CREATING AND MANAGING NAT POLICY RULES

GET OUTBOUND TRAFFIC FLOWING

- Network address translation
- Source NAT configuration
- Destination NAT configuration

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

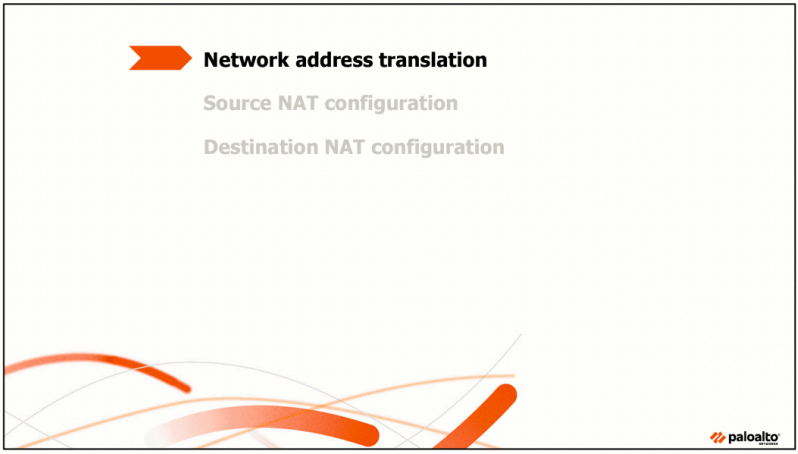
After you complete this module, you should be able to:

- Configure a NAT policy to implement source NAT
- Configure a NAT policy to implement destination NAT

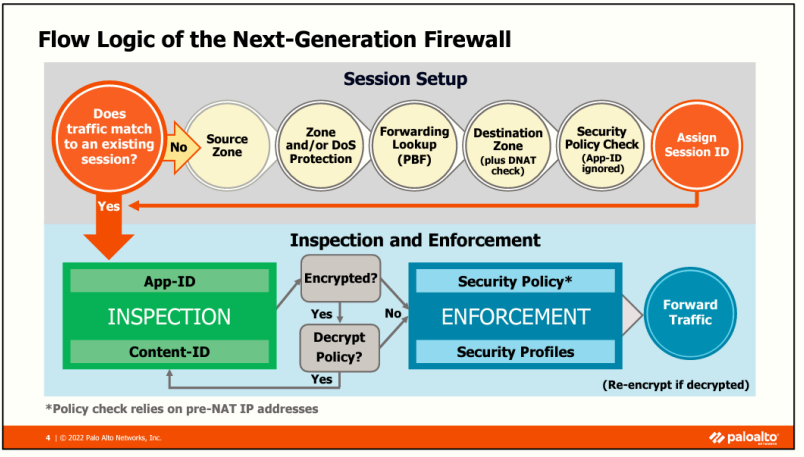
This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

- Configure a NAT policy to implement source NAT
- Configure a NAT policy to implement destination NAT



This section provides an introduction to network address translation.

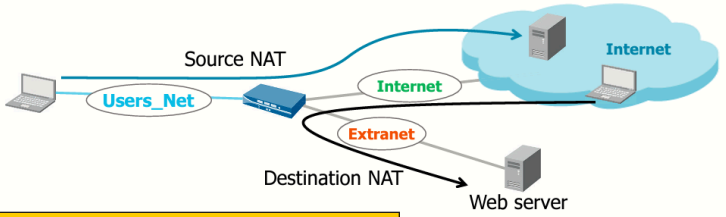


Administrators are better equipped to create Security policy rules and NAT policy rules if they understand how the firewall processes packets and uses NAT to translate IP addresses. Security policy rules must allow traffic manipulated by NAT policy rules.

The Layer 3 information is processed when the firewall receives the packet before the deep inspection of the packet, and its payload begins. At this stage in the logic flow, the NAT policy is evaluated to determine if packets would be subjected to a NAT policy rule and, if so, the kind of translation that is applicable. However, no translation has taken place yet. The packet retains all original header information. This retention has implications for the Security policy rules that will match the NAT traffic.

NAT Types

- Source NAT commonly is used for private (internal) users to access the public internet (outbound traffic).
- Destination NAT often is used to provide hosts on the public (external) network access to private (internal) servers.



For a Tech Doc about this topic, log into Live and search for "NAT Policy Overview"

Network Address Translation (NAT) rules provide address translation. NAT rules are different from security policy rules, which allow or deny packets. When a packet arrives at the firewall (ingress), the firewall inspects the packet and does a route lookup to determine the destination (egress) interface and zone. Then the firewall determines if the packet matches one of the NAT rules that have been defined, based on source and destination zone, and applies the NAT rule. The firewall then evaluates and applies any security policies that match the packet based on the original (pre-NAT) source and destination addresses, but the post-NAT zones. Security policies examine post-NAT zones to determine whether the packet is allowed or not. Because the very nature of NAT is to modify the source or destination IP addresses, which can modify the packet's outgoing interface and zone, security policies are enforced on the post-NAT zone.

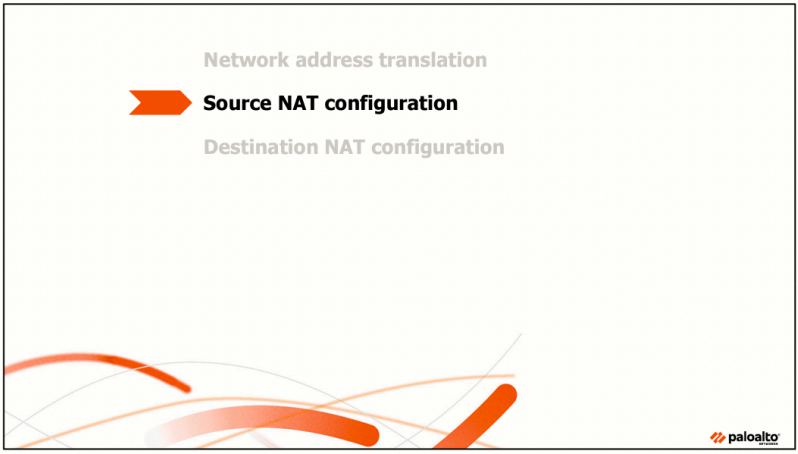
NAT configuration can take two forms: source NAT and destination NAT. The forms are directional and are described from the perspective of the NAT device, the firewall.

You often will use source NAT to translate the address of outbound traffic, traffic originating on a private network and being forwarded out toward the internet.

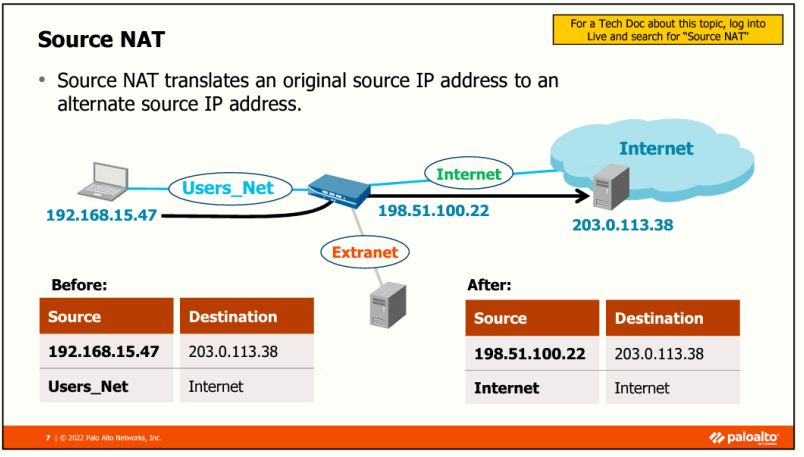
You often will use destination NAT to translate the address of inbound traffic, traffic coming from the internet into the local private network.

The firewall maintains the mapping of pre-NAT to post-NAT IP addresses for both source and destination NAT. In the example shown, both the *Users_Net* zone and *Extranet* zone are within the private network. The *Internet* link is the firewall's connection to the internet.

Note: This example shows the common practice of creating an Extranet or DMZ to segment externally accessible web servers securely.



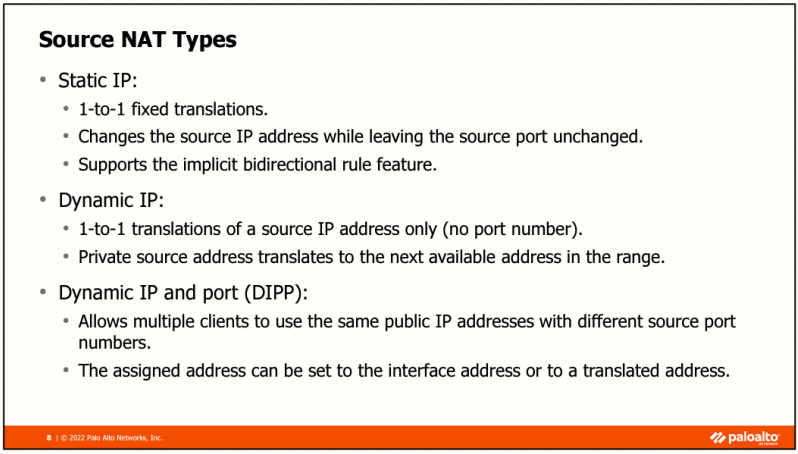
This section describes how source NAT operates and how to configure it on a firewall.



Source NAT, by definition, changes the source address of packets that match the NAT policy as the packets transit the firewall. Depending on the firewall configuration, source NAT also might change the source port number. Source NAT commonly is used to allow host devices configured with a private IP address to send and receive traffic on the internet.

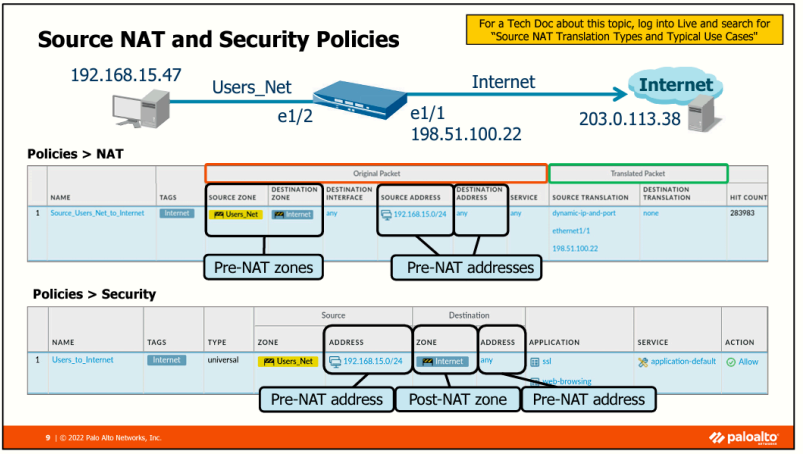
This diagram shows the firewall performing a source NAT function. A host residing at 192.168.15.47 on the private network needs to access a service residing at 203.0.113.38 on the public internet. The firewall receives the host traffic on the *Users_Net* interface. It forwards it on the *Internet* interface, replacing the source IP of the packet with the configured *Internet* interface IP of the firewall.

Without this translation, the ISP carrier's traffic from the host would be discarded because it would be sourced from a private address, 192.168.15.47. Source NAT translates the private address and makes the traffic routable across the internet.



Source NAT types provide the different administrator options for setting the size and nature of the translated source address pool. The firewall supports three ways of provisioning a translated source address pool:

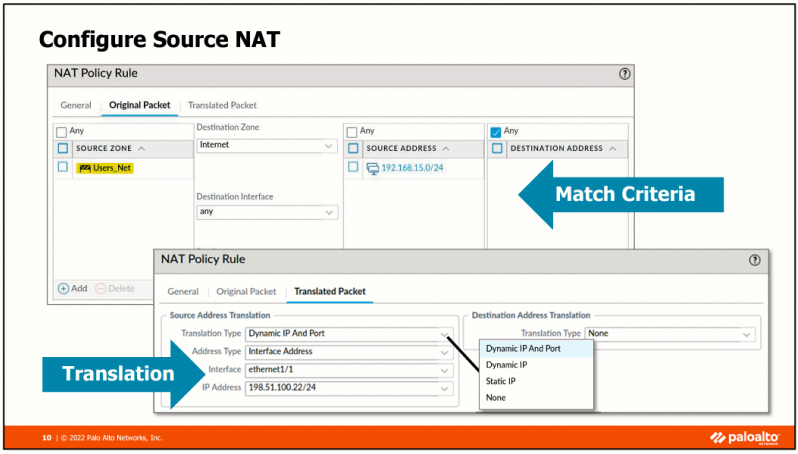
- Static IP: Static IP is used to change the source IP address while leaving the source port unchanged. **Note:** The bidirectional option in static source NAT rules implicitly creates a destination NAT rule for traffic to the same resources in the reverse direction.
- Dynamic IP: With this form of NAT, private source addresses are translated to the next available address in the specified address range. Dynamic IP NAT policies enable you to specify a single IP address, a range of IP addresses, a subnet, or a combination as the translation address pool. By default, if the source address pool is larger than the translated address pool, new IP addresses seeking translation are blocked while the translated address pool is fully used. You can choose to use a DIPP configuration if the pool is exhausted.
- DIPP: Multiple clients can use the same public IP address with different source port numbers. Dynamic IP and port NAT rules allow translation to a single IP address, a range of IP addresses, a subnet, or a combination. In cases where an egress interface has a dynamically assigned IP address, specify the interface itself as the translated address. By specifying the interface in the DIPP rule, you ensure that NAT policy updates automatically to use any address acquired by the interface for subsequent translations. You also can configure a new address to serve as the assigned address by choosing a translated address.



To configure source NAT, first, create a NAT policy rule. When creating a source NAT policy rule, identify the **Original Packet** characteristics. Use the fields in the **Original Packet** tab to define the match criteria used to select traffic for the NAT translation. A NAT policy rule matches the packet based on the original pre-NAT source and destination addresses and the pre-NAT destination zone.

Then, create a Security policy rule to support the NAT traffic flow. The Security policy rule will include **Source**, **Destination**, and **Application** characteristics, along with an **Action**. Because of the flow logic discussed, the Security policy rule is enforced after the NAT policy rule is evaluated but before the NAT translation is applied. Therefore, as is shown, a Security policy rule matches the packet based on the original pre-NAT source and destination addresses, but it matches the post-NAT destination zone. **Note:** The rule action must be configured as "Allow" to permit traffic matching the defined characteristics to cross the specified zone.

In this example, a host with the IP address 192.168.15.47 wants to connect to a server on the internet residing at IP address 203.0.113.38. The firewall administrator has configured a NAT policy rule to support this connectivity so that all traffic from the private network appears to come from the publicly routable address on the ethernet1/1 interface. For this configuration example, the administrator uses the DIPP type source NAT. When configuring DIPP, use **Address Type** to define addresses for the pool. There are two options: The **Translated Address** option uses a new address, not on an external interface. It is used for interfaces that receive an IP address dynamically from a pool. The **Interface Address** option uses a current address on an external interface. In the example shown, the **Interface Address** option was used, and the interface specified is ethernet1/1 with IP address 198.51.100.22.



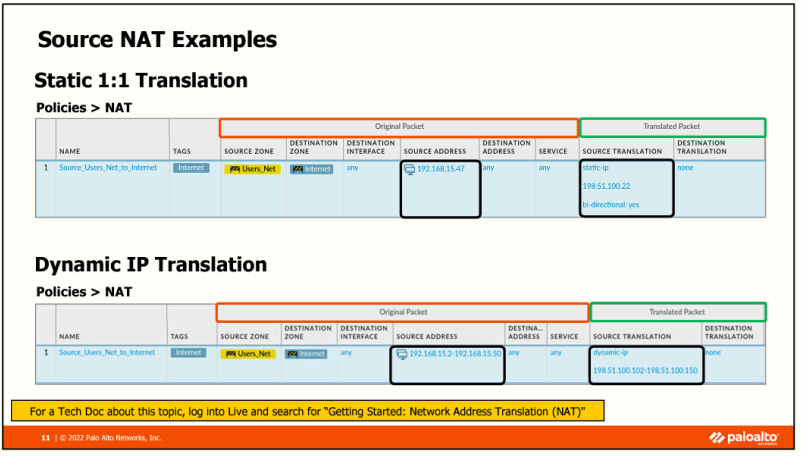
NAT rules are based on source and destination zones, source and destination IP addresses, and application services. As with Security policy rules, NAT policy rules are compared against incoming traffic in sequence. The first rule that matches the traffic is applied. Every NAT policy rule is configured in the web interface under **Policies > NAT**.

To configure source NAT, use the **Original Packet** tab to define the source and destination zones of the packets that the firewall will translate and, optionally, specify the destination interface and type of service. You can configure multiple source and destination zones of the same type and apply the rule to specific networks or specific IP addresses. Click the **Translated Packet** tab to configure the type of translation to perform on the source and the address and port to which the source will be translated.

Although the **General** tab is not shown here, it is used to name the NAT policy and specify which type of traffic the NAT rule will translate. Options are:

- **ipv4** for translation between IPv4 addresses.
- **nat64** (pronounced “NAT 6-to-4”) for translation between IPv6 and IPv4 addresses. This option most commonly is used for connecting IPv6 corporate intranets to the internet.
- **natv6** for translation between IPv6 addresses.

Examples in this module will use translation type IPv4 because it is the most common type implemented.



Translated Packet characteristics determine which translation will be done with packets that match the criteria defined under the **Original Packet** tab. **Translated Packet** characteristics include translation types. Two translation types correspond to the two kinds of source NAT:

- Static IP: For this type, a single **Original Packet** IP address is mapped to a single **Translated Packet** IP address. The same address always is used, and the port is unchanged. For example, if the configured source range is 192.168.15.1 to 192.168.15.10 and the configured translation range is 198.51.100.1 to 198.51.100.10, address 192.168.15.2 is always translated to 198.51.100.2. However, the number of source IPs using this policy must match the translated address range.
- Dynamic IP: With this type of NAT, the following available address in the specified range is used, but the port number is unchanged. Each concurrent session uses an address from the configured pool, making it unavailable to other source IPs. This option most commonly is used when there are two or more public IPs from the ISP but not enough public IPs to allocate one to each internal host on the network, and you want to assign them to outbound hosts only as needed.

Be careful when using dynamic IP. The translated pool of addresses can be exhausted if the number of internal hosts concurrently creating outbound sessions exceeds the number of IP addresses in the dynamic pool. You can protect against IP address exhaustion by setting the **Advanced (Dynamic IP/Port Failback)** button (in the **Translated Packet** tab when you choose dynamic IP), which results in the use of DIPP if the dynamic IP pool runs out of unused IP addresses.

Source NAT Examples (Cont.)

Dynamic IP and Port Translation

Policies > NAT

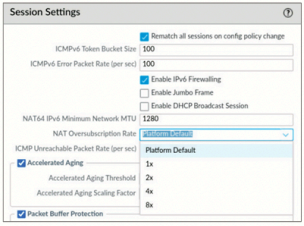
With the DIPP type of NAT, an available address in the specified range can be used multiple times because the address is paired with a different port number each time. This option most commonly is used when there are one or more public IP addresses from the ISP and not enough public IP addresses to allocate one address to each internal host on the network. Because each address is used multiple times by pairing it with a unique port number, DIPP mitigates the problem of having more internal hosts than external, routable IP addresses.

DIPP NAT Oversubscription

For a Tech Doc about this topic, log into Live and search for "Dynamic IP and Port NAT Oversubscription"

- The same translated IP address and port pair can be used multiple times in concurrent sessions:
  - Assumes that hosts are connecting to different destinations

Device > Setup > Session > Session Settings



Internal Source Port	Firewall Source Port	Destination Address
26435	198.51.100.22:25661	51.6.33.12
35435	198.51.100.22:25661	161.8.55.4
21569	198.51.100.22:25661	201.55.45.1
51043	198.51.100.22:25661	17.39.25.6

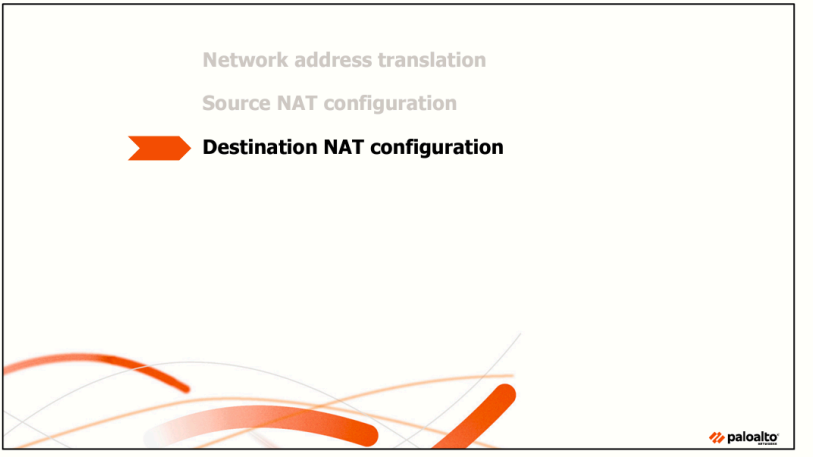
Concurrent sessions = oversubscription rate (8/4/2) x address pool size

13 | © 2022 Palo Alto Networks, Inc.

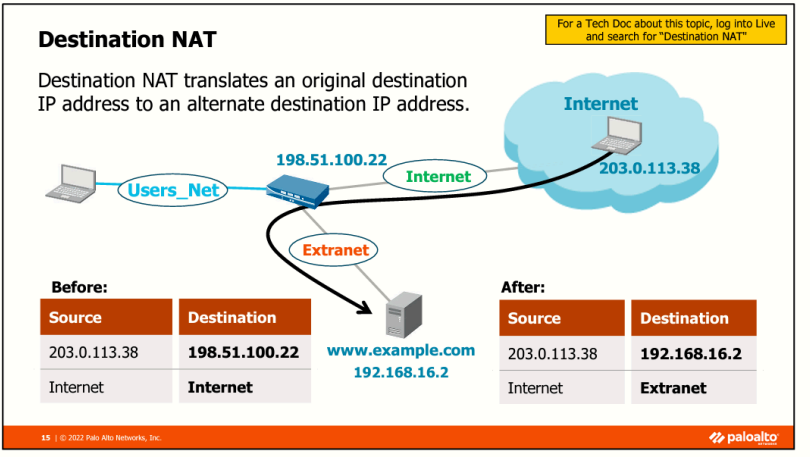
For a given IP address, the TCP protocol recognizes a maximum of about 64,000 port numbers (16 header bits for source port yields 65,536 total – 1,024 well-known = 64,512 available ports). Based on this limitation, DIPP source NAT will support a maximum of about 64,000 concurrent sessions on each IP address configured within the NAT pool.

On some platforms, the PAN-OS DIPP NAT implementation supports oversubscription. Oversubscription allows the reuse of port numbers by using the destination IP address as an additional NAT session identifier. In the example, the same post-NAT translated source IP and source port are used for traffic streams flowing to four different IP addresses, which constitutes 4x oversubscription.

The NAT oversubscription rate is configurable up to the maximum rate supported by the platform. For information about how to display the oversubscription information for each firewall model, log into Live and search for "Product Selection" or see the documentation at https://www.paloaltonetworks.com/network-security.



This section describes how destination NAT operates and how to configure it on a firewall.



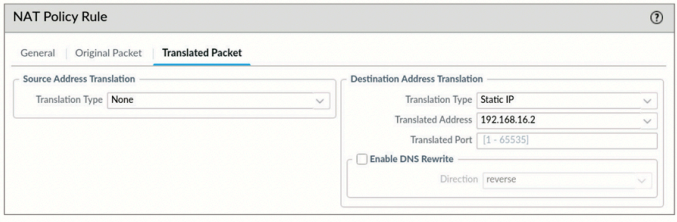
Destination NAT by definition, will change the destination address in the IP header of packets that match the NAT policy as they transit the firewall. Destination NAT commonly is used to make a server within a private network reachable from the public internet.

In the example shown, a user at an external system with the IP address 203.0.113.38 queries the DNS server for the IP address of the webserver www.example.com. The DNS server returns an address of 198.51.100.22, which is the external address of the firewall interface in the *Internet* zone. For the packet to reach the webserver, the destination IP address must be translated to the private IP address 192.168.16.2.

Destination NAT Attributes

- Static IP:
  - 1-to-1 fixed translations
  - Changes the destination IP address while leaving the destination port unchanged
  - Also enabled by static source NAT with the **Bi-directional** option set

Policies > NAT > Add

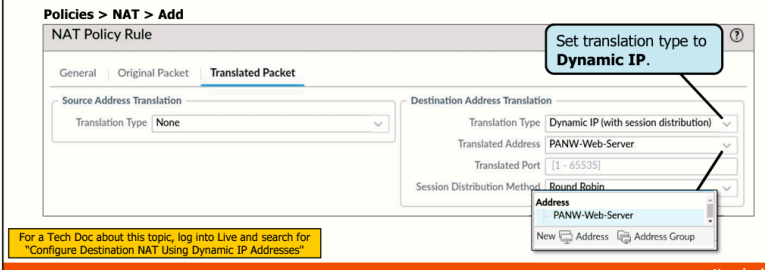


Destination NAT provides the administrator options for provisioning public access to servers and services within their network. Destination NAT uses static IP mapping with optional port forwarding.

Static IP is used for one-to-one translation of inbound traffic. Static IP allows you to change the destination IP address and, optionally, the port. When destination address translation is 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. Use static IP to change the destination IP address while leaving the destination port unchanged.

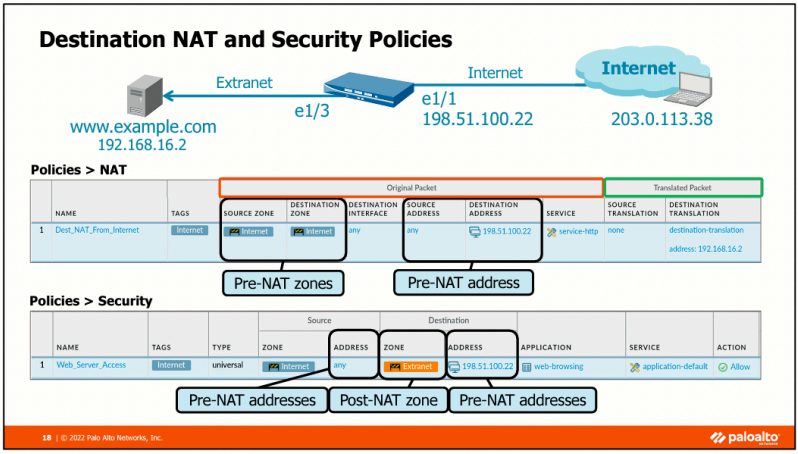
Dynamic IP Address Support for Destination NAT

- Translates original IP address to destination host with a DHCP-assigned IP address.
- Translated address can be an FQDN, address object, or address group.



In PAN-OS 8.1, destination NAT was enhanced to translate the original destination address to a destination host with a DHCP-assigned IP address. The translated address can be an FQDN, an address object, or an address group that uses an FQDN. After the DHCP server assigns a new address to the host, you will not have to manually update the FQDN, the DNS server, or the NAT policy rule. You also will not need to use a separate external component to update the DNS server with the latest FQDN-to-IP address mapping. This translation type is in addition to the static, one-to-one translation that previously was the only type of destination NAT available.

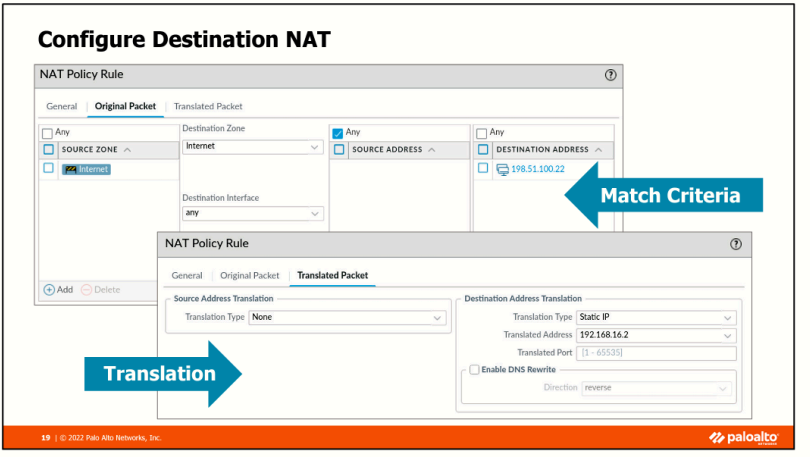
Suppose an FQDN in the translated destination address resolves to more than one address. In that case, the firewall automatically will distribute translated sessions among those addresses, based on a round-robin algorithm, to provide more equitable session loading. Each FQDN can support up to 32 IPv4 addresses and 32 IPv6 addresses. If a DNS server returns more than 32 addresses for an FQDN, the firewall uses the first 32 addresses in the packet.



To configure destination NAT, first, create a NAT policy rule. When creating a destination NAT policy rule, identify the **Original Packet** characteristics. Use the fields in the **Original Packet** tab to define the match criteria used to select traffic for the NAT translation. A NAT policy rule matches the packet based on the original pre-NAT source and destination addresses and the pre-NAT destination zone. Use the **Translated Packet** tab to specify packets' desired translation that meets the **Original Packet** criteria.

Then, create a Security policy rule to support the NAT traffic flow. The Security policy rule will include **Source**, **Destination**, and **Application** characteristics, along with an **Action**. Because of the flow logic discussed, the Security policy is enforced after the NAT policy is evaluated but before the NAT translation is applied. Therefore, as is shown, the Security policy rule matches the post-NAT destination zones and the pre-NAT destination IP addresses.

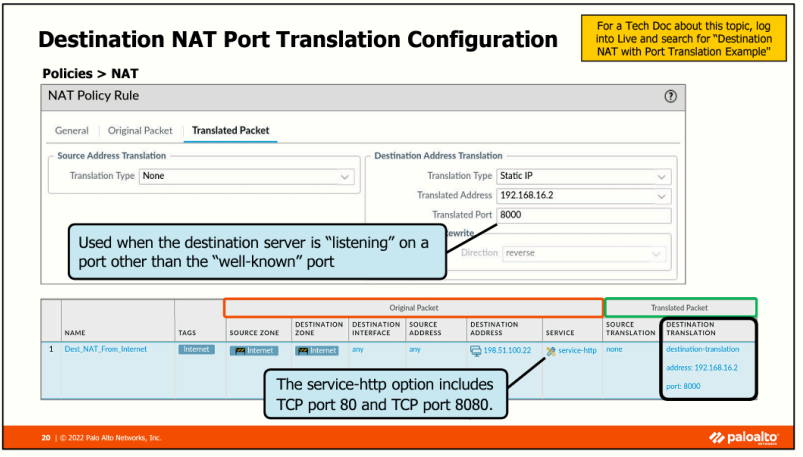
In this example, a user with IP address 203.0.113.38 wants to browse webpages hosted at www.example.com. Though DNS resolution is not shown in the diagram, you should assume that www.example.com is associated with 198.51.100.22, the IP address on the e1/1 interface of the firewall. To support this connectivity, the firewall administrator has configured a destination NAT policy rule so that traffic arriving at e1/1 destined for 198.51.100.22:80 has its destination address changed to 192.168.16.2:80 to match the service-http specification. After the firewall determines the translated address, the firewall performs a route lookup to determine the egress interface. In this example, the egress interface is e1/3. The administrator has configured a security policy rule to support this traffic flow. The Security policy rule permits web browsing traffic from the pre-NAT zone (Internet), with a pre-NAT destination IP address of 198.51.100.22 to cross into the *Extranet* zone.



Configuration of destination NAT is similar to the configuration of source NAT. As with source NAT, destination NAT uses the **Original Packet** tab to define the source and destination zones of the packets that the firewall will translate and, optionally, specify the destination interface and type of service.

You can configure multiple source and destination zones of the same type, and you can apply the rule to specific networks or a specific IP address. Click the **Translated Packet** tab and select the **Destination Address Translation** check box to flag this rule as a destination NAT rule. Leave the **Translation Type** in **Source Address Translation** set to **None** if this is a destination NAT-only rule.

Note: NAT rules must be configured to use the zones associated with pre-NAT IP addresses configured in the policy. In the example, the source and destination zones are the same. A Security policy differs from the NAT policy because post-NAT zones must control traffic. NAT may influence the source or destination IP addresses, modifying the outgoing interface and zone. After creating security policy rules with specific IP addresses, the pre-NAT IP addresses are used in the Security policy rule match. Traffic subjected to NAT must be permitted explicitly by the Security policy when traffic traverses multiple zones.



PAN-OS software supports two destination NAT types:

- Static IP, which is used for one-to-one translation of inbound traffic. Configuration of static IP destination NAT changes the destination IP address while leaving the destination port unchanged.
- Port forwarding is a technique used to manage traffic through NAT policies based on destination port numbers. For example, assume that a company has three separate servers: one for email, one for web hosting, and an application server in a zone named Server-Trust. All systems in Server-Trust are configured with a NAT policy to appear as if they have the same IP address. When traffic is received at the shared address, the port forwarding feature of the inbound NAT policy can send the traffic to the appropriate server based on the destination port associated with the session.

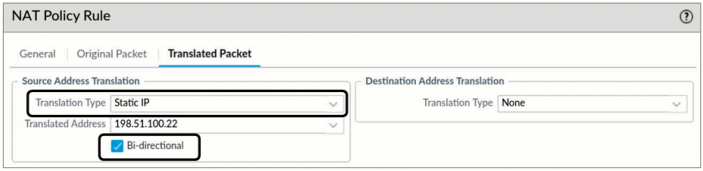
To configure destination NAT, enter an IP address or range of IP addresses and a translated port number (1 to 65535) that the destination address and port number are translated to. If the **Translated Port** field is blank, the destination port is not changed. Destination translation is typically used to allow an internal server, such as an email server, to be accessed from the public network.

You can complete the **Translated Address** field with either an IP address or an Address object. Address objects are named objects configured on the firewall to help administrators complete configurations with a predefined address. To configure Address objects, go to **Objects > Addresses**.

Configure Bidirectional Source NAT

- Enables internal servers to send and receive traffic through the firewall
- Available only for static NAT

Policies > NAT



For a Tech Doc about this topic, log into Live and search for "Enable Bi-Directional Address Translation"

Your public-facing servers must be able to both send and receive packets. You need a reciprocal policy that translates the public address (the destination IP address in incoming packets from internet users) into the private address so that the firewall can route the packet to an IP address on your internal network. You create a bidirectional static NAT rule. The bi-directional translation is an option for static NAT only.

To create a bidirectional source NAT rule, select the **Bi-directional** check box as shown in the example. This action creates an invisible rule in your NAT policy that enables the server to send and receive network traffic through the firewall.

Module Summary

Now that you have completed this module, you should be able to:

- Configure a NAT policy to implement source NAT
- Configure a NAT policy to implement destination NAT

Now that you have completed the module, you should be able to perform the tasks listed.

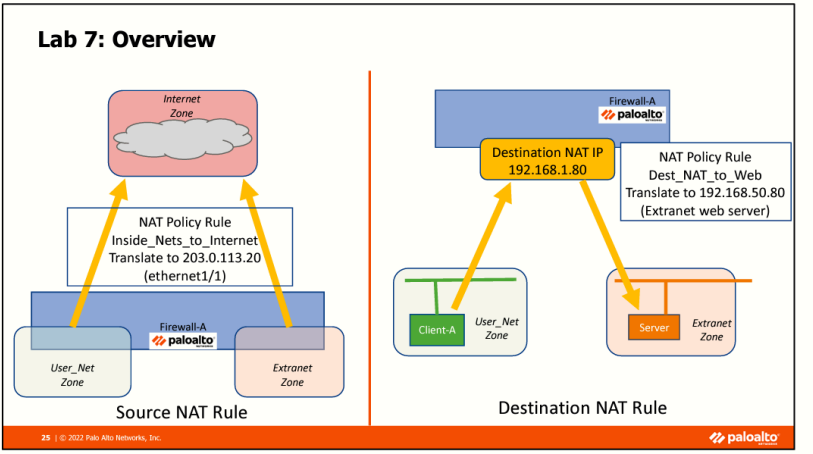
Additional Resources

For a digital review of this module, log into Beacon and search for:

"Next-Generation Firewall Setup and Management Connection"

Review Questions

1. NAT oversubscription is used in conjunction with which NAT translation type?
   a. static
   b. dynamic IP
   c. dynamic IP and port
   d. dynamic IP with session distribution
2. Which source NAT type changes the course IP address while leaving the source port unchanged?
   a. Static IP
   b. Dynamic IP
   c. Dynamic IP and port
3. When configuring a destination NAT Security policy, what destination address would you use?
   a. address of the web server
   b. address of the egress firewall interface
   c. address of the ingress firewall interface
4. True or false? Source NAT is commonly used for private users to access the public internet.
   a. true
   b. false



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 7: Creating and Managing NAT Policy Rules

- Configure source NAT
- Configure destination NAT

Answers to Review Questions

1. c
2. a
3. c
4. a (true)