Sport]/Zone/Proto (translated IP[Port])	Dst[Dport]/Zone (translated IP[Port])
187	web-browsing	ACTIVE	FLOW	ND	172.16.1.250[60848]/trust-l3/6	(172.16.1.250[60848])
vsys1					3.1.1.100[80]/dmz-l3	(10.1.1.100[80])

Case 5: Server in the Same Zone as the Clients



In this example, the clients and the server are in same network/zone. The clients access the server using the public IP address of 3.1.1.100. The response from the server is also routed back through the firewall.

Configuration:

The NAT rule required for this configuration is similar to the previous example. The NAT rule is required to match traffic from the trust-l3 zone to the untrust-l3 zone. Because the response from the server is also routed back through the firewall, source NAT must also be enabled on the rule.

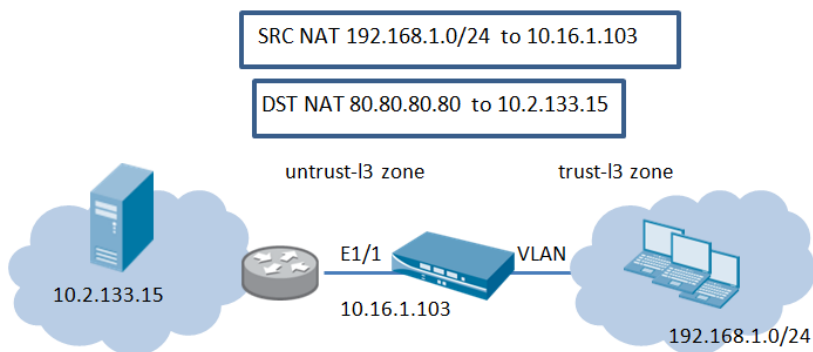
NAT rule

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
webserver access	trust-l3	untrust-l3	any	any	webserver public	any	dynamic-ip-and-port ethernet1/1	address: webserver private

After translation, security policy is matched. In this example, because the clients and the server are in the same network/zone, no security policy is needed.

Translating source and destination IP address

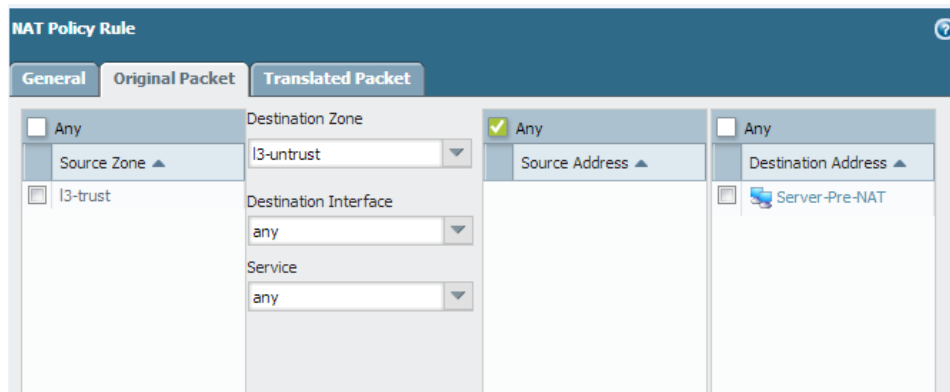
In this example, we will configure NAT rule to translate both the source and destination IP address of the packet.

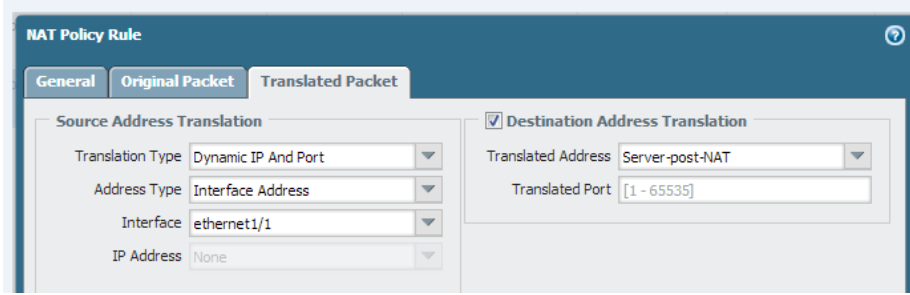


The following address objects are created

1. Server-Pre-NAT: 80.80.80.80
2. Server-post-NAT: 10.2.133.15

Screen shot of the NAT policy is as shown





Verification

```
admin@santaclara-1> show session all filter destination 80.80.80.80
```

```
-----
ID      Application      State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                         Dst[Dport]/Zone (translated IP[Port])
-----
24351   ssh                  ACTIVE  FLOW  NB    192.168.1.11[50281]/13-trust/6 (10.16.1.103[23707])
vsys1                                         80.80.80.80[22]/13-untrust (10.2.133.15[22])
admin@santaclara-1>
```

The output of the relevant debug is shown below with ICMP traffic is shown below

```
== Oct 26 17:16:52 ==
Packet received at slowpath stage
Packet info: len 74 port 17 interface 266 vsys 1
wqe index 178615 packet 0x0x80000000b6dce0c6
Packet decoded dump:
L2:      5c:26:0a:45:e7:b6->b4:0c:25:f5:8b:01, type 0x0800
IP:      192.168.1.11->80.80.80.80, protocol 1
        version 4, ihl 5, tos 0x00, len 60,
        id 5220, frag_off 0x0000, ttl 128, checksum 50185
ICMP:    type 8, code 0, checksum 19769, id 1, seq 34
Session setup: vsys 1
PBF lookup (vsys 1) with application ping
Session setup: ingress interface vlan.1 egress interface ethernet1/1 (zone 9)
NAT policy lookup, matched rule index 0
Destination NAT, translated IP 10.2.133.15
PBF lookup (vsys 1) with application ping
Session setup: egress zone 9 for natted IP
Translated IP in zone 9, egress id 16
Policy lookup, matched rule index 0
DP0 is selected to process this session.
Allocated new session 24411.
Packet matched vsys 1 NAT rule 'Server NAT' (index 1),
source translation 192.168.1.11/1 => 10.16.1.103/1
destination translation 80.80.80.80/34 => 10.2.133.15/34
Created session, enqueue to install

---__pan_debug_tag=5---pan_sys_up_ticks=559796534266160---

== Oct 26 17:16:52 ==
Packet received at fastpath stage
Packet info: len 74 port 17 interface 266 vsys 1
wqe index 178615 packet 0x0x80000000b6dce0c6
Packet decoded dump:
L2:      5c:26:0a:45:e7:b6->b4:0c:25:f5:8b:01, type 0x0800
IP:      192.168.1.11->80.80.80.80, protocol 1
        version 4, ihl 5, tos 0x00, len 60,
```

```

        id 5220, frag_off 0x0000, ttl 128, checksum 50185
ICMP:   type 8, code 0, checksum 19769, id 1, seq 34
Flow fastpath, session 24411
NAT session, run address/port translation

---__pan_debug_tag=5---pan_sys_up_ticks=559796534454301---

== Oct 26 17:16:52 ==
Packet received at forwarding stage
Packet info: len 74 port 17 interface 266 vsys 1
wqe index 178615 packet 0x0x80000000b6dce0c6
Packet decoded dump:
L2:     5c:26:0a:45:e7:b6->b4:0c:25:f5:8b:01, type 0x0800
IP:     10.16.1.103->10.2.133.15, protocol 1
        version 4, ihl 5, tos 0x00, len 60,
        id 5220, frag_off 0x0000, ttl 128, checksum 35797
ICMP:   type 8, code 0, checksum 19769, id 1, seq 34
Forwarding lookup, ingress interface 266
L3 mode, virtual-router 1
Route lookup in virtual-router 1, IP 10.2.133.15
Route found, interface ethernet1/1, zone 9, nexthop 10.16.0.1
Resolve ARP for IP 10.16.0.1 on interface ethernet1/1
ARP entry found on interface 16
Transmit packet on port 16

```

Virtual Wire NAT

With PAN-OS version 4.1, it is possible to configure NAT for interfaces configured in a virtual wire. The following types of NAT configurations are supported in virtual wire NAT:

- Source NAT
 - Dynamic IP
 - Dynamic IP and port
 - Static NAT
- Destination NAT

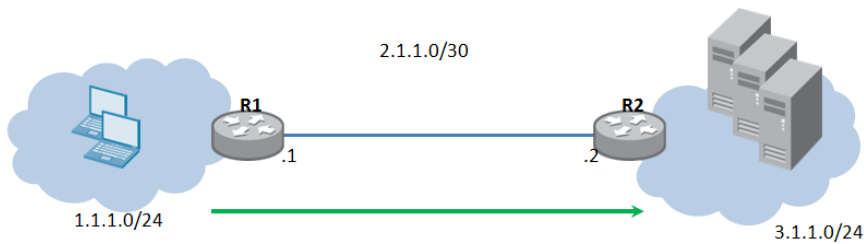
Note:

- Because interfaces in a virtual wire do not have an IP address assigned, it is not possible to translate an IP address to an interface IP address. You must configure IP address pool.
- The firewalls will not proxy ARP for NAT addresses. Ensure that routes are configured on the upstream and downstream devices.
- Proper routing must be configured on the upstream and downstream routers in order for the packets to be translated in virtual wire mode.
- Virtual wire NAT policies do allow using “ANY” as the destination zone.

Some of the virtual wire NAT scenarios are discussed in the sections that follow. The security policies for both source NAT and static NAT are configured to be from virtual wire zones “vw-trust” to “vw-untrust”.

Source NAT

Virtual wire deployment of a Palo Alto Networks firewall provides the benefit of providing security transparently to the end devices. In the following topology example, two routers are configured to provide connectivity between the subnets 1.1.1.0/24 and 3.1.1.0/24 respectively. The link between the routers is configured in subnet 2.1.1.0/30. Static routing is configured on both the routers to establish connectivity between the networks.



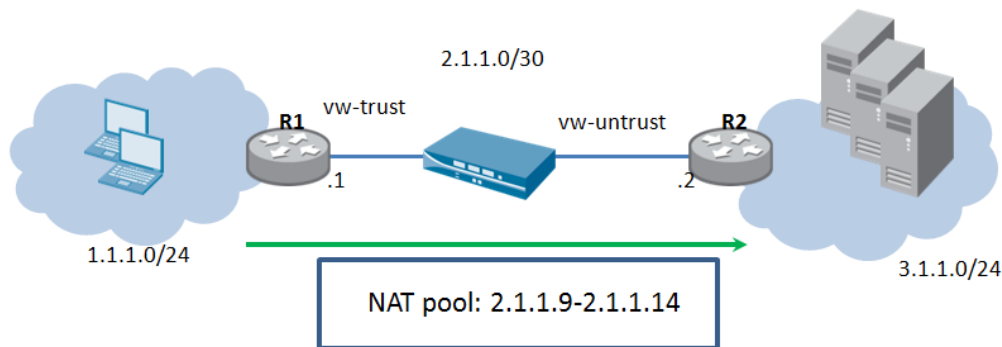
Route on R1:

Destination	Next hop
3.1.1.0/24	2.1.1.2

Route on R2:

Destination	Next hop
1.1.1.0/24	2.1.1.1

In this example, the firewall is deployed in virtual wire mode between two layer 3 devices. All connections from clients in network 1.1.1.0/24 accessing servers in network 3.1.1.0/24 will be translated to IP range of 2.1.1.9-2.1.1.14. A NAT IP address pool with range 2.1.1.9-2.1.1.14 is configured on the firewall.



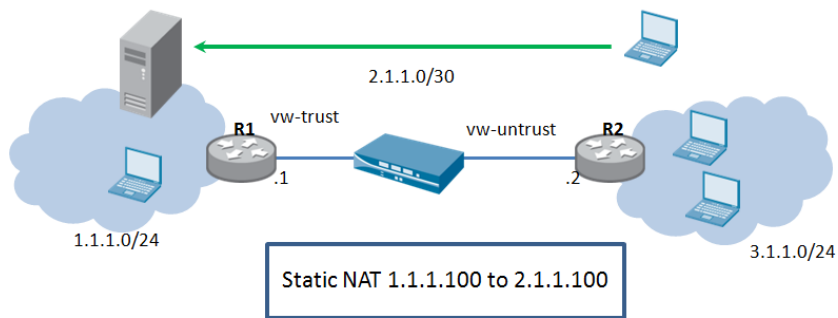
All connections from the clients in subnet 1.1.1.0/24 will arrive at the router R2 with translated source address in the range 2.1.1.9-2.1.1.14. The response from servers will be directed to these addresses. In order for source NAT to work, proper routing must be configured on router R2. The table below shows the modified routing table on router R2. This will ensure the traffic to the destination 2.1.1.9-2.1.1.14 i.e. subnet 2.1.1.8/29, will be sent back via the firewall to router R1.

Route on R2:

Destination	Next hop
2.1.1.8/29	2.1.1.1

Static NAT

In this example, host 1.1.1.100 is statically translated to address 2.1.1.100. Static NAT with the bi-directional option is also supported in virtual wire mode. In this example, with the bi-directional option enabled, system generated NAT policy is generated from the vw-untrust zone to vw-trust zone. Clients on the vw-untrust zone access the server using the IP address 2.1.1.100, which will be translated by the firewall to 1.1.1.100. Any connections initiated by the server at 1.1.1.100 will be translated to source IP address 2.1.1.100.



Route on R2:

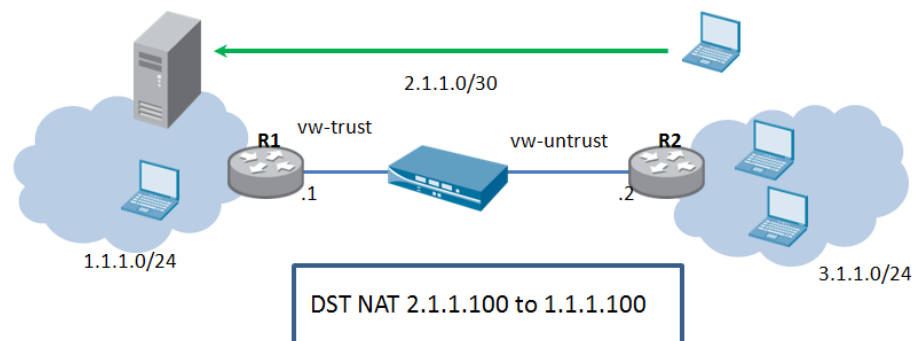
Destination	Next hop
2.1.1.100/32	2.1.1.1

NAT policy

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Static NAT	vw-trust	vw-untrust	any	webserver private	any	any	static-ip webserver public bi-directional: yes	none

Destination NAT




Clients in the vw-untrust zone access the server using the IP address 2.1.1.100, which will be translated by the firewall to 1.1.1.100. Both the NAT and security policy must be configured from vw-untrust zone to vw-trust zone.



Route on R2:

Destination	Next hop
2.1.1.100/32	2.1.1.1

NAT policy

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
DST NAT	 vw-untrust	 vw-trust	any	any	 webserver public	any	none	address: webserver private

NAT with IPsec VPN

NAT can be configured to translate packets before they are encrypted. For configuration examples, refer to the document at <https://live.paloaltonetworks.com/docs/DOC-1594>.

Verifying NAT rules

With multiple NAT rules configured on the device, the order of the NAT rules is important for address translation. NAT rule processing can be verified from the CLI using the operational mode `test nat-policy-match` command.

```
test nat-policy-match <options>
+ destination          destination IP address
+ destination-port      Destination port
+ from                 From zone
+ protocol              IP protocol value
+ source               source IP address
+ source-port          Source port
+ to                   To zone
+ to-interface         Egress interface to use
```

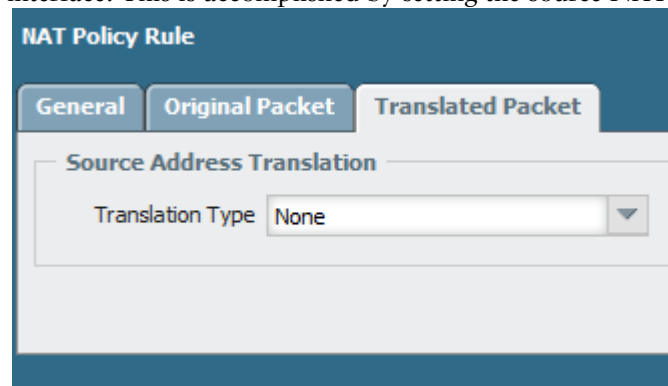
For example:

```
admin@FW> test nat-policy-match from l3-untrust source 10.1.1.1 destination 66.151.149.20
destination-port 443 protocol 6
```

```
Destination-NAT: Rule matched: CA2-DEMO
66.151.149.20:443 => 192.168.100.15:443
```

NAT Exemptions

Both source NAT and destination NAT rules can be configured to disable address translation. This is used in scenarios where NAT has to be disabled for certain hosts in a subnet, or when NAT is not required for traffic exiting a specific interface. This is accomplished by setting the source NAT translation type to NONE as follows:



NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type None

NAT interaction with applications

Dynamic-IP address translation works with only TCP- and UDP-based applications. Traceroute is not supported with dynamic-IP translation.

Summary

PAN-OS rule-based NAT offers a very flexible way of implementing address translation to meet challenging network requirements while offering increased ease of use. When combined with application visibility, application control and threat prevention, Palo Alto Network firewalls offer the best of breed in security and networking functions.

Revision History

Date	Revision	Comment
8/26/2012	C	Editorial updates and included scenario with source and destination NAT
6/15/2012	B	Updated with new flow chart, example on U turn NAT
10/10/2011	A	First draft