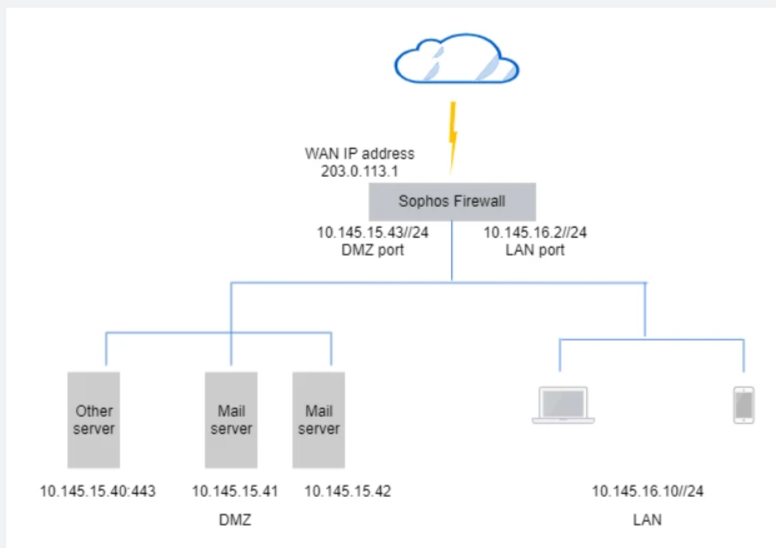
Step-1. Configure a port forwarding rule

You can create a port forwarding rule to forward incoming SMTP and SMTPS traffic to mail servers based on the ports.

## **Network diagram**



This example shows how to forward SMTP and SMTPS traffic, which use ports 25 and 587, to the mail servers in the DMZ.

You must configure the following rules and settings:

1. Destination NAT (DNAT) rule: Translates traffic from external sources to the internal mail servers.
2. (Optional) Loopback NAT rule: Translates traffic from internal sources to the internal mail servers.
3. Reflexive NAT rule: Translates outgoing traffic from the servers.
4. Firewall rules: Allow incoming and outgoing mail server traffic.

## **Configure NAT rule with port forwarding**

To forward SMTP and SMTPS traffic to the mail servers, do as follows:

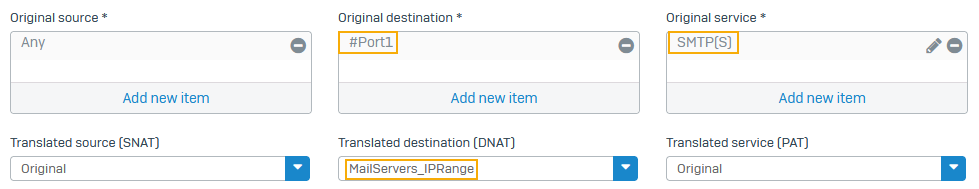
1. Go to **Rules and policies** > **NAT rules** and select **IPv4**.
2. Click **Add NAT rule** and click **New NAT rule**.
3. Specify the rule name and rule position.
4. Set **Original destination** to **Port1**.
5. Set **Translated destination** to the IP host MailServers\_IPRange.

In this example, the IP host is configured with the mail servers' IP range shown in the network diagram.

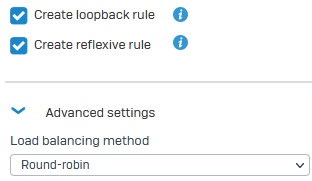
1. Set **Original services** to **SMTP(s)**.

The default destination ports for the service are 25 and 587 on the firewall.

1. Set **Translated services** to **Original**.



1. (Optional) Select **Create loopback rule** to translate traffic from internal users to the internal mail servers.
2. Select **Create reflexive rule** to create a source NAT rule that translates outgoing traffic from the mail servers.
3. Set **Load balancing method** to **Round-robin**.
4. Click **Save**.



## **Configure firewall rule for incoming traffic**

Configure a firewall rule to allow incoming traffic from internal and external sources to the mail servers.

1. Go to **Rules and policies** > **Firewall rules** and select **IPv4**
2. Click **Add firewall rule** and click **New firewall rule**.
3. Set **Source zones** to **LAN** and **WAN**.

The settings allow traffic from internal and external sources.

1. Set **Destination zones** to **DMZ**.

In this example, the mail servers are in the DMZ.

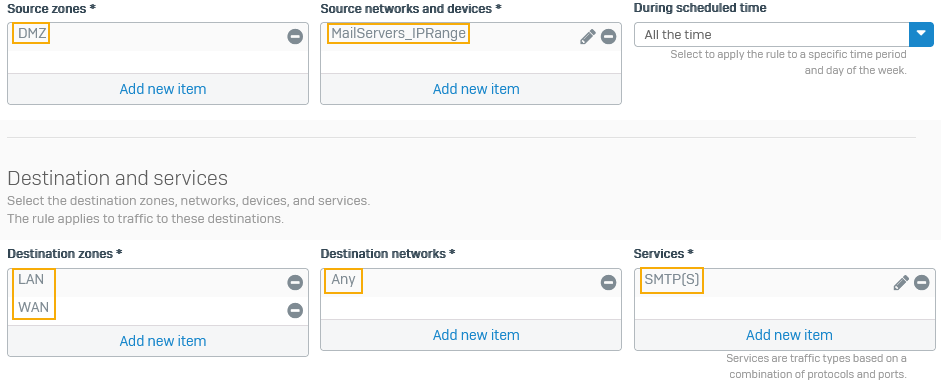
1. Set **Source networks and devices** to **Any**.
2. Set **Destination networks** to MailServers\_IPRange.
3. Set **Services** to **SMTP(s)**.
4. Click **Save**.

## Firewall rule corresponding to the DNAT rule

## **Configure firewall rule for outgoing traffic**

Configure a firewall rule to allow outgoing traffic from the mail servers to internal and external sources.

1. Go to **Rules and policies** > **Firewall rules** and click **IPv4**.
2. Click **Add firewall rule** and click **New firewall rule**.
3. Specify the rule name and rule position.
4. Set **Source zones** to **DMZ**.
5. Set **Destination zones** to **LAN** and **WAN**.
6. Set **Source networks and devices** to MailServers\_IPRange.
7. Set **Destination networks** to **Any**.
8. Set **Services** to **SMTP(s)**.
9. Click **Save**.



# STEP-2 Create a source NAT rule

This example shows how to create a source NAT rule to translate outgoing traffic from the LAN zone.

## **Objectives**

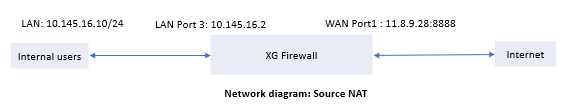
When you complete this unit, you'll know how to do the following:

* Create a source NAT rule to translated outgoing traffic from the LAN.
* Create a firewall rule to allow outgoing traffic from LAN to WAN zone.

## **SNAT network diagram**

Source NAT is typically used to translate outgoing traffic from the internal network to external resources on the internet. The source IP address is translated, keeping it private. The following network information is illustrative:

* Pre-NAT IP address of LAN users: 10.145.16.10/24
* Post-NAT IP address of LAN users: MASQ (IP address of the applicable outbound interface)



Here's an example:

* Source NAT from the internal network to WAN: Network LAN (10.145.16.0/24) to Any
* Firewall rule to allow traffic from LAN zone to WAN: LAN to Any

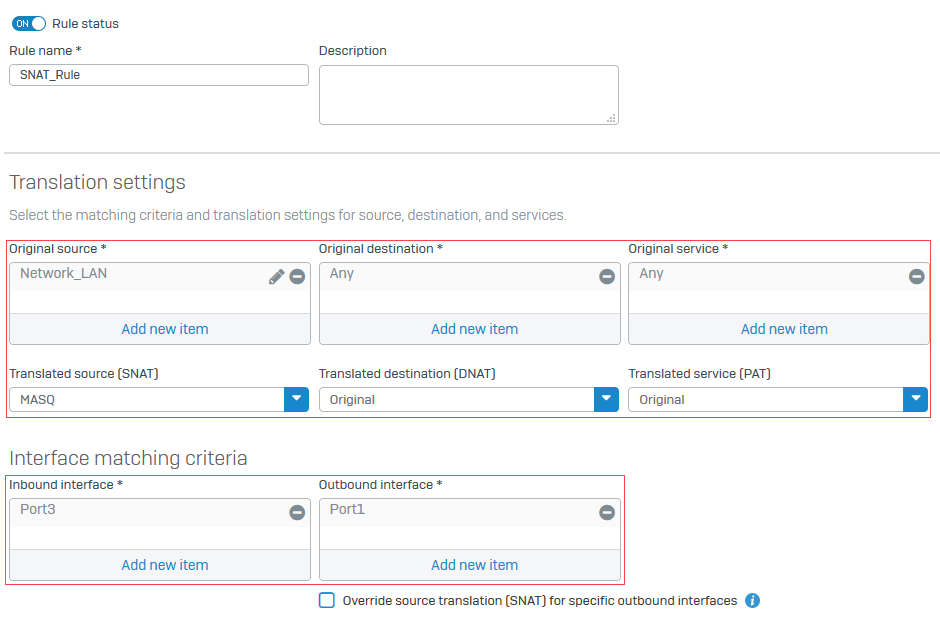
## **Specify the NAT rule settings**

1. Go to **Rules and policies** > **NAT rules**, select **IPv4** or **IPv6** and click **Add NAT rule**.
2. Specify the rule name and rule position.
3. Select the translation settings for outgoing traffic.

| **Name** | **Description** |
| --- | --- |
| **Original source** | Network\_LAN |
| **Translated source (SNAT)** | MASQ |
| **Original destination** | Any |
| **Translated destination (DNAT)** | Original |
| **Original service** | Any |
| **Translated service (PAT)** | Original |
| **Inbound interface** | Port3 |
| **Outbound interface** | Port1 |

1. Click **Save**.

The following image shows an example of how to configure the settings:



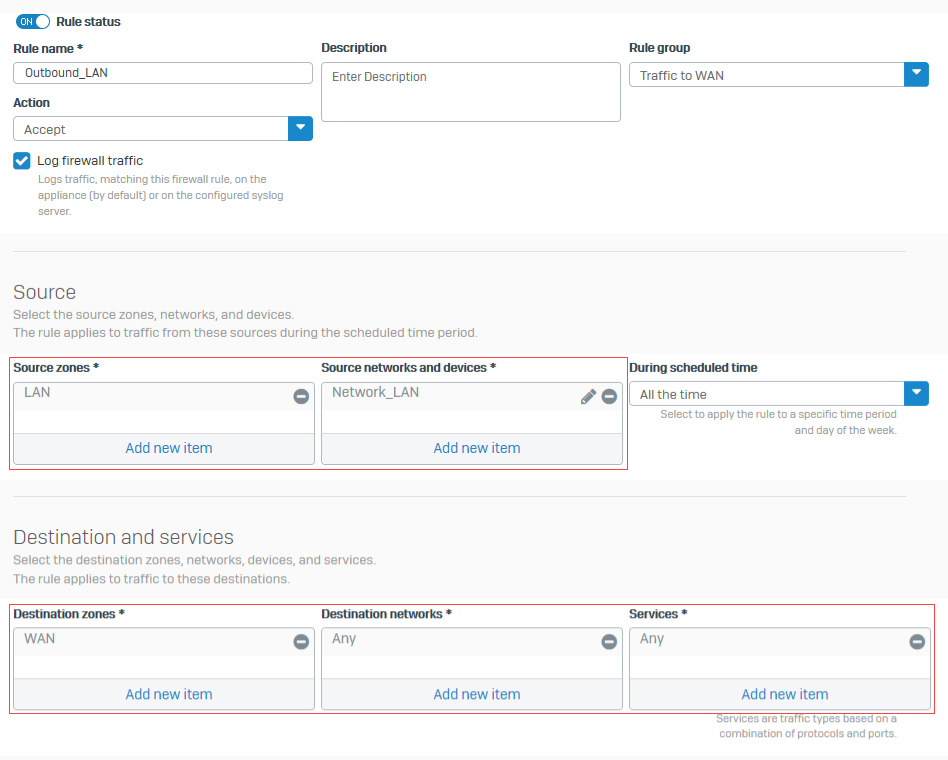
Create a firewall rule to allow traffic that matches the source NAT rule.

## **Specify firewall rule settings for SNAT traffic**

1. Go to **Rules and policies** > **Firewall rules**. Select protocol **IPv4** or **IPv6** and select **Add firewall rule**. Select **New firewall rule**.
2. Specify the rule name and rule position.
3. Specify the source, destination, and services as follows:

| **Name** | **Description** |
| --- | --- |
| **Source zones** | LAN |
| **Source networks and devices** | Network LAN |
| **Destination zones** | WAN |
| **Destination networks** | Any |
| **Services** | Any |

1. Specify the security settings and click **Save**.



You created a firewall rule to allow traffic from the LAN zone to external networks.