



Pocket Guide

Connect to Parent Proxy on Internet

Product: Sophos XG Firewall

Contents

| | |
|---|----------|
| Overview | 3 |
| Prerequisites | 3 |
| Network Diagram | 4 |
| Configuration | 5 |
| Step 1: Enable IPv4 Parent Proxy | 5 |
| Step 2: Create a firewall rule to masquerade outgoing traffic | 5 |
| Result | 8 |
| Copyright Notice | 9 |

Overview

This guide describes how to configure Sophos XG Firewall to connect to a parent proxy server deployed on the Internet.

Parent proxies can be used in countries in which routing Internet access through government-approved proxy servers is mandatory.

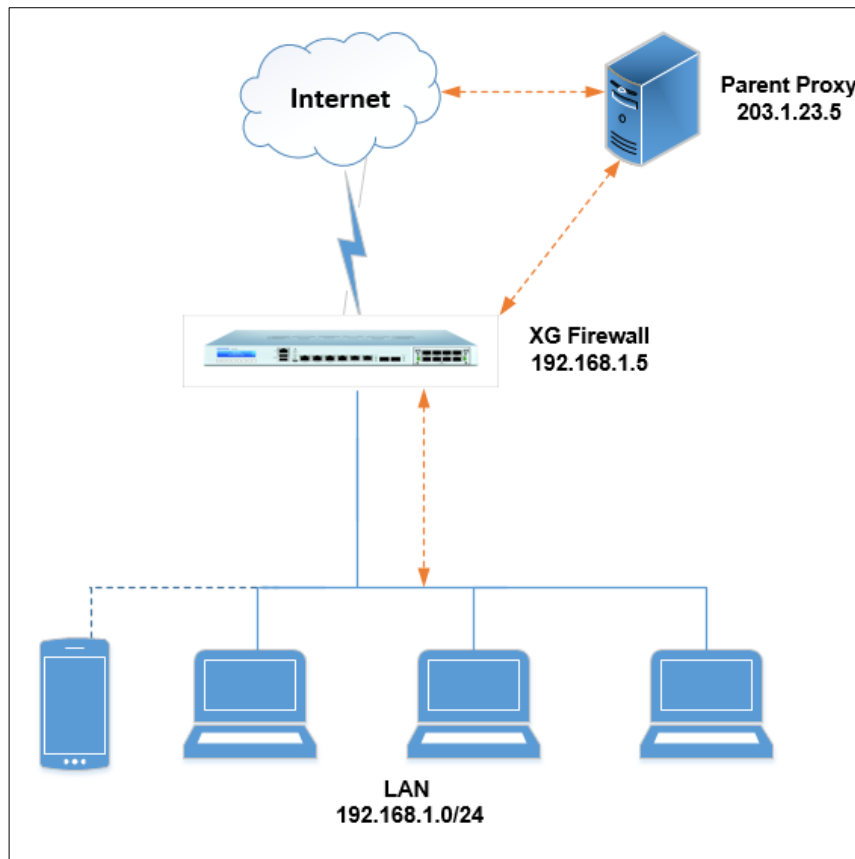
Parent proxy is also known as upstream proxy or forward proxy.

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 that is deployed on the Internet (WAN).



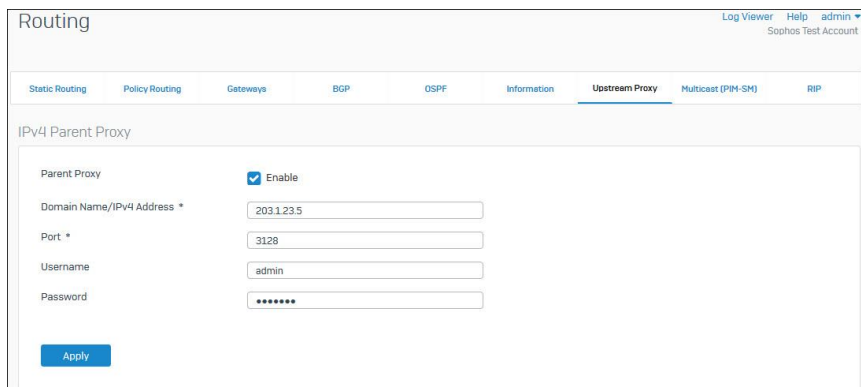
Configuration

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**.



The screenshot shows the 'Routing' configuration page in the SF-OS Admin Console. The 'Upstream Proxy' tab is selected. Under the 'IPv4 Parent Proxy' section, the 'Parent Proxy' checkbox is checked and labeled 'Enable'. The 'Domain Name/IPv4 Address *' field contains '203.123.5', the 'Port *' field contains '3128', the 'Username' field contains 'admin', and the 'Password' field is masked with asterisks. An 'Apply' button is located at the bottom of the form.

Step 2: 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. 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 **Source Zones** to **LAN**. Set **Destination Zones** to **WAN**. This enables the 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.

| | | |
|---|--------------------------------------|---------------------------------------|
| Rule Name * ParentProxy_LAN_WAN | Description Enter Description | Rule Position Bottom |
| Action <input checked="" type="radio"/> Accept <input type="radio"/> Drop <input type="radio"/> Reject | | |
| Source | | |
| Source Zones * LAN | Source Networks and Devices * Any | During Scheduled Time All the Time |
| Destination & Services | | |
| Destination Zones * WAN | Destination Networks * Any | Services * Any |

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

| | |
|---|--|
| Identity | |
| <input checked="" type="checkbox"/> Match known users | User or Groups * Any |
| <input type="checkbox"/> Show captive portal to unknown users | <input type="checkbox"/> Exclude this user activity from data accounting |
| Malware Scanning | |
| <input type="checkbox"/> Scan HTTP | |
| <input type="checkbox"/> Decrypt & Scan HTTPS | |
| <input type="checkbox"/> Detect zero-day threats with Sandstorm | |
| <input type="checkbox"/> Scan FTP | |

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

Advanced

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

Click **Save**.

Result

You have established a connection between Sophos XG firewall and an external parent proxy server. Web requests from LAN users will be routed by the XG firewall to the parent proxy.

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.