SOPHOS
Security made simple.

Pocket Guide

Connect to Parent Proxy in the Internal Network

Product: Sophos XG Firewall

Contents

Overview

This guide describes how to configure Sophos XG Firewall to connect to a parent proxy server deployed in LAN or DMZ.

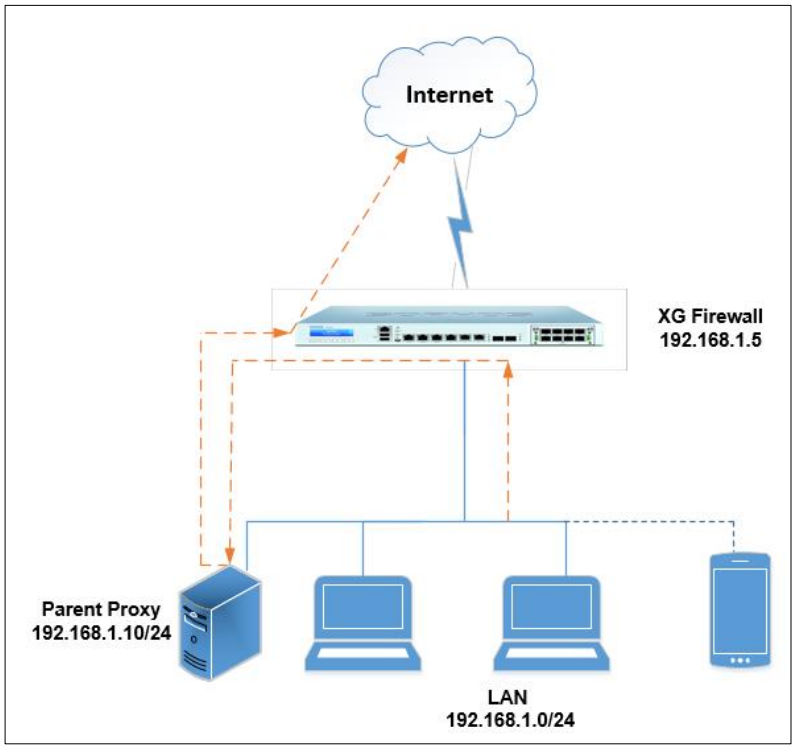
Parent proxy is also known as upstream proxy or forward proxy.

Prerequisites

You must have read-write permissions on the SF-OS Admin Console for the relevant features.

Network Diagram

In this scenario, web requests from the LAN are redirected to the parent proxy (LAN) which will forward these to WAN.



Configuration

Log in to the SF-OS Admin Console.

Step 1: Enable IPv4 Parent Proxy

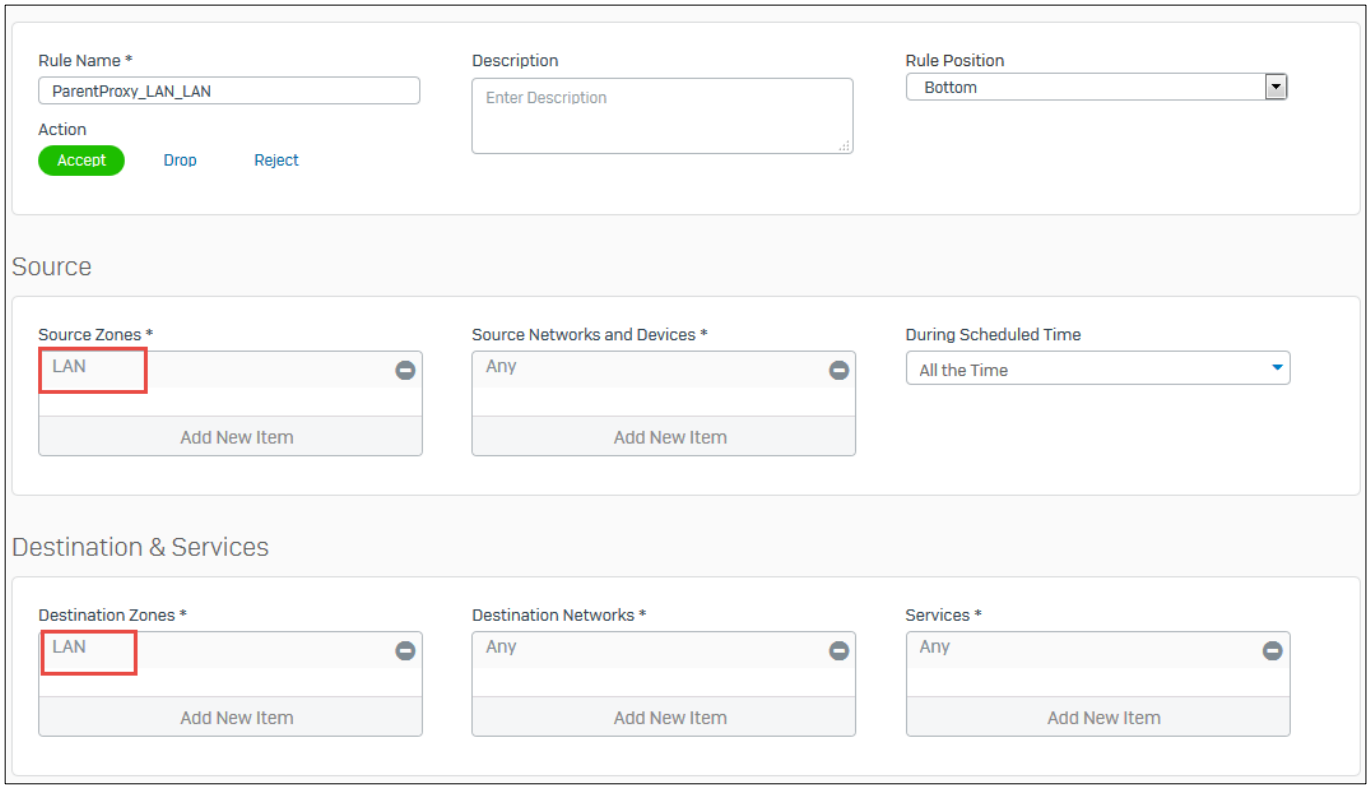
- Go to **Configure** > **Routing** > **Upstream Proxy**.
- Select to enable **Parent Proxy** and enter the **Domain Name/IPv4 Address** of the parent proxy.

Click **Apply**.

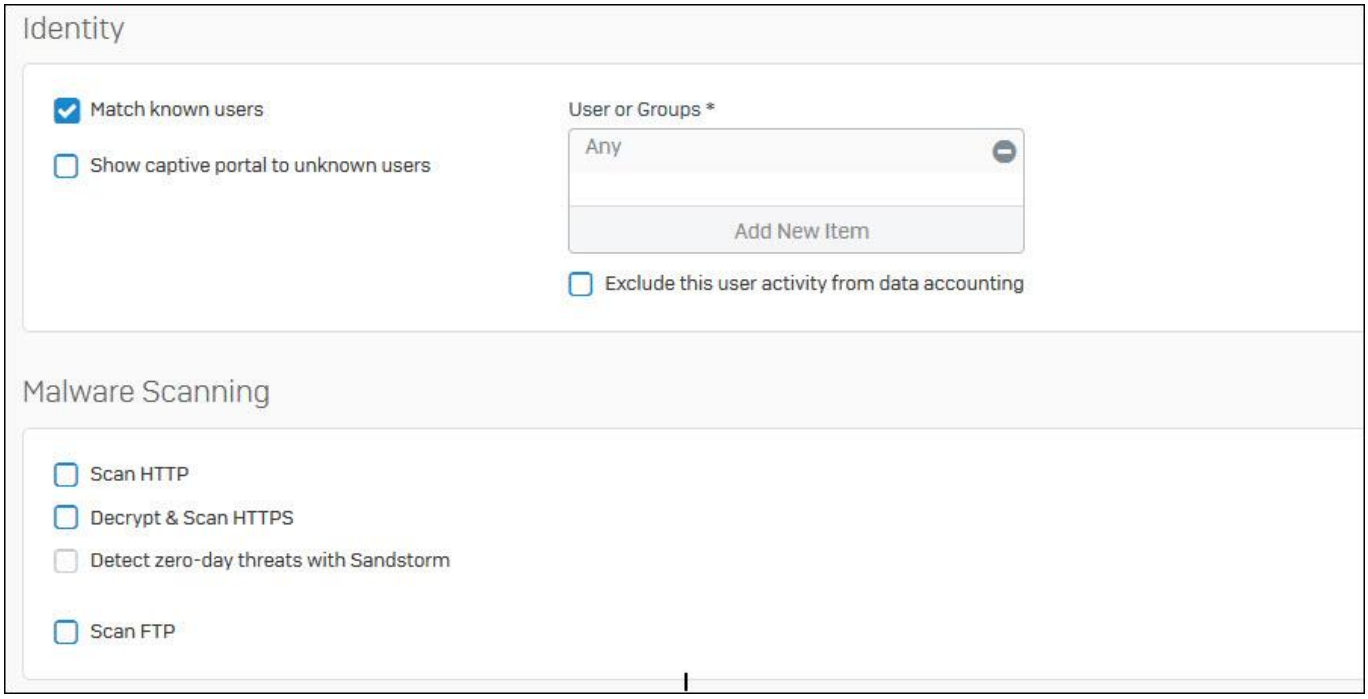
Step 2: Create a firewall rule to forward requests to the parent proxy

- Go to **Protect > Firewall,** click **Add Firewall Rule** and click **User/Network Rule.**
- Select the **Rule Position** from the list. Firewall rules are evaluated from top to bottom until a matching rule is found. You can drag the rule upwards or downwards to a specific position in the rule table.
- Set both **Source** and **Destination Zones** to **LAN**. This enables XG Firewall to forward requests to the parent proxy.

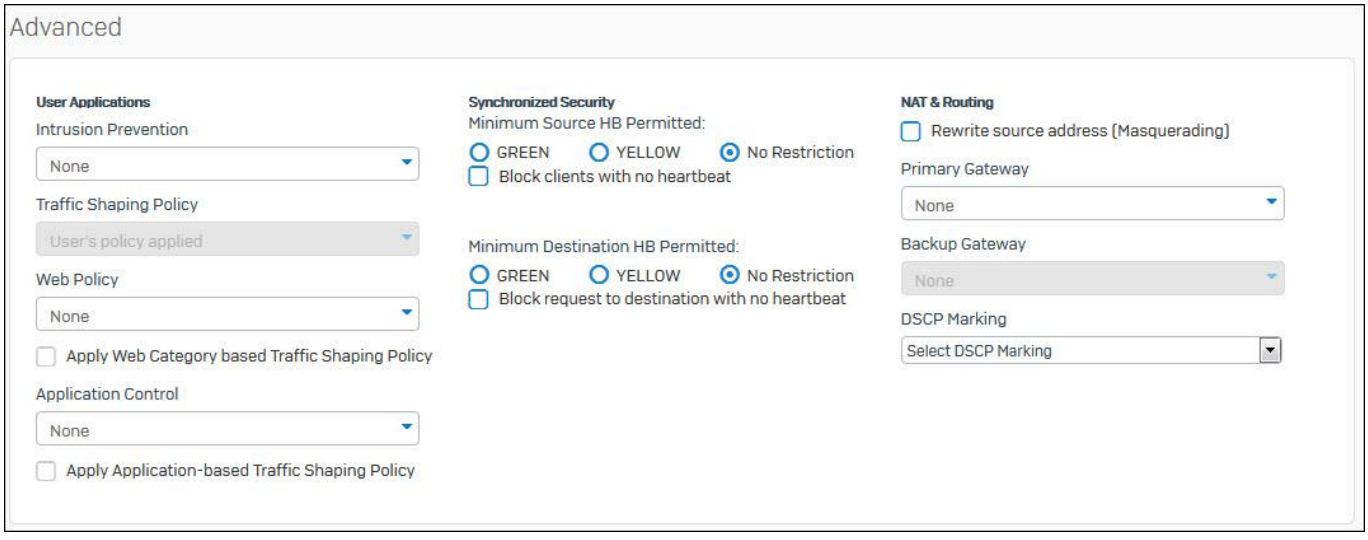
Note: If parent proxy is deployed in DMZ, create a User/Network Rule with **Source Zones** set to LAN and **Destination Zones** set to DMZ.



Under **Identity** and **Malware Scanning**, retain the default settings.



Under **Advanced**, retain the default settings.



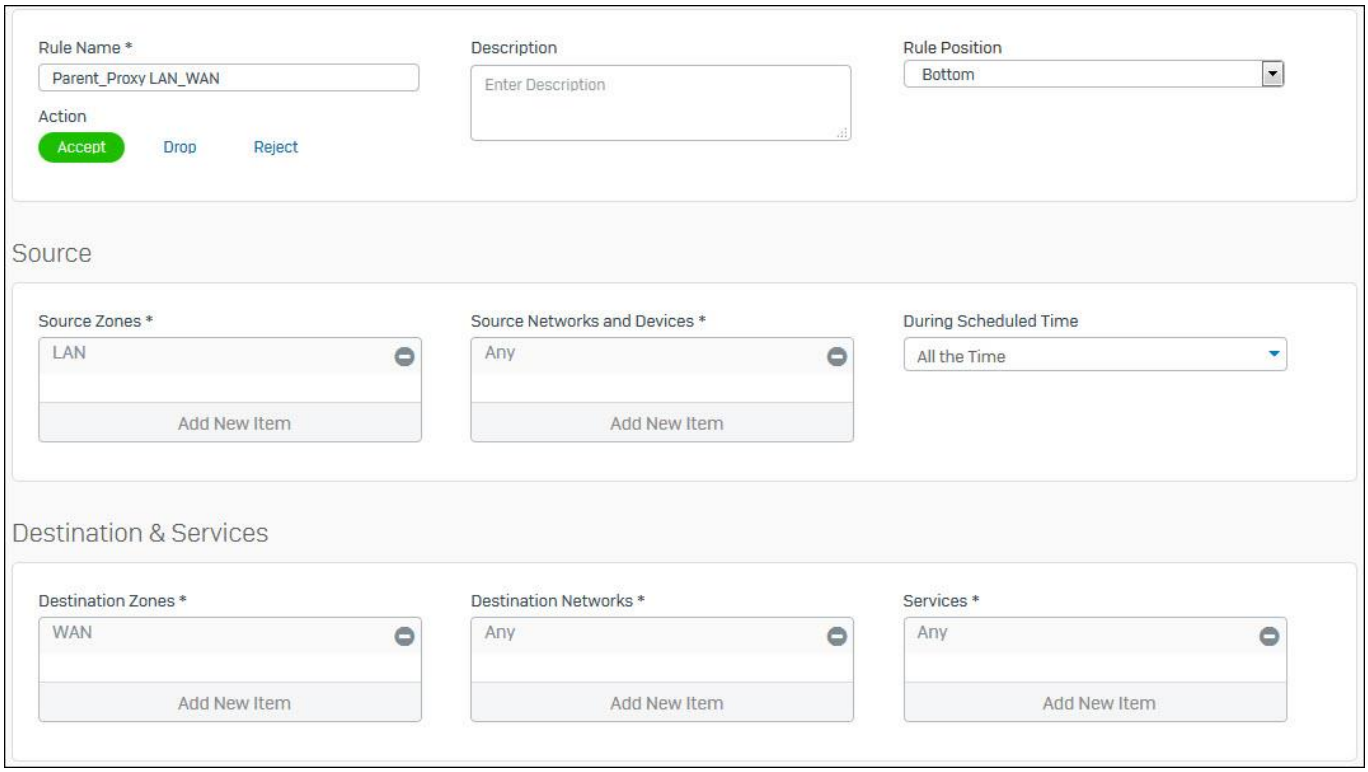
Click **Save**.

Step 3: Create a firewall rule to masquerade outgoing traffic

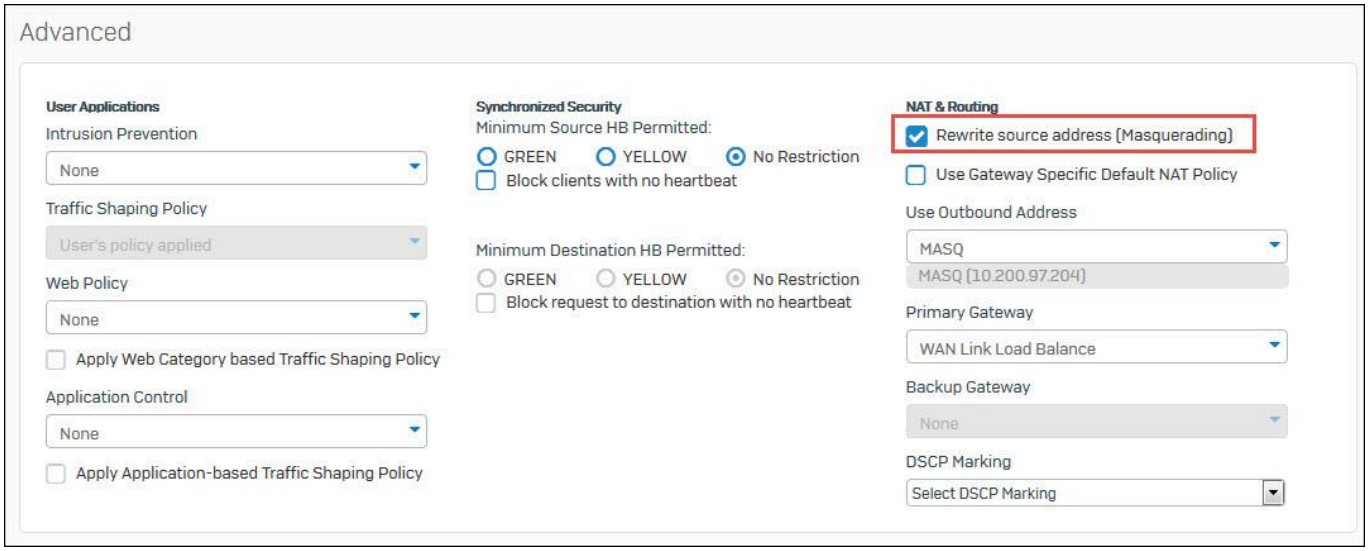
- Go to **Protect > Firewall,** click **Add Firewall Rule** and click **User/Network Rule.**
- Select the **Rule Position** from the list.

- Set **Source Zones** to **LAN**. Set **Destination Zones** to **WAN**. This forwards traffic from the parent proxy to WAN.

Note: If parent proxy is deployed in DMZ, create a User/Network Rule with **Source Zones** set to DMZ and **Destination Zones** set to WAN to masquerade outgoing traffic.



Under **Advanced**, in **NAT & Routing**, select the **Rewrite source address (Masquerading)** check box to masquerade the IP address of parent proxy.


Advanced
User Applications
Intrusion Prevention
None
Traffic Shaping Policy
User's policy applied
Web Policy
None
Apply Web Category based Traffic Shaping Policy
Application Control
None
Apply Application-based Traffic Shaping Policy
Synchronized Security
Minimum Source HB Permitted:
GREEN
YELLOW
No Restriction
Block clients with no heartbeat
Minimum Destination HB Permitted:
GREEN
YELLOW
No Restriction
Block request to destination with no heartbeat
NAT & Routing
Rewrite source address (Masquerading)
Use Gateway Specific Default NAT Policy
Use Outbound Address
MASQ
MASQ (10.200.97.204)
Primary Gateway
WAN Link Load Balance
Backup Gateway
None
DSCP Marking
Select DSCP Marking

Click **Save**.

Result

You have established a secure connection between Sophos XG firewall and the internal parent proxy server which is deployed in LAN. Web requests from LAN users will be routed by the XG firewall to the parent proxy which will forward these to WAN.

Copyright Notice