



Pocket Guide

Configure SF-OS to use RADIUS Server
for authentication

Product: Sophos XG Firewall

Contents

Overview 3

Prerequisites..... 3

Configuration 4

Step 1: Configure SF-OS to use the RADIUS Server 4

Step 2: Select RADIUS as the Authentication Server 5

Test Configuration 6

Results 6

Copyright Notice 7

Overview

This guide describes how to integrate Sophos XG Firewall (SF-OS) with RADIUS (Remote Authentication Dial in User Service) to provide authentication, authorization, and accounting to users against a central database.

Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You will need the following RADIUS parameters during the integration:
 - IP address
 - Shared secret
 - Administrator username and password

Configuration

Log in to the SF-OS Admin Console.

Step 1: Configure SF-OS to use the RADIUS Server

- Go to **Configure > Authentication > Servers** and click **Add**.
- Set **Server Type** to **RADIUS Server**.
- Select **Enable Accounting** for accounting start/stop request and login/logout time. Enter the **Accounting Port**.
- **Group Name Attribute** is vendor-specific.
- If **Enable Additional Settings** is **ON**, enter the **NAS-Identifier** and **NAS-Port-Type**.

Click **Save**.

Add External Server

Servers Services Groups Users One-Time Password Captive Portal

Server Type

RADIUS Server

Server Name *

SF_Radius

Server IP *

172.16.16.18

Authentication Port *

1812

☒ Enable Accounting

Accounting Port

1812

Shared Secret *

.....

Group Name Attribute *

Filter_id

ON

 Enable Additional Settings

NAS-Identifier

copernicus

e.g. copernicus

NAS-Port-Type

(0) Async

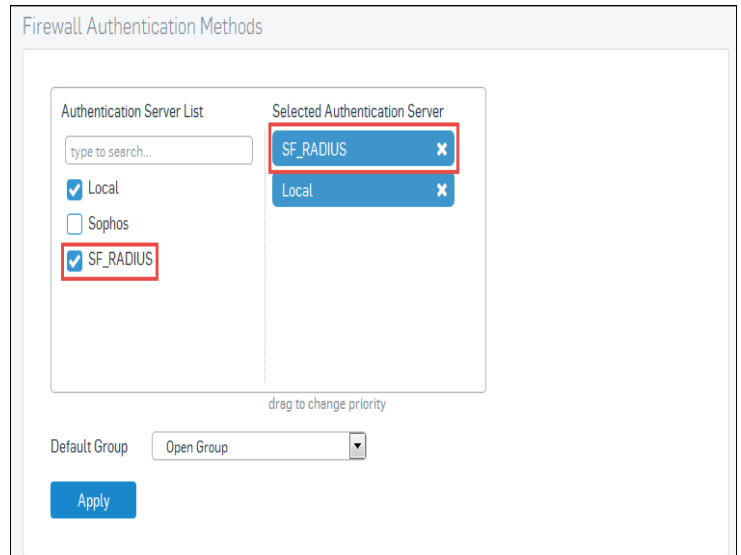
Test Connection

Save

Cancel

Step 2: Select RADIUS as the Authentication Server

- Go to **Configure > Authentication > Services**
- Within **Firewall Authentication Methods**, go to the **Authentication Server List** and select the **RADIUS** server you have configured in Step 1.
- In the **Selected Authentication Server** list, drag the selected **RADIUS** server to the top. This **RADIUS** server will act as the primary authentication server.



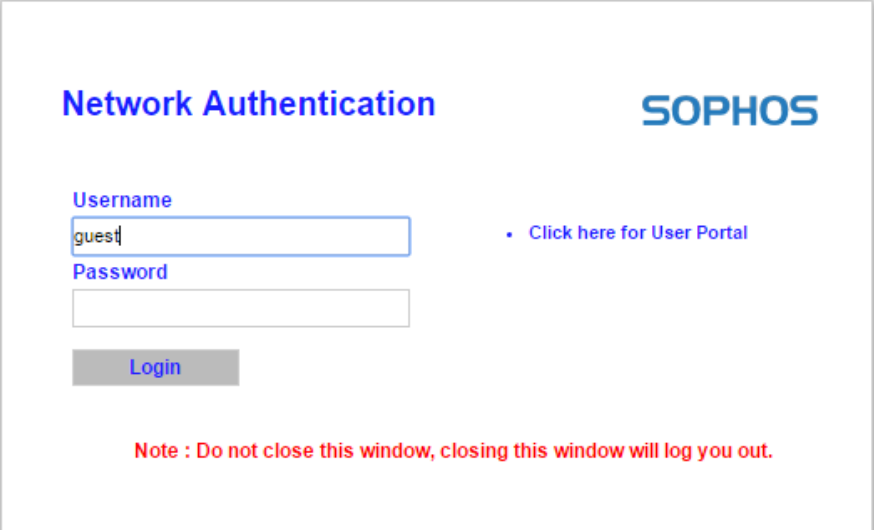
Click **Apply**.

Note:

- The default authentication server (Local) is SF-OS.
- For multiple authentication servers, authentication request is forwarded based on the order configured in the **Selected Authentication Server** list.

Test Configuration

1. Go to <https://<SF LAN IP>:8090> [Captive Portal login page] and login as a user to check if you have internet access.
2. Go to <https://<SF LAN IP>:4444> and login as Admin. Go to **Monitor & Analyze > Current Activities > Live Users** and check if the user logged in step 1 is live.



The screenshot shows the 'Network Authentication' page of a Sophos firewall. The page has a blue header with the title 'Network Authentication' and the 'SOPHOS' logo. Below the header, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'guest'. To the right of the 'Username' field, there is a link that says 'Click here for User Portal'. Below the 'Password' field, there is a 'Login' button. At the bottom of the page, there is a red note that says 'Note : Do not close this window, closing this window will log you out.'

The configuration is successful if:

- You are able to login as a user with internet access.
- The user is displayed as a live user in admin console, then the configuration is successful.

Results

You have integrated SF-OS with RADIUS. All users will be authenticated by this RADIUS server.

Copyright Notice

Copyright 2015-2016 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.