Pocket Guide

Configure SFOS to use RADIUS Server for authentication

Product: Sophos XG Firewall
Configure SFOS to use RADIUS Server for authentication

Contents

Overview ........................................................................................................................................... 3
Prerequisites ...................................................................................................................................... 3
Configuration .................................................................................................................................... 4
Step 1: Configure SFOS to use the RADIUS Server ........................................................................ 4
Step 2: Select RADIUS as the Authentication Server ....................................................................... 5
Test Configuration ............................................................................................................................ 6
Result ................................................................................................................................................ 7
Copyright Notice .............................................................................................................................. 8
Configure SFOS to use RADIUS Server for authentication

**Overview**

This guide describes how to integrate Sophos XG Firewall (SFOS) 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 SFOS 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 SFOS Admin Console.

**Step 1: Configure SFOS 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.
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 SFOS.
- 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 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.
Configure SFOS to use RADIUS Server for authentication

**Result**

You have integrated SFOS with RADIUS. All users will be authenticated by this RADIUS server.
Configure SFOS to use RADIUS Server for authentication

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.