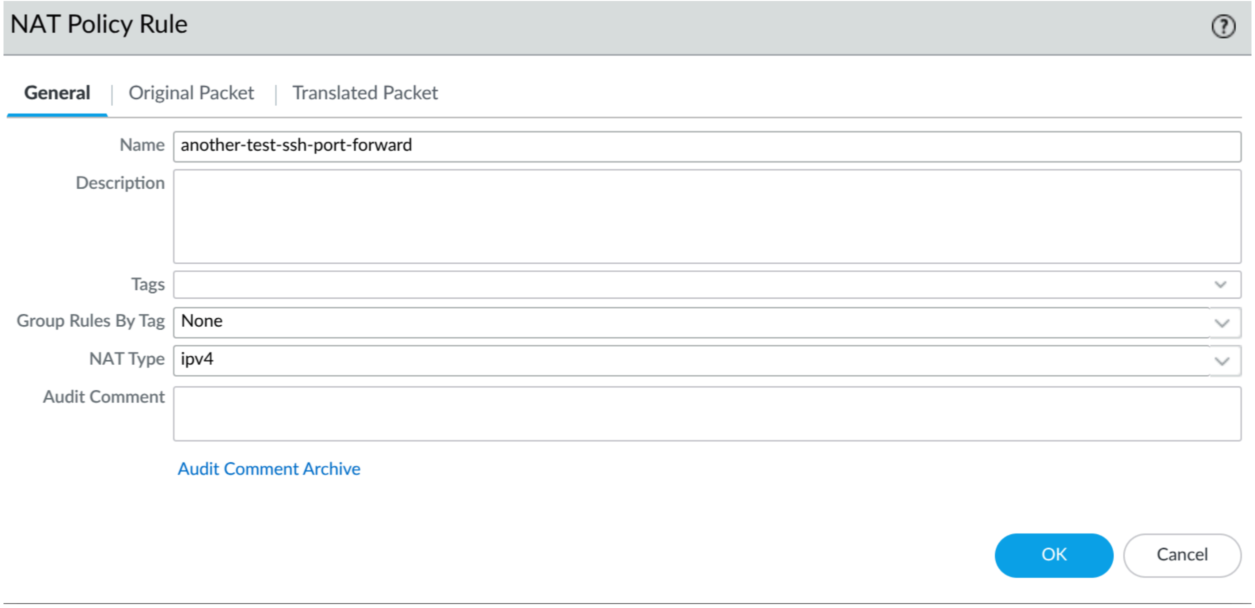
Purpose

Set up a NAT rule that forwards incoming SSH traffic from the **WAN Zone** on port `2222` to an internal server (`10.0.2.2`) on port `22`.

Final Version of DNAT Configuration

Step 1: Create a NAT Rule

1. **Go to NAT Policies**:
   - Navigate to **Policies > NAT** in the Palo Alto Web Interface.
2. **Add a New NAT Rule**:
   - Click **Add** to create a new NAT policy.
3. **Name the NAT Rule**:
   - Enter a descriptive name, e.g., `PortForward-SSH`.



NAT Policy Rule

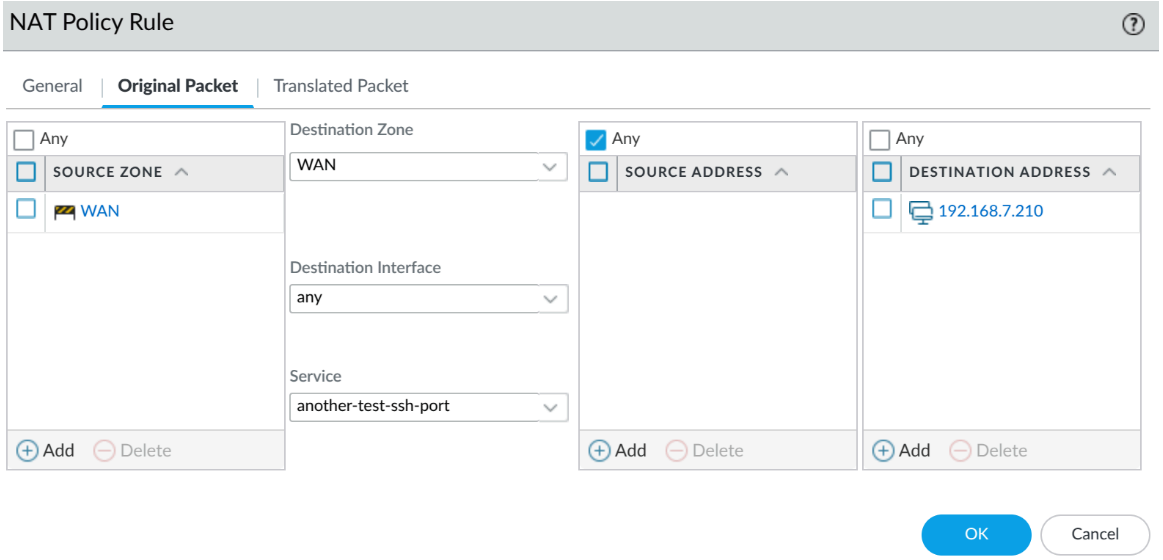
General | Original Packet | Translated Packet

Name	another-test-ssh-port-forward
Description	
Tags	
Group Rules By Tag	None
NAT Type	ipv4
Audit Comment	

Step 2: Configure the Original Packet

1. **Source Zone**:
   - Set the **Source Zone** to `WAN`.
   - This specifies that the traffic originates from the internet.
2. **Destination Zone**:
   - Set the **Destination Zone** to `WAN`.
   - This specifies that the destination is the public IP on the WAN interface.
3. **Destination Interface**:
   - Leave the **Destination Interface** as **Any**.

4. **Service**:
   - **Create a New Custom Service**:
     - Click **Add** to define a custom service for the incoming traffic.
     - **Name**: `SSH-2222`.
     - **Protocol**: Select **TCP**.
     - **Destination Port**: Enter `22` (this is the port it will enter on the system).
     - Leave **Source Port** as 2222 (or this is the external port users will connect to).
     - Save the service and select it in the NAT rule.
5. **Destination Address**:
   - Specify the **public IP address** of your WAN interface, e.g., `192.168.7.210`


NAT Policy Rule

General | **Original Packet** | Translated Packet

☐ Any
☐ SOURCE ZONE
☐ WAN

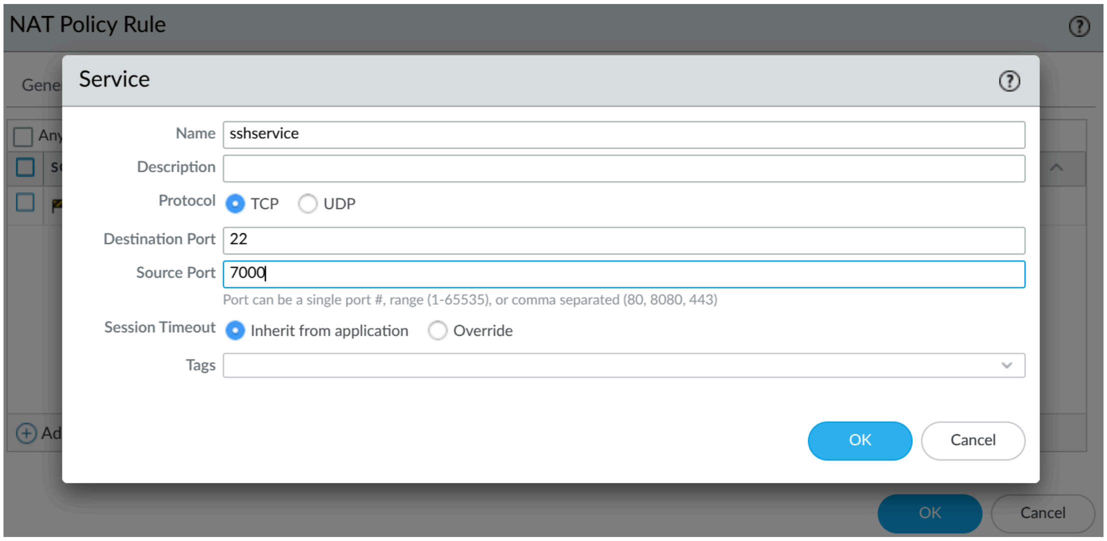
Destination Zone: WAN

Destination Interface: any

Service: another-test-ssh-port

☑ Any
☐ SOURCE ADDRESS

☐ Any
☐ DESTINATION ADDRESS
☐ 192.168.7.210


NAT Policy Rule

Service

Name: sshservice

Description:

Protocol: ● TCP ○ UDP

Destination Port: 22

Source Port: 7000

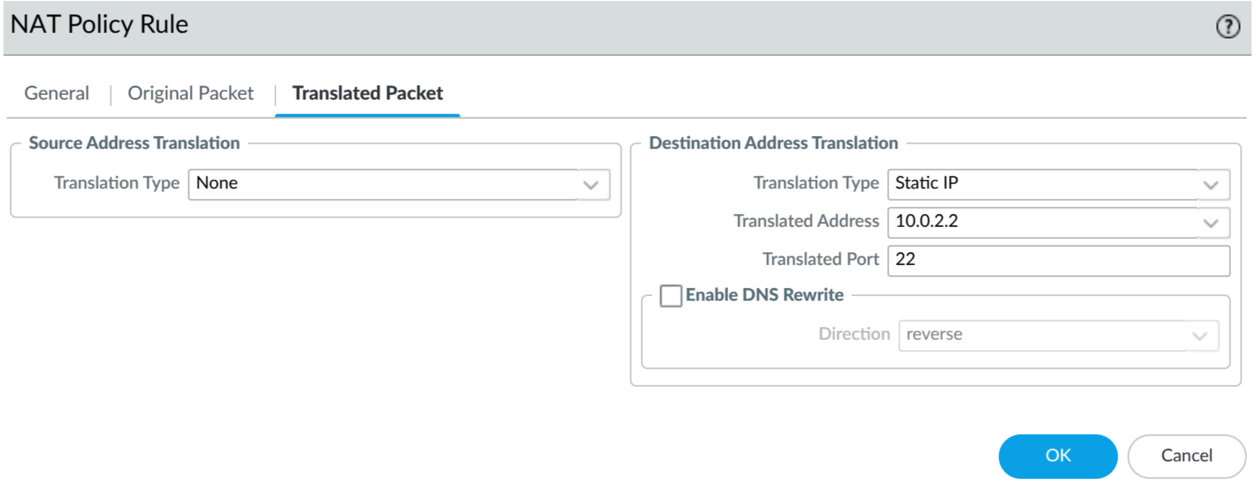
Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)

Session Timeout: ● Inherit from application ○ Override

Tags:

Step 3: Configure the Translated Packet

1. **Translation Type**:
   - Select **Destination Address Translation**.
2. **Translated Address**:
   - Enter the **internal IP** of the target server (e.g., `10.0.2.2` for the SSH server).
3. **Translated Port**:
   - Set the port to **22** (standard SSH port on the internal server).
4. **Save the Rule**:
   - Click **OK** to save the NAT rule.



NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: Static IP

Translated Address: 10.0.2.2

Translated Port: 22

□ Enable DNS Rewrite

Direction: reverse

Create a Security Policy

NAT rules only handle the translation of traffic; you also need a **Security Policy** to allow the forwarded traffic.

1. **Go to Security Policies**:
   - Navigate to **Policies > Security**.
2. **Add a New Security Policy**:
   - Click **Add** to create a new policy.
3. **Name the Security Policy**:
   - Give it a name, e.g., `Allow-WAN-to-SSH`.
4. **Source Zone**:
   - Set the **Source Zone** to `WAN`.
5. **Destination Zone**:
   - Set the **Destination Zone** to `LAN` (or wherever the internal server resides).

6. **Source Address**:
   - Leave as **Any** (or restrict to trusted IPs for tighter security).
7. **Destination Address**:
   - Set the **Destination Address** to the **public IP** of your WAN interface (e.g., `192.168.7.100`).
8. **Application**:
   - Select **SSH** (or **Any** for testing purposes).
9. **Action**:
   - Set the action to **Allow**.
10. **Save and Commit**:
    - Save the policy and click **Commit**.

.