



# Pocket Guide

## Connect to Parent Proxy in the Internal Network

Product: Sophos XG Firewall

## Contents

<b>Overview .....</b>	<b>3</b>
<b>Prerequisites .....</b>	<b>3</b>
<b>Network Diagram .....</b>	<b>3</b>
<b>Configuration .....</b>	<b>4</b>
Step 1: Enable IPv4 Parent Proxy .....	4
Step 2: Create a firewall rule to forward requests to the parent proxy.....	5
Step 3: Create a firewall rule to masquerade outgoing traffic .....	6
<b>Result .....</b>	<b>9</b>
<b>Copyright Notice.....</b>	<b>10</b>

## Overview

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

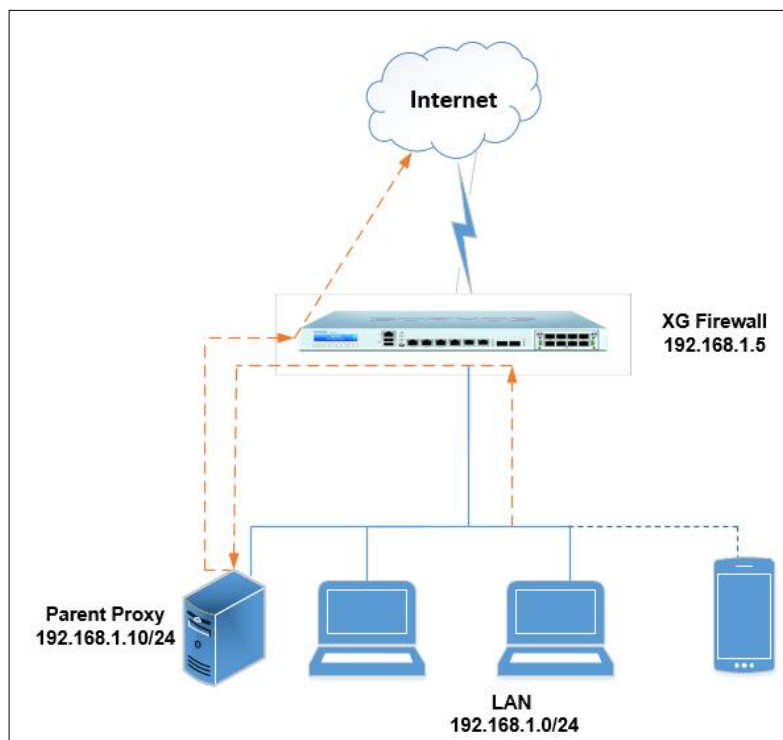
Parent proxy is also known as upstream proxy or forward proxy.

## 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.

#### IPv4 Parent Proxy

Parent Proxy	<input checked="" type="checkbox"/> Enable
Domain Name/IPv4 Address *	<input type="text" value="192.168.1.10"/>
Port *	<input type="text" value="3128"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

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.

The screenshot displays the configuration page for a new firewall rule. At the top, the 'Rule Name' is 'ParentProxy\_LAN\_LAN', the 'Rule Position' is 'Bottom', and the 'Action' is 'Accept'. Below this, the 'Source' section has 'Source Zones' set to 'LAN', 'Source Networks and Devices' set to 'Any', and 'During Scheduled Time' set to 'All the Time'. The 'Destination & Services' section has 'Destination Zones' set to 'LAN', 'Destination Networks' set to 'Any', and 'Services' set to 'Any'. Red boxes highlight the 'LAN' selections in both the Source and Destination Zones fields.

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

### Identity

Match known users

Show captive portal to unknown users

User or Groups \*

Any

Add New Item

Exclude this user activity from data accounting

### Malware Scanning

Scan HTTP

Decrypt & Scan HTTPS

Detect zero-day threats with Sandstorm

Scan FTP

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

### 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)

Primary Gateway: None

Backup Gateway: None

DSCP Marking: Select DSCP Marking

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.

The screenshot shows a firewall rule configuration interface. At the top, there are three fields: 'Rule Name \*' with the value 'Parent\_Proxy LAN\_WAN', 'Description' with the placeholder 'Enter Description', and 'Rule Position' with a dropdown menu set to 'Bottom'. Below these is the 'Action' section, which has three buttons: 'Accept' (highlighted in green), 'Drop', and 'Reject'. The 'Source' section contains three sub-sections: 'Source Zones \*' with a dropdown menu set to 'LAN' and an 'Add New Item' button; 'Source Networks and Devices \*' with a dropdown menu set to 'Any' and an 'Add New Item' button; and 'During Scheduled Time' with a dropdown menu set to 'All the Time'. The 'Destination & Services' section also contains three sub-sections: 'Destination Zones \*' with a dropdown menu set to 'WAN' and an 'Add New Item' button; 'Destination Networks \*' with a dropdown menu set to 'Any' and an 'Add New Item' button; and 'Services \*' with a dropdown menu set to 'Any' and an 'Add New Item' button.

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

Advanced

<p><b>User Applications</b></p> <p>Intrusion Prevention None</p> <p>Traffic Shaping Policy User's policy applied</p> <p>Web Policy None</p> <p><input type="checkbox"/> Apply Web Category based Traffic Shaping Policy</p> <p>Application Control None</p> <p><input type="checkbox"/> Apply Application-based Traffic Shaping Policy</p>	<p><b>Synchronized Security</b></p> <p>Minimum Source HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block clients with no heartbeat</p> <p>Minimum Destination HB Permitted: <input type="radio"/> GREEN <input type="radio"/> YELLOW <input checked="" type="radio"/> No Restriction <input type="checkbox"/> Block request to destination with no heartbeat</p>	<p><b>NAT &amp; Routing</b></p> <p><input checked="" type="checkbox"/> Rewrite source address [Masquerading]</p> <p><input type="checkbox"/> Use Gateway Specific Default NAT Policy</p> <p>Use Outbound Address MASQ MASQ [10.200.97.204]</p> <p>Primary Gateway WAN Link Load Balance</p> <p>Backup Gateway None</p> <p>DSCP Marking Select DSCP Marking</p>
--	---	--

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

Copyright 2016-2017 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.