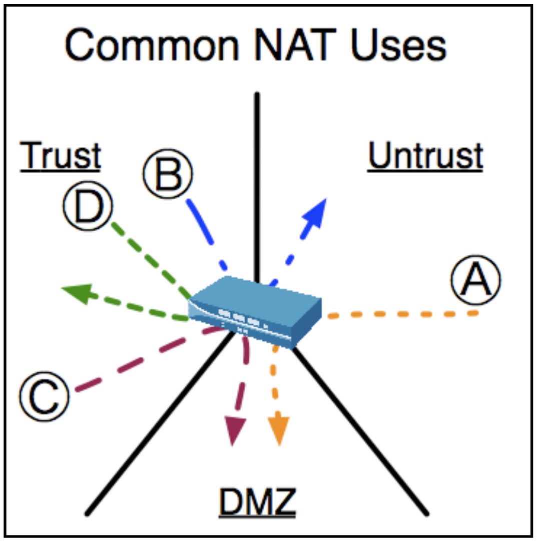
Understanding NAT

Tech Note

Overview

Network Address Translation (NAT) allows computers without a public IP address to communicate with the public network. The diagram below shows four instances of NAT across three different security zones:

A. Inbound, destination changes
B. Outbound, source changes
C. U-Turn between zones, destination changes
D. U-Turn on same network, both the source and destination change



Since the way firewall platforms implement these four NAT cases varies, this document explains the NAT architecture as implemented in PAN-OS.

NAT Offerings

PAN-OS provides three types of NAT:

- **Dynamic IP/Port**: used for outbound traffic; multiple clients can use the same public IP address(es) with different source port numbers

- **Dynamic IP**: used for outbound traffic; private source addresses translate to the next available address in a range

- **Static IP**: used for inbound or outbound traffic; can be used to change the source or the destination IP address, with the source or destination port unchanged. When used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports.

In the previous descriptions, inbound and outbound refer to the direction the connection is initiated.

The table below reviews the three NAT types. The two dynamic methods map a range of client addresses (M) to a pool (N) of NAT addresses, where M and N are different numbers. N can also be 1. Dynamic IP/Port NAT differs from Dynamic IP NAT in that the TCP and UDP source ports are not preserved in Dynamic IP/Port, whereas they are unchanged with Dynamic IP NAT. There are also differing limits to the size of the translated IP pool, as noted below.

With Static IP NAT, there is a one-to-one mapping between each original address and its translated address. This can be expressed as 1-to-1 for a single mapped IP address, or M-to-M for a pool of many one-to-one, mapped IP addresses.

PAN-OS NAT Type	Source Port stays same	Dest. Port can change	A.K.A.	Size of Translated Address Pool
Dynamic IP/Port	No	No	Many-to-1 M-to-N	up to 3 consecutive addresses
Dynamic IP	Yes	No	M-to-N	up to 32 consecutive addresses
Static IP	Yes	No	1-to-1 M-to-M MIP	unlimited
		Optional	1-to-Man VIP PAT	

NAT Requirements

NAT can only be performed on Layer 3 interfaces. Interfaces configured as Virtual Wires or Layer 2 interfaces cannot use NAT.

Also, when specifying service (TCP or UDP) ports for NAT, the pre-defined service *service-http* includes two TCP ports - 80 and 8080. To specify a single port such as TCP 80, define a new service.

Zones

All interfaces on PA-series firewalls must be assigned a zone.

Zones help segment the network, helping maintain control and organization of traffic. While zones help with overall scaleability and manageability of a firewall configuration, they do add an extra support option when using NAT, causing confusion for administrators new to zone-based firewalls. When understood and implemented correctly, the use of zones within NAT rules gives an organization more flexibility and simplicity with their firewall management.

For organizations unfamiliar with using firewall zones for configuration, administrators can start by assigning all interfaces to the same zone, until the concepts of NAT and zones have been mastered.

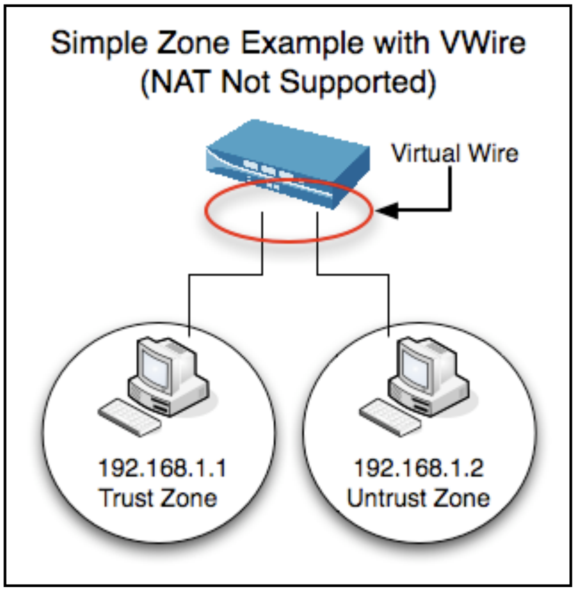
A zone groups interfaces with the same security posture, allowing for a minimal, easy to understand ruleset. For the most part, traffic of interest is that which traverses from one security zone to another.

Scope of Zones

Zones can be segmented as small as an individual IP address on an interface or grow as large as multiple networks across multiple interfaces.

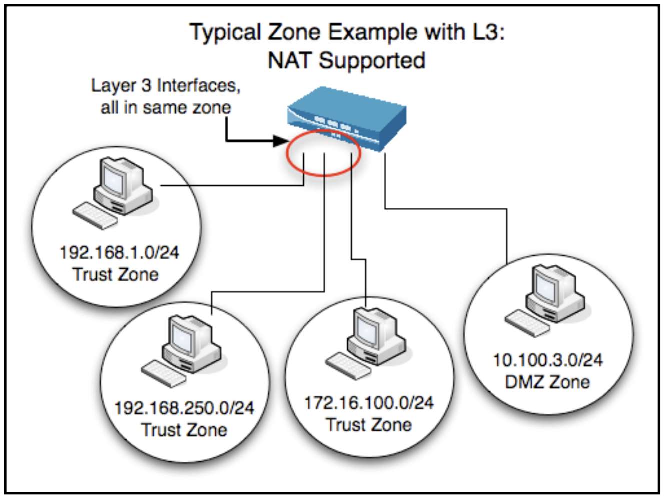
Objects reside in a particular zone because the PA-series firewall interface the traffic traverses has been assigned to a given zone.

The example to the right is an extreme case of zone segmenting - individual hosts are in different zones, even though they are on the same IP network!



This last example is actually a poor example for NAT, since NAT can only be used on Layer 3 (L3) interfaces. The second figure (below to the right) is a good example of NAT use with zones. When policy is written for the three internal networks in the Trust zone, a single rule can be applied, without maintaining a list of the individual networks. The Security rules on the next page highlight the differences when using zones (or not) for the network in the diagram to the right.

The security rule at the top of the next page shows how just specifying traffic from the Trust zone to the Untrust zone makes it unnecessary to maintain a list of all networks matching this rule.



Security Rule - proper use of zones					
Source Zone	**Destination Zone**	**Source Addr.**	**Destination Addr**	**Application**	**Action**
Trust	Untrust	Any	Any	Any	Allow

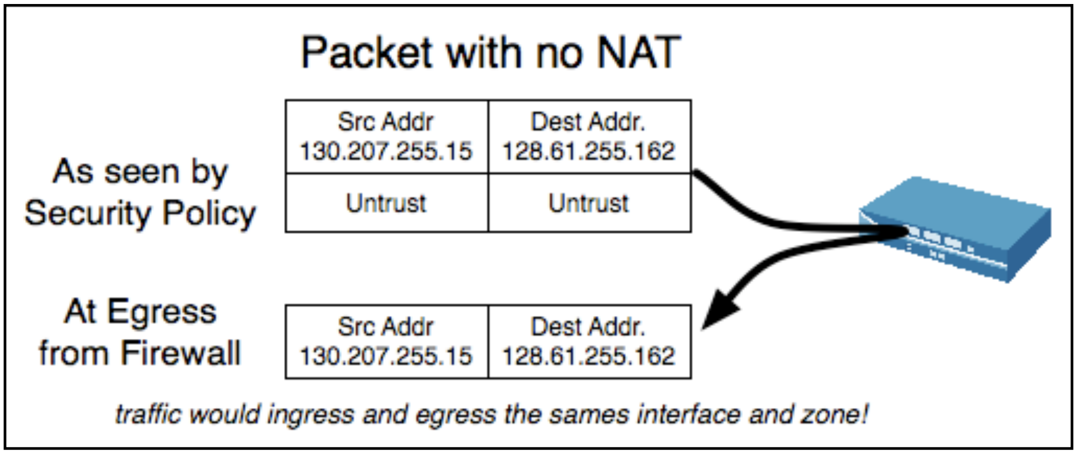
The next security rule shows what security rules are like when multiple zones in PAN-OS are **not** used. In this case, all layer 3 interfaces are placed in the same zone, called onezone below.

Without zones to distinguish traffic passing from one interface to another, each network is specifically called out in the rule.

Security Rule - same zone for all L3 interfaces					
Source Zone	**Destination Zone**	**Source Addr.**	**Destination Addr**	**Application**	**Action**
onezone	onezone	192.168.1.0/24 192.168.250.0/24 172.17.100.0/24	Any	Any	Allow

Choosing Zones

Both Security and NAT rulebases utilize source and destination zones. PAN-OS administrators must reference the correct zone when writing Security and NAT rules. This can be a little confusing if an administrator does not understand how zones associated with packets are managed by PAN-OS. For example, on a DMZ network, the same physical server could have a real local address, along with a public address - with each address in a different zone.



Src Addr 130.207.255.15	Dest Addr. 128.61.255.162
Untrust	Untrust

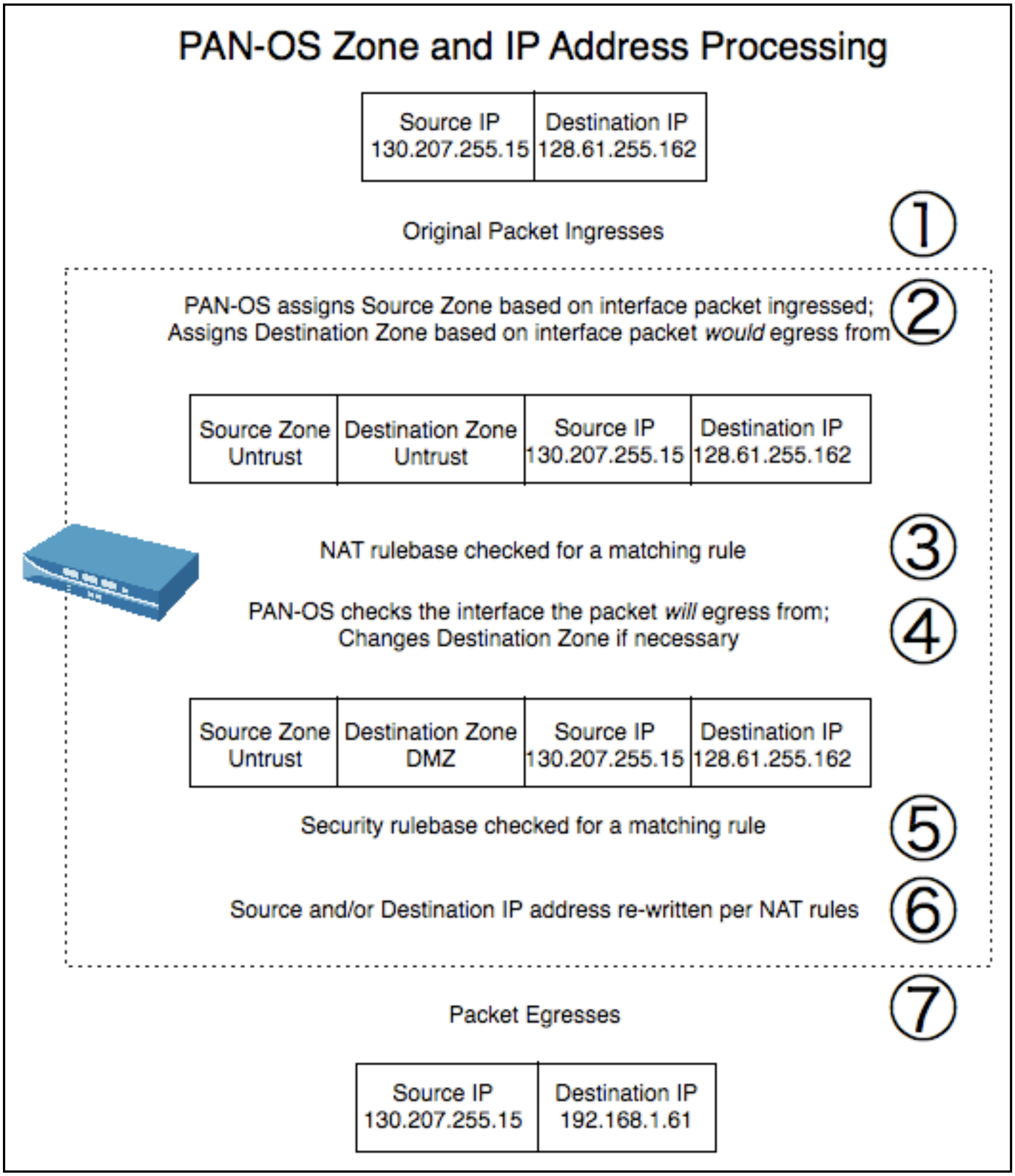
Src Addr 130.207.255.15	Dest Addr. 128.61.255.162

traffic would ingress and egress the sames interface and zone!

When writing NAT rules, chose the zone based on the IP address information as the packets arrive into the PA-series firewall. In the example[1] above, a packet arrives with both the source and destination addresses in the same zone (Untrust). This is normal! No NAT has been applied to the packet - yet. NAT rules must FIRST match an incoming IP packet. Only then can NAT transform the packet, preparing the packet for all other policies.

[1] This example is known as Example #2 later in the document

The diagram below walks through the process PAN-OS goes through to assign a source and destination zone to packets. Step 1 shows the incoming source and destination IP addresses. Step 2 shows how PAN-OS assigns the Source Zone, easily determined as the packet has already arrived via an interface and zone into the firewall. To determine Destination Zone, PAN-OS must consider which interface the packet *would* egress the firewall from. Then, NAT policy is consulted in Step 3 - looking for a matching NAT rule. If not matching any NAT rules, the packet skips to Step 5. If a NAT rule was matched, in Step 4 the Destination Zone is updated to reflect the zone associated with the interface the packet *will* egress on. In Step 5, the Security rulebase is checked. Only in Step 6 are the final source and destination IP address changed (if necessary) to reflect a matching NAT rules. Finally in Step 7, the packet egresses the firewall.



PAN-OS Zone and IP Address Processing

Source IP	Destination IP
130.207.255.15	128.61.255.162

Original Packet Ingresses ①

PAN-OS assigns Source Zone based on interface packet ingressed; Assigns Destination Zone based on interface packet *would* egress from ②

Source Zone	Destination Zone	Source IP	Destination IP
Untrust	Untrust	130.207.255.15	128.61.255.162

NAT rulebase checked for a matching rule ③

PAN-OS checks the interface the packet *will* egress from; Changes Destination Zone if necessary ④

Source Zone	Destination Zone	Source IP	Destination IP
Untrust	DMZ	130.207.255.15	128.61.255.162

Security rulebase checked for a matching rule ⑤

Source and/or Destination IP address re-written per NAT rules ⑥

Packet Egresses ⑦

Source IP	Destination IP
130.207.255.15	192.168.1.61

With the previous diagram in mind, we know we can reference the correct zone when writing a NAT or Security rule, by remembering the following:

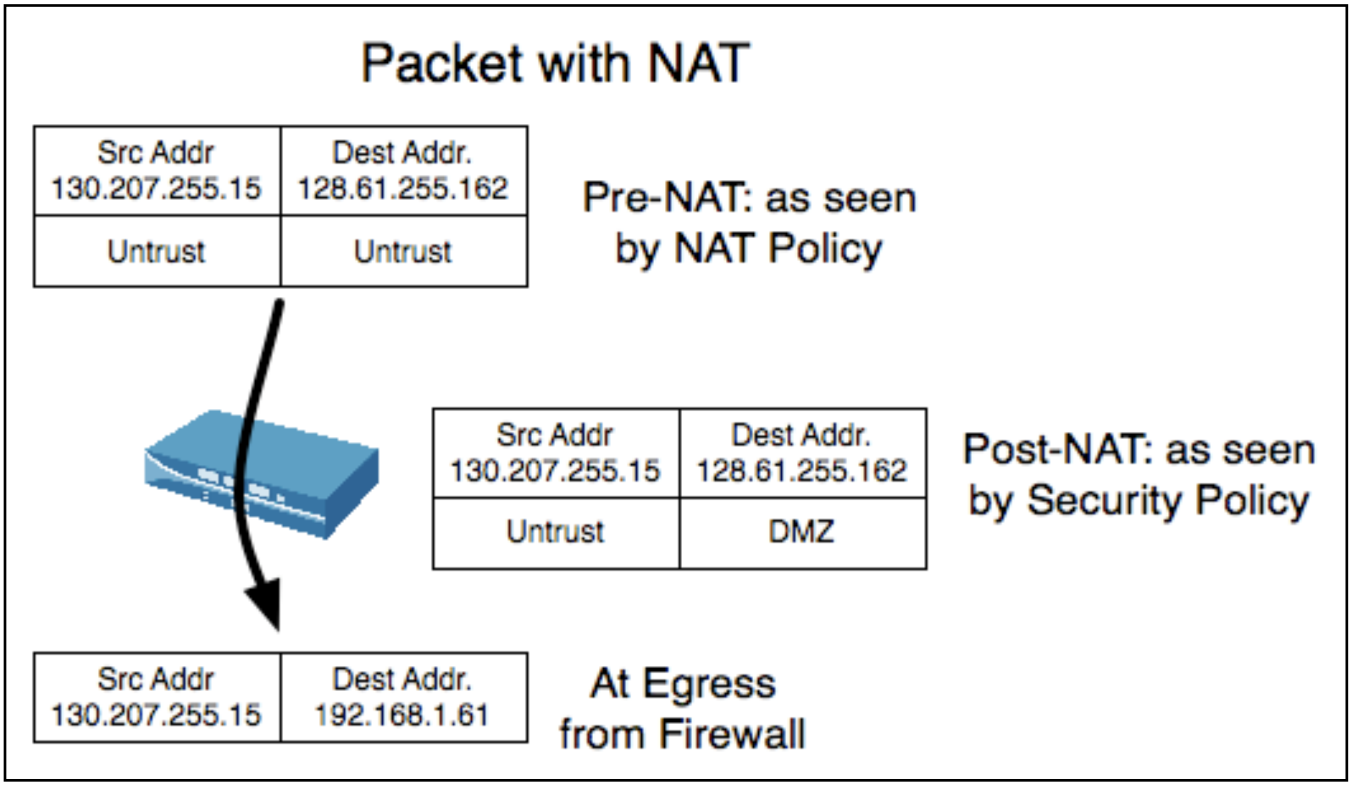
- NAT rules match incoming traffic by the zones associated with the original source and destination IP addresses. Remember: NAT has not occurred yet.
- Original IP addresses are ALWAYS used with rules, no matter which policy. Note: NAT address translation does not actually happen until the packet egresses the firewall.
- NAT, Security, and other rules will ALWAYS reference the original source ingress zone. Note: The packet already arrived at a firewall interface and zone. We cannot go back and change how it ingresses!
- The ONLY address or zone that may change from the original packet is the Destination Zone. Note: NAT may change the egress interface

---

Note: Always use the incoming IP addresses and Source Zone. ALL rules reference these always.

Once NAT policy has been applied, all other Policies, - such as Security, SSL, Application Override, and Captive Portal - will use the post-NAT zones associated with the connection.

The diagram below shows, in a shorthand notation, the Source IP address, Destination IP address, Source Zone, and Destination Zone needed for NAT and Security rules. This example is the same as for Example #2 later in the document.



Packet with NAT

Src Addr 130.207.255.15	Dest Addr. 128.61.255.162
Untrust	Untrust

Pre-NAT: as seen by NAT Policy

Src Addr 130.207.255.15	Dest Addr. 128.61.255.162
Untrust	DMZ

Post-NAT: as seen by Security Policy

Src Addr 130.207.255.15	Dest Addr. 192.168.1.61

At Egress from Firewall

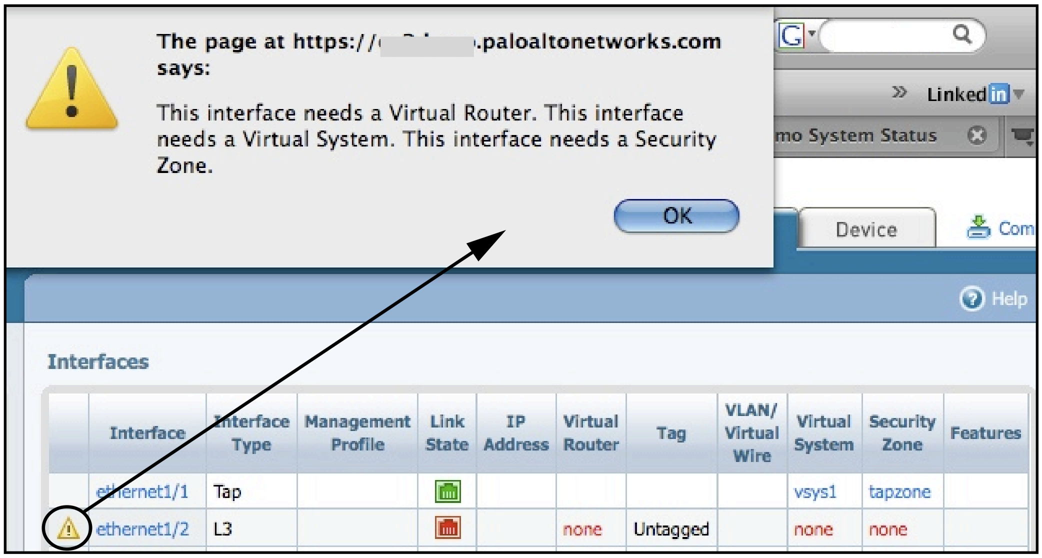
IPSec and NAT

When using NAT in conjunction with IPSec, policy rules should not be affected. IPSec functions as part of the routing for Layer 3 interfaces. Example #5 shows an example with IPSec.

Now that zones are understood, the next section reviews PAN-OS configuration items for NAT.

Configuration Basics

Before starting, at least two Layer 3 interfaces must exist on the PA-series firewall. When an L3 interface is created, a zone must be set for the PAN-OS commit to succeed. Zones can be changed at any time, if needed. If a zone is not assigned to an interface, PAN-OS tries to notify the user of the problem, as seen in the screenshot below. The configuration will not successfully commit to the system until the zones are added.



The page at https://[redacted].paloaltonetworks.com says:

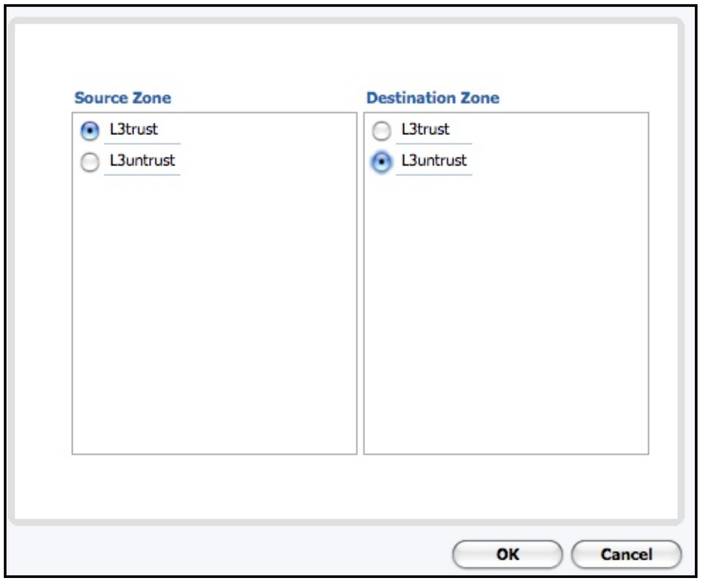
This interface needs a Virtual Router. This interface needs a Virtual System. This interface needs a Security Zone.

Interfaces

	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Virtual System	Security Zone	Features
	ethernet1/1	Tap		🟩					vsys1	tapzone	
⚠	ethernet1/2	L3		🟥		none	Untagged		none	none	

Creating a NAT Rule

When creating a new NAT rule, source and destination zones must be specified (as in the screenshot to the right) before a rule appears for editing in the NAT Rulebase.

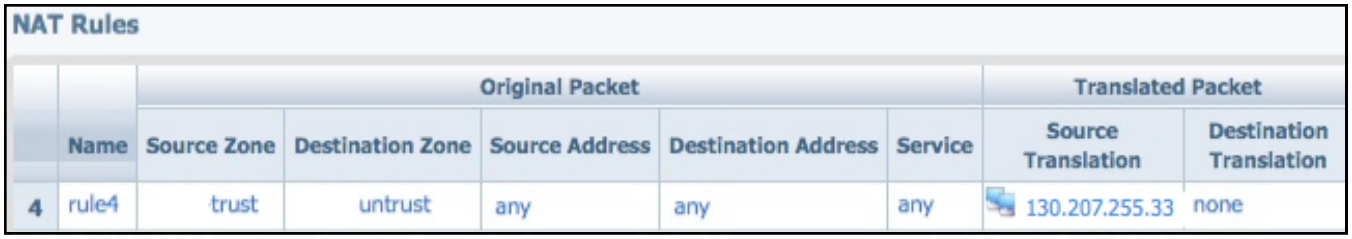


Source Zone
● L3trust
○ L3untrust

Destination Zone
○ L3trust
● L3untrust

Outbound Rules: Source NAT

Below is an example of a functional Dynamic IP/Port outbound rule, showing all NAT columns.



NAT Rules

		Original Packet					Translated Packet	
	Name	Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
4	rule4	trust	untrust	any	any	any	130.207.255.33	none

The match for outbound traffic can be for all UDP and TCP traffic - ‘any’ in the Service column - or a more granular match for specific UDP and TCP ports.

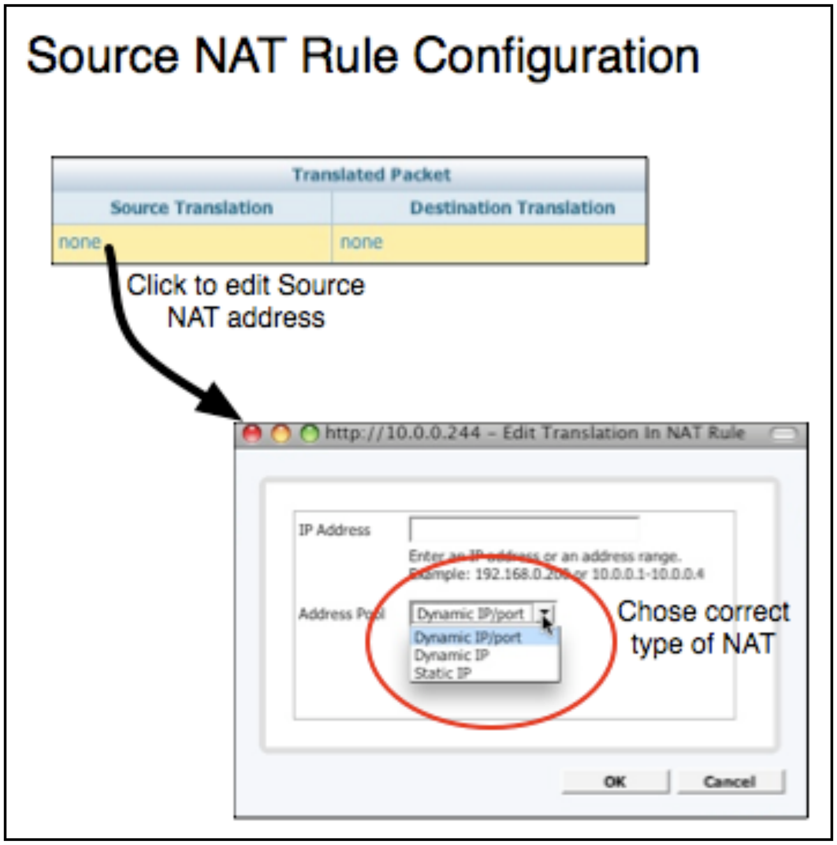
For outbound NAT, source IP addresses will change - but destination IP addresses will not.

To configure a new outbound NAT rule, select the field in the Source Translation column. The address pool (as in the screenshot below) shows the different NAT options available.

Notice the lack of port configuration options - only IP addresses or a range of addresses can be specified.

Selecting Dynamic IP/Port means both the source IP and source port will be different.

Using Dynamic IP or Static IP means the source address will change, but the source port will be the same.



Source NAT Rule Configuration

Translated Packet	
Source Translation	Destination Translation
none	none

Click to edit Source NAT address

http://10.0.0.244 - Edit Translation In NAT Rule

IP Address

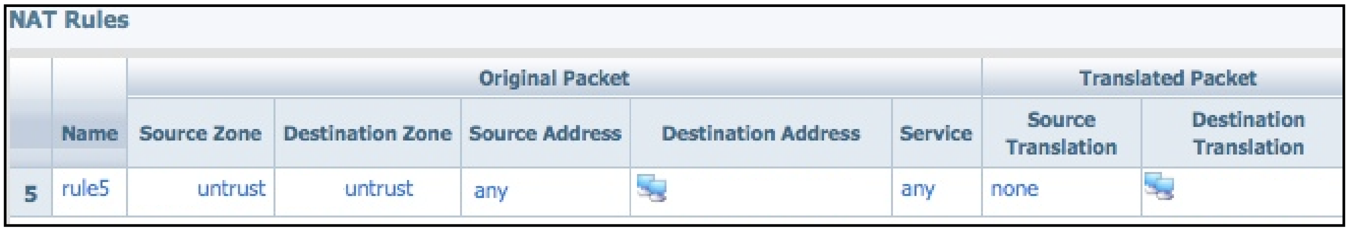
Enter an IP address or an address range.
Example: 192.168.0.200 or 10.0.0.1-10.0.0.4

Address Pool: Dynamic IP/port

Chose correct type of NAT

Inbound Rules: Destination NAT

For inbound NAT, destination IP addresses will change. Below is an example of a functional inbound NAT rule.



NAT Rules

		Original Packet					Translated Packet	
	Name	Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
5	rule5	untrust	untrust	any		any	none	

The Destination Address in the Original Packet can be either:

- 1 or more IP addresses, specified with slash (/) notation for the netmask
- An existing network object

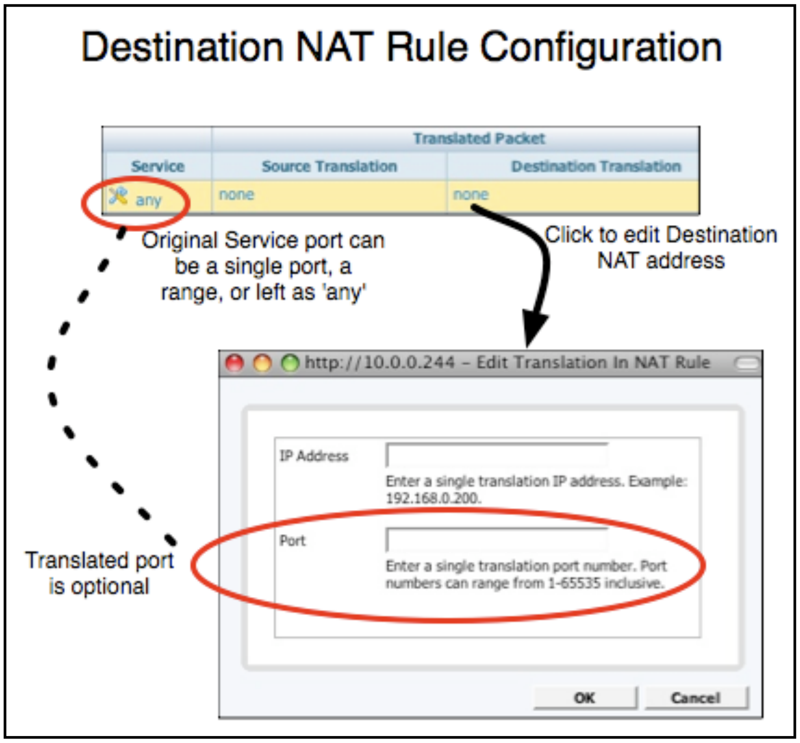
The service port in the rule can specify:

- Any, for all TCP and UDP ports
- A range of TCP or UDP ports
- A single TCP or UDP port
- a service object

Service groups are not allowed. Also, remember that the service *service-http* includes TCP port 80 and 8080, and may not be used with NAT.

For the case when a single public IP address is used for multiple servers and services with private addresses, a rule is created for each internal service, matching the external service port, with the translated destination port specified in the window above.

For a reference, a few examples follow, showing use of NAT and Security zones.



Destination NAT Rule Configuration

	Translated Packet	
Service	Source Translation	Destination Translation
any	none	none

Original Service port can be a single port, a range, or left as 'any'

Click to edit Destination NAT address

http://10.0.0.244 – Edit Translation In NAT Rule

IP Address

Enter a single translation IP address. Example: 192.168.0.200.

Port

Enter a single translation port number. Port numbers can range from 1-65535 inclusive.

Translated port is optional

NAT Examples

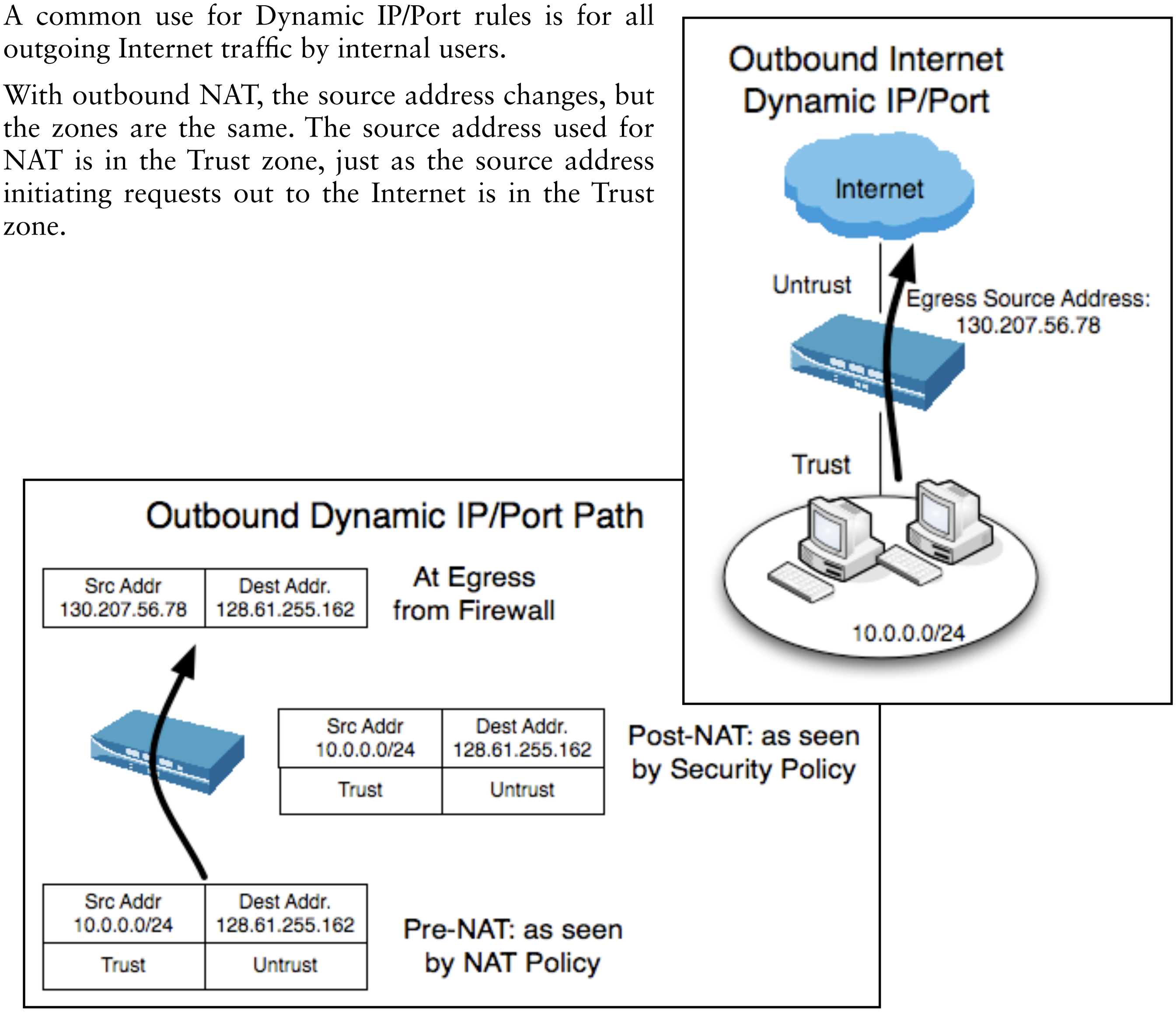
Since many deployments are possible using NAT, 5 major examples are listed below (with 3 alternates). Each of the 8 is expanded on, with recommended Security rules, NAT rules, and any other caveats.

#	Description	NAT Type	Direction	IP Address Changing
1	Typical outbound user traffic	Dynamic IP/Port	Outbound	Source
1A	Outbound user applications that requires the source port to stay the same.	Dynamic IP	Outbound	Source
2	Make servers on the DMZ reachable by the Internet, each server with their own public IP address	Static IP	Inbound	Destination
2A	Limited number of public IP addresses mapped to multiple servers on the DMZ (PAT).	Static IP	Inbound	Destination
3	Email gateway needs to communicate with other mail servers on the Internet	Static IP	Outbound	Source
4	U-Turn between zones: commonly used when an internal user wants to test services to the external address of servers on the DMZ	Dynamic IP/Port Dynamic IP	Inbound	Destination
4A	U-Turn on the same zone; internal user wants to test services to the external address of servers which are also on the same local network.	Dynamic IP/Port Dynamic IP	Outbound Inbound	Source Destination
5	Remote Site-to-Site IPSec VPN with Static IP NAT covering the entire range of IP addresses	Static IP	Outbound Inbound	Source Destination

Example #1: Outbound User Traffic

A common use for Dynamic IP/Port rules is for all outgoing Internet traffic by internal users.

With outbound NAT, the source address changes, but the zones are the same. The source address used for NAT is in the Trust zone, just as the source address initiating requests out to the Internet is in the Trust zone.



Outbound Internet Dynamic IP/Port
Internet
Untrust
Egress Source Address: 130.207.56.78
Trust
10.0.0.0/24
Outbound Dynamic IP/Port Path
At Egress from Firewall
Post-NAT: as seen by Security Policy
Pre-NAT: as seen by NAT Policy

Src Addr 130.207.56.78	Dest Addr. 128.61.255.162

Src Addr 10.0.0.0/24	Dest Addr. 128.61.255.162
Trust	Untrust

Src Addr 10.0.0.0/24	Dest Addr. 128.61.255.162
Trust	Untrust

NAT Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Service**	**Translated Source**	**Translated Dest**
For Internal users going out	Trust	Untrust	any	any	any	130.207.56.78	none

Security Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Application**	**Service**	**Action**
Allow Web Surfing	Trust	Untrust	any	any	web-browsing	application-default	allow

Example #1A: Outbound User Traffic, Source Port Unchanged

This example is a variation on the previous, except a few users have applications that require the TCP or UDP source ports unchanged, or the use of other IP-protocol types than TCP or UDP.

The rules and pre-NAT/post-NAT zone processing are the same, except Dynamic IP is chosen instead of Dynamic IP/Port.

Use external public network addresses as a pool. This way, a number of internal users can share the pool of addresses when needed.

NAT Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Service**	**Translated Source**	**Translated Dest**
Users with Special App	Trust	Untrust	any	any	any	130.207.56.78	none

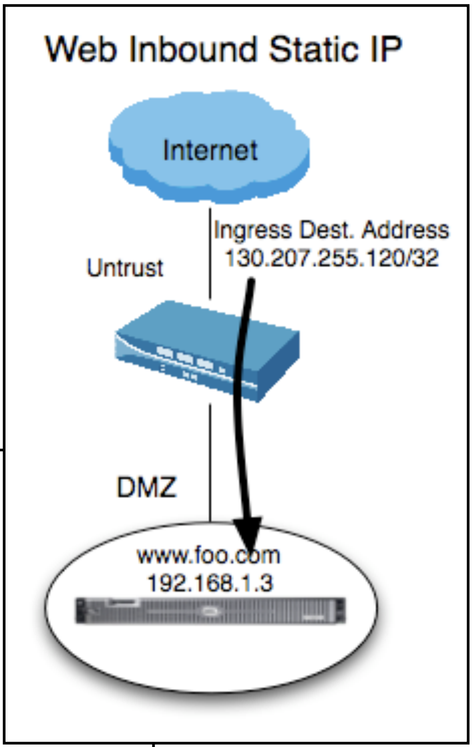
Security Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Application**	**Service**	**Action**
Users with Special App	Trust	Untrust	any	any	special-app	application-default	allow

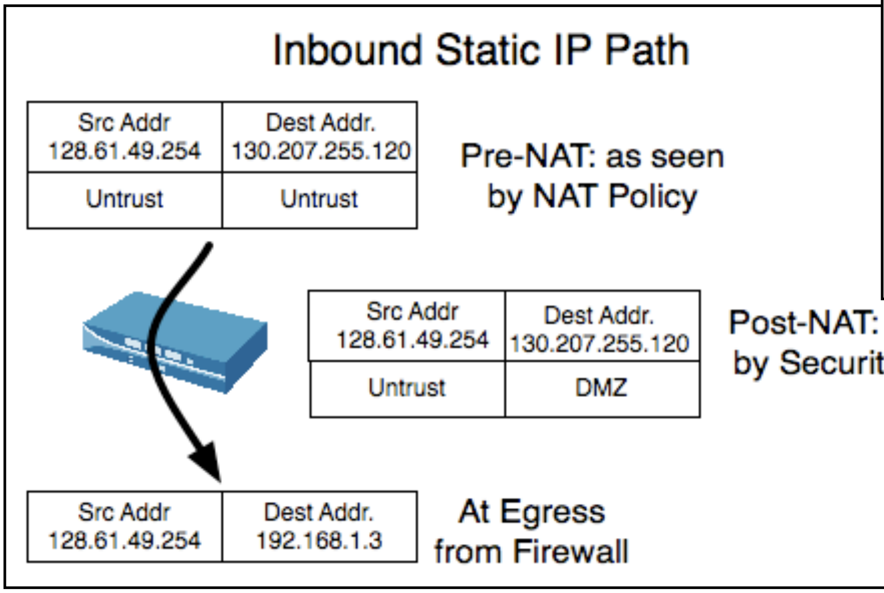
Example #2: Internet Inbound to DMZ servers

For servers in the DMZ zone, such as web and email servers, inbound Static NAT rules are required. This allows public networks to reach those servers even if they reside on a network with private addressing.

The NAT rules for each server will go from the Untrust Source zone, to the Untrust Destination zone.

Users on the internal, Trust zone using native IP addressing to contact the same webserver - no NAT rules needed. When internal users want to use the external IP address of the webserver, they should add a U-Turn rule, such as described in Example #4.




Inbound Static IP Path

Src Addr 128.61.49.254	Dest Addr. 130.207.255.120
Untrust	Untrust

Pre-NAT: as seen by NAT Policy

Src Addr 128.61.49.254	Dest Addr. 130.207.255.120
Untrust	DMZ

Post-NAT: as seen by Security Policy

Src Addr 128.61.49.254	Dest Addr. 192.168.1.3

At Egress from Firewall

NAT Rule

Comment	Source Zone	Dest. Zone	Source Addr	Dest. Addr	Service	Translated Source	Translated Dest
For Internet Users	Untrust	Untrust	any	130.207.255.120	mytcp80	none	192.168.1.3

Security Rule

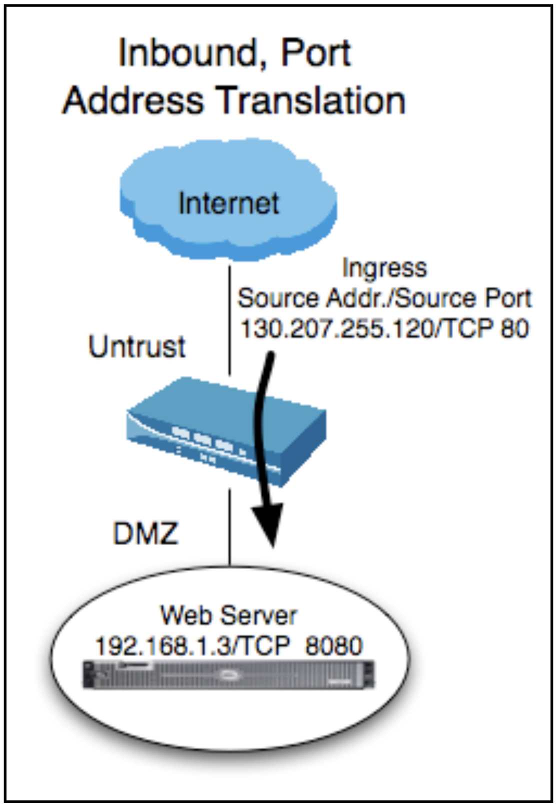
Comment	Source Zone	Dest. Zone	Source Addr	Dest. Addr	Application	Service	Action
For Internet Users	Untrust	DMZ	any	130.207.255.120	web-browsing	application-default	allow
For Internal Users	Trust	DMZ	any	192.168.1.3	web-browsing	application-default	allow

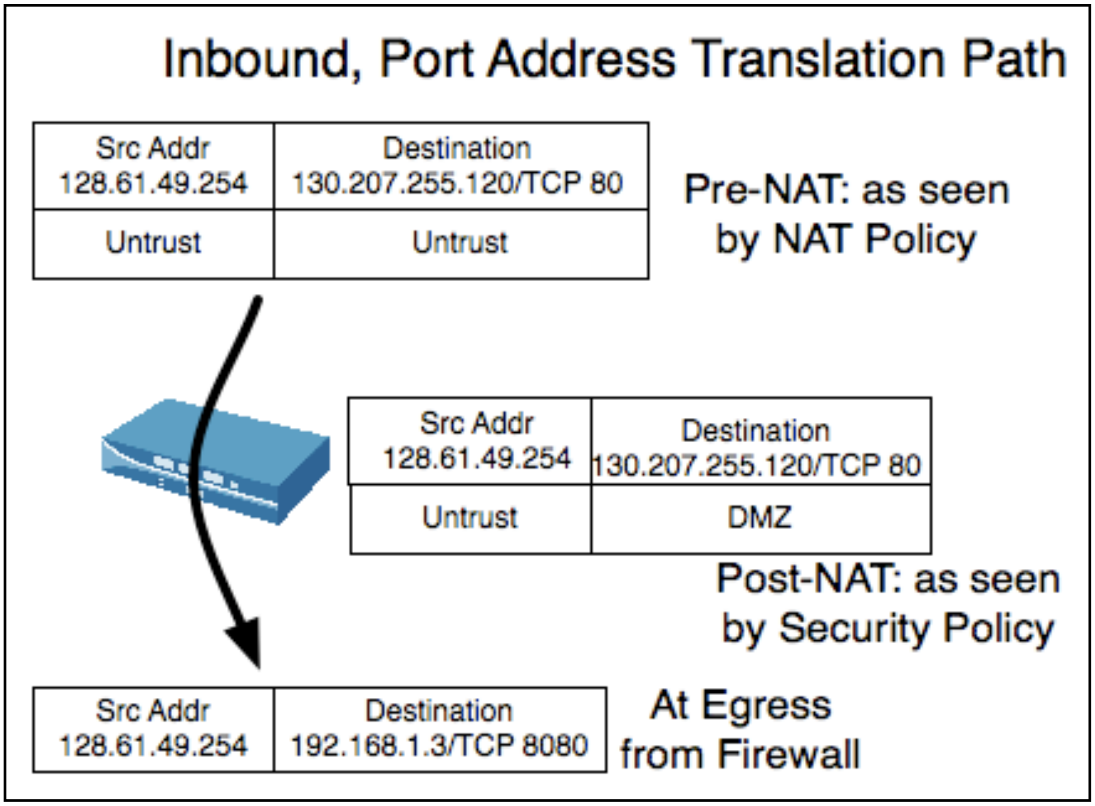
Example #2A: Multiple DMZ Servers, Limited Public IPs

Sometimes, organizations have a very limited number of IP addresses and are unable to assign public IP addresses to each internal server in a one-to-one fashion. When this is the case, traffic can be translated by matching on the incoming destination IP address and destination port.

The rules for this scenario will be almost identical to Example #2, except the service port will also be changed on egress.

This configuration can be used when there is a single, external IP address out to the Internet. Inbound traffic to servers can be mapped to different TCP ports on this public interface.





Inbound, Port Address Translation Path

Src Addr 128.61.49.254	Destination 130.207.255.120/TCP 80
Untrust	Untrust

Pre-NAT: as seen by NAT Policy

Src Addr 128.61.49.254	Destination 130.207.255.120/TCP 80
Untrust	DMZ

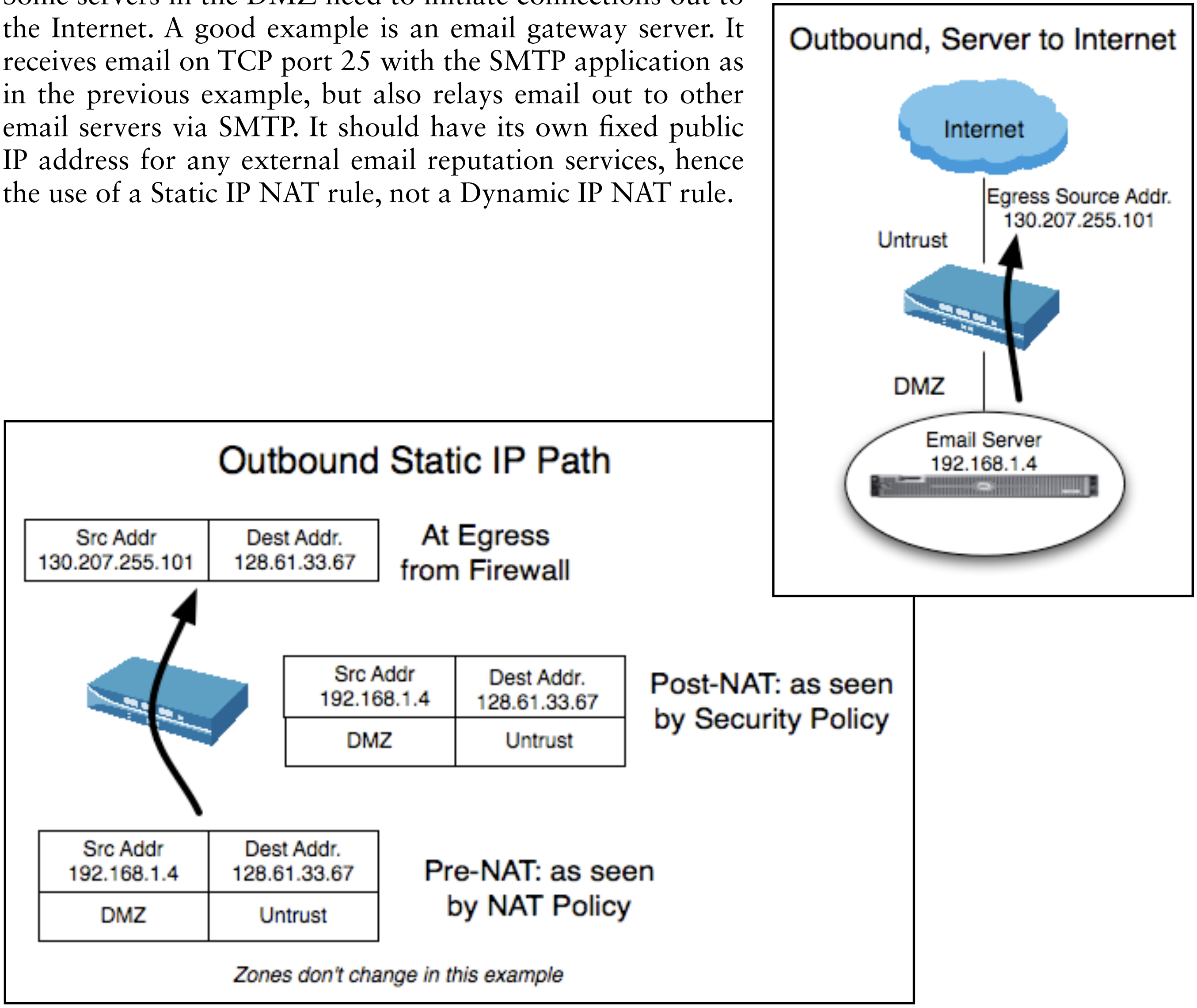
Post-NAT: as seen by Security Policy

Src Addr 128.61.49.254	Destination 192.168.1.3/TCP 8080

At Egress from Firewall

Example #3: DMZ Server Outbound to Internet

Some servers in the DMZ need to initiate connections out to the Internet. A good example is an email gateway server. It receives email on TCP port 25 with the SMTP application as in the previous example, but also relays email out to other email servers via SMTP. It should have its own fixed public IP address for any external email reputation services, hence the use of a Static IP NAT rule, not a Dynamic IP NAT rule.



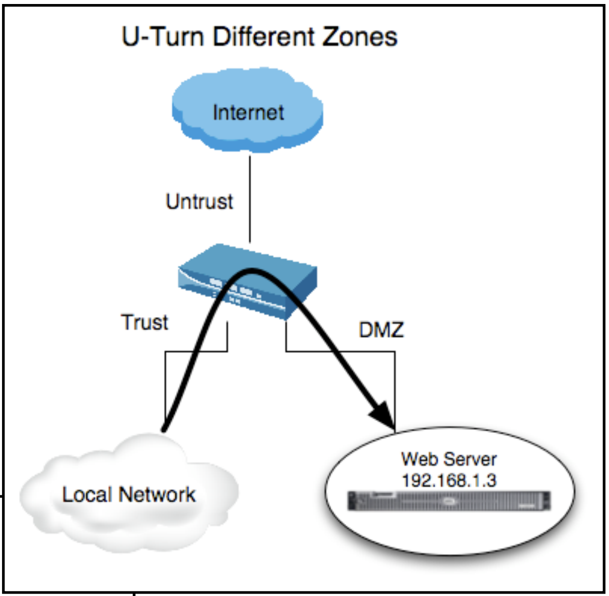
NAT Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Service**	**Translated Source**	**Translated Dest**
Outbound mail relaying	DMZ	Untrust	192.168.1.4	any	smtp25	130.207.1.101	none

Security Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Application**	**Service**	**Action**
Allow outbound mail relaying	DMZ	Untrust	192.168.1.4	any	smtp	application-default	allow

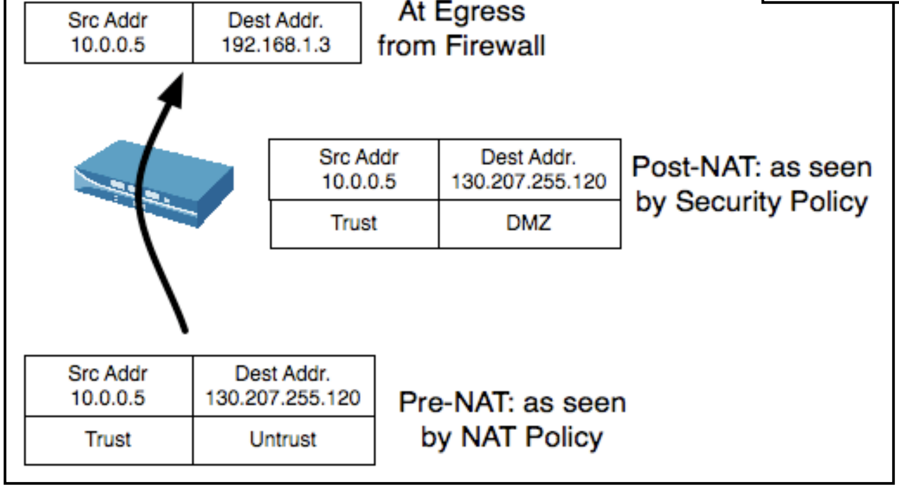
Example #4: U-Turn Between Zones

When internal users want to verify operation of their DMZ servers with the external IP addresses assigned to those servers, a rule sometimes referred to as a U-Turn is employed. This name comes about because the traffic logically appears to enter form the Internal zone, exit the Untrust zone, and finally enter the DMZ zone.

In reality, a correctly written set of rules will allow the traffic to enter from the trust zone and exit to the DMZ zone, in spite of using an address on the Untrust zone.



U-Turn Different Zones Path

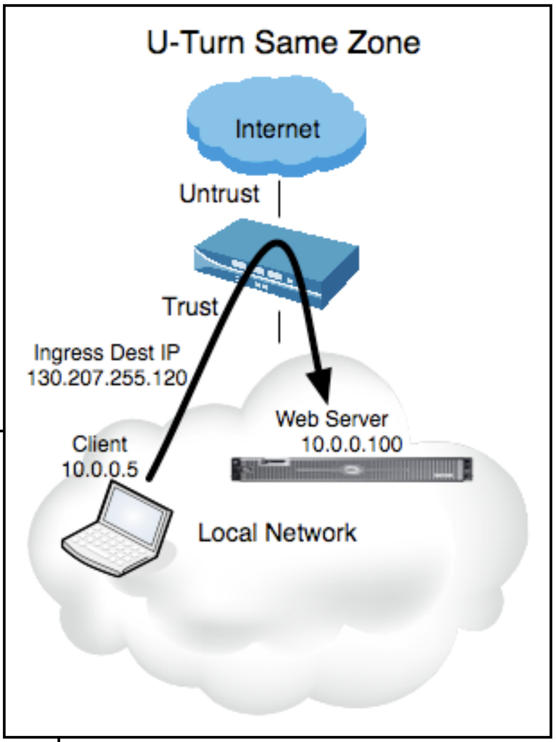


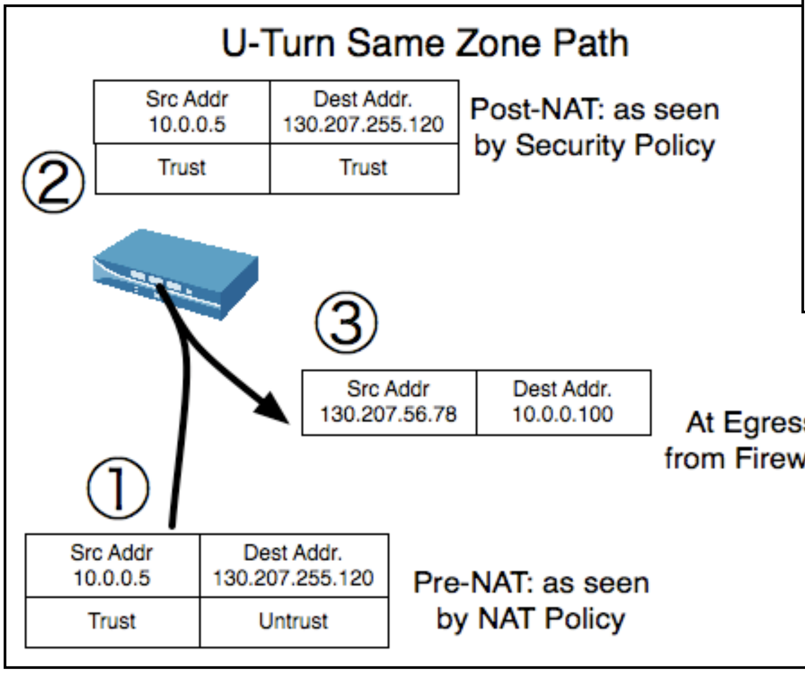
NAT Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Service**	**Translated Source**	**Translated Dest**
Internal users test DMZ server	Trust	Untrust	Any	130.207.255.120	http	none	192.168.1.3

Security Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Application**	**Service**	**Action**
Internal users test DMZ server	Trust	DMZ	Any	130.207.255.120	any	mytcp80	allow

Example #4A: U-Turn in the Same Zone

While not as common, sometimes an administrator wants to use the external IP address for a local server - while the administrator is on the same local network! Similar to the previous example, the destination zone lists the Untrust Network on arrival into the firewall. However, the source addresses must also have NAT applied, for if the server believes the client resides on the same network, it will send packets directly back instead of through the firewall.



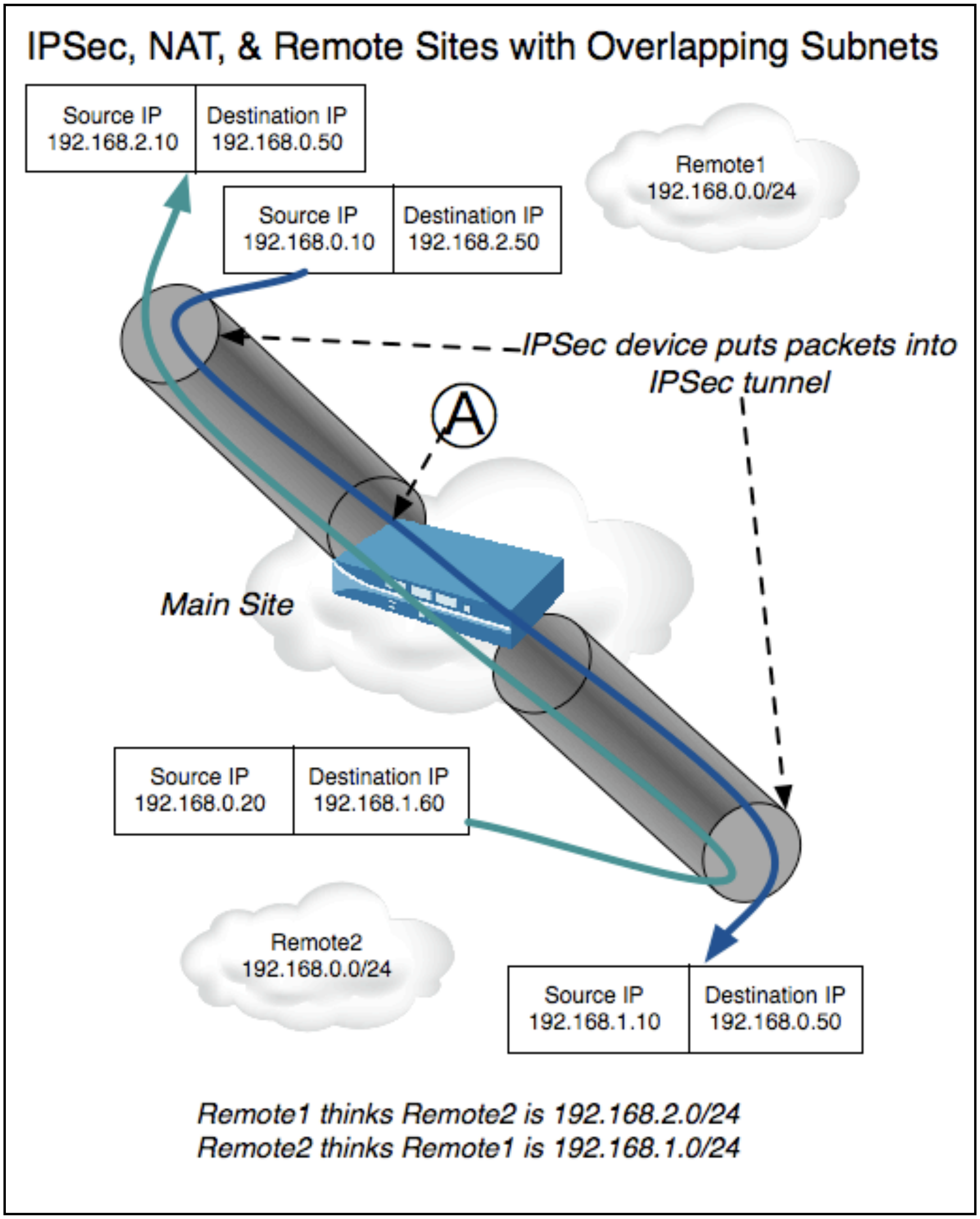


NAT Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Service**	**Translated Source**	**Translated Dest**
Internal users test DMZ server	Trust	Untrust	Any	130.207.255.120	http	130.207.56.78	192.168.1.3

Security Rule							
Comment	**Source Zone**	**Dest. Zone**	**Source Addr**	**Dest. Addr**	**Application**	**Service**	**Action**
Internal users test DMZ server	Trust	Trust	Any	130.207.255.120	any	mytcp80	allow

Example #5: Remote IPSec Site-To-Site with Static IPs

In a hub and spoke IPSec network, two remote sites connect with IPSec tunnels through a main site. If the two remote sites have the same local IP network, source and destination NAT can be used with a range of addresses and Static NAT to enable connectivity.



In the example above, each remote site believes the other site has been assigned a different subnet. In reality, both use the same network - 192.168.0.0/24.

Also note point ‘A’ above - the ingress point of the session from Remote1 to Remote2 into the firewall is shown in the diagram on page 20.

Two NAT rules are required, as listed below to statically NAT the entire range of IP addresses at both sites in each directions.

NAT Rule						
Source Zone	Dest. Zone	Source Addr	Dest. Addr	Service	Translated Source	Translated Dest
Remote1	Remote2	192.168.0.0/24	192.168.2.0/24	any	192.168.1.0/24	192.168.0.0/24
Remote2	Remote1	192.168.0.0/24	192.168.1.0/24	any	192.168.2.0/24	192.168.0.0/24

The security rules below allow all traffic between the remote sites. In reality, services would be restricted. The example below shows the simplest example of required security policy rules between the two sites. Also, because of zones, it is not necessary to specify the actual source and destination IP addresses unless the ranges are less than the networks covered by the zones listed in the rule.

For example, in the first rule below, we could specify the source address as 192.168.0.0/24 and the destination address as 192.168.2.0/24 - just like in the corresponding NAT rule - because the incoming IP addresses for packets are not changed (as far as ALL policies are concerned) until the packets actually egress from the firewall.

Security Rule						
Source Zone	Dest. Zone	Source Addr	Dest. Addr	Application	Service	Action
Remote1	Remote2	Any	Any	Any	Any	Allow
Remote2	Remote1	Any	Any	Any	Any	Allow

The diagram on the next pages shows how NAT and IPSec transform packets from the ingress point 'A' from the previous page. Very little changes from the original version of this flow diagram on page 5. The only change occur at Step 2, where the firewall first decrypt the packet, and in Step 6, when the firewall encrypt the packet to send into the second IPSec tunnel.

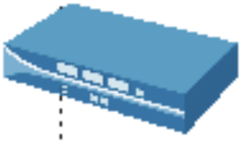
PAN-OS IPSec with Source & Destination NAT: Remote1 to Remote2 (session A)

	Source IP	Destination IP
IPSec Packet	192.168.0.10	192.168.2.50

①

② PAN-OS decrypts IPSec tunnel;
Assigns Source Zone based on interface packet ingressed;
Assigns Destination Zone based on interface packet *would* egress from

Source Zone	Destination Zone	Source IP	Destination IP
Remote1	Remote2	192.168.0.10	192.168.2.50



③ NAT rulebase checked for a matching rule

④ PAN-OS checks the interface the packet *will* egress from;
Changes Destination Zone if necessary

Source Zone	Destination Zone	Source IP	Destination IP
Remote1	Remote2	192.168.0.10	192.168.2.50

⑤ Security rulebase checked for a matching rule

⑥ Source and/or Destination IP address re-written per NAT rules;
packet encrypted for next IPSec tunnel

⑦ Packet Egresses

	Source IP	Destination IP
IPSec Packet	192.168.1.10	192.168.0.50

Limits/Capacity

		PA-2020	PA-2050	PA-4020	PA-4050 PA-4060
NAT Rule Limit Per Box		250	500	1,000	2,000
Concurrent Sessions supported per box		125,000	250,000	500,000	2,000,000

Dynamic IP/Port NAT

The use of dynamic IP/Port across all PAN-OS platforms is limited to 64,000 sessions per IP address. This is due to the inherent nature of sharing an IP address with TCP and UDP protocols.

In addition, per rule, only 3 dynamic IP/Port addresses can be used, resulting in a limit of 192,000 sessions per rule across PAN-OS.

Miscellaneous

- The PAN-OS proxy-arps for destination NAT addresses
- Since entries in the each rulebase always refers to the IP address of traffic as it enters the firewall, 2 different network objects should be created for servers when using an inbound Static IP - an External/Untrust version with the public address for the NAT rulebase, and a DMZ version with the real IP address for the Security rulebase
- NAT can only be used for traffic living on a Layer 3 interface
- traceroute is not supported with Dynamic IP/Port
- only TCP and UDP is supported with Dynamic IP/Port