Pocket Guide

Configure SF-OS to use AD Server for authentication

Product: Sophos XG Firewall

Contents

Scenario

This guide describes how to integrate Sophos XG Firewall (SF-OS) with Windows Active Directory (AD) to authenticate users based on groups, domains and organizational units listed within the Active Directory Server (ADS).

Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You will need the following SF-OS and AD parameters during the integration:
    - **IP address** of the SF-OS interface connected to ADS
    - **IP address** of ADS
    - **Administrator username** and **password** for ADS

- To get the following parameters, log in to ADS as Admin. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

    - NetBIOS domain name
    - FQDN (example: sophos.com)
    - Search DN (example: dc=sophos, dc=com)
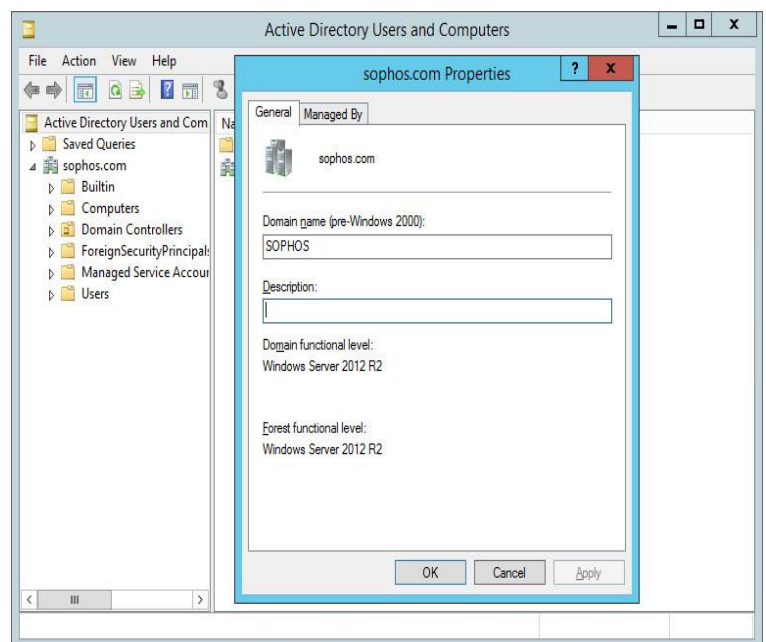
Configuration

Log in to the SF-OS Admin Console.

Step 1: Configure Active Directory

- Go to **Configure > Authentication > Servers** and click **Add**.
- Set **Server Type** to **Active Directory**.
- Enter the **NetBIOS Domain**, **Display Name Attribute** and **Email Name Attribute** from the ADS.
- The **default Port** is based on the **Connection Security** option that you select. Change the port number, if required.

- For **Connection Security** options **SSL/TLS** or **STARTTLS**, select **Validate Server Certificate**, if required.
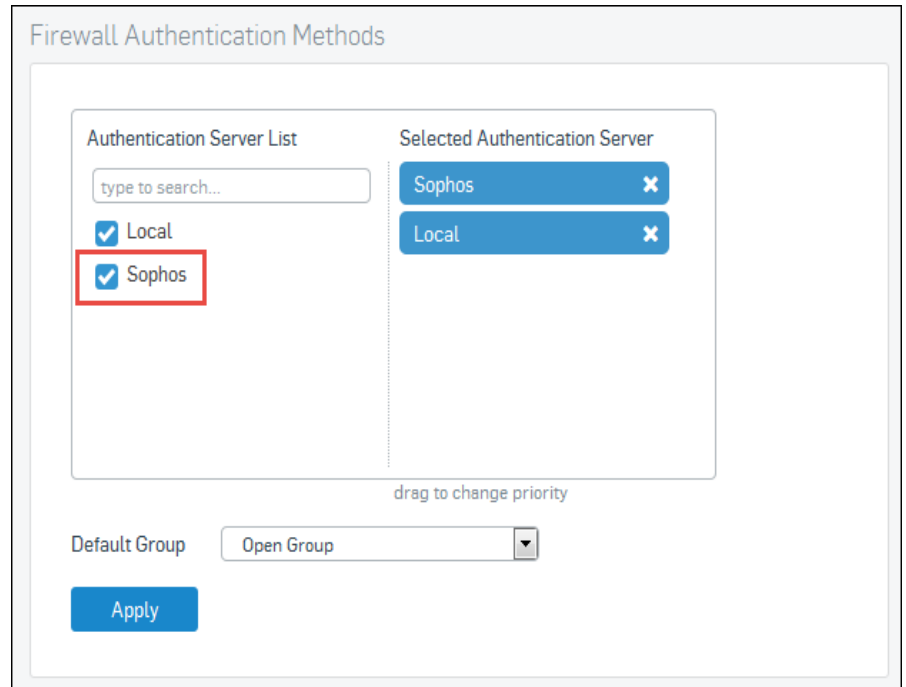
Note:
For **Connection Security** option **Simple**, **username** and **password** are communicated in plain text between SF-OS and ADS.

Click **Save**.

Step 2: Select AD as the Primary Authentication Method

- Go to **Configure** > **Authentication** > **Services**.

- Within **Firewall Authentication Methods**, go to the **Authentication Server List** and select the ADS you have configured in Step 1.

- In the Selected **Authentication Server list**, drag the selected ADS to the top position. This ADS will act as the primary authentication server.

Note:

The default authentication server (Local) is SF-OS.

Click **Apply**.

Results

You have configured ADS as your primary authentication server. All users will be authenticated by this ADS.

Suggested Reading

Import Active Directory Groups using Wizard.

Copyright Notice