SOPHOS
Security made simple.

Pocket Guide

Configure SF-OS to use LDAP server for authentication

Product: Sophos XG Firewall

Contents

Scenario

This guide describes how to integrate Sophos XG Firewall (SF-OS) with LDAP (Lightweight Directory Access Protocol) to authenticate users.

Prerequisites

- You must have read-write permissions on the SF-OS Admin Console for the relevant features.
- You will need the following LDAP parameters during the integration:
  - LDAP server IP address and port
  - LDAP version
  - LDAP administrator username and password (If Anonymous Login is disabled)
  - Authentication Attribute is used to perform user search. By default, LDAP uses UID attribute to identify user entries.
  - Group Name Attribute, Display Name Attribute, Email Address Attribute and Expire Date Attribute

Configuration

- Log in to the SF-OS Admin Console.

Step 1: Create the LDAP group (optional)

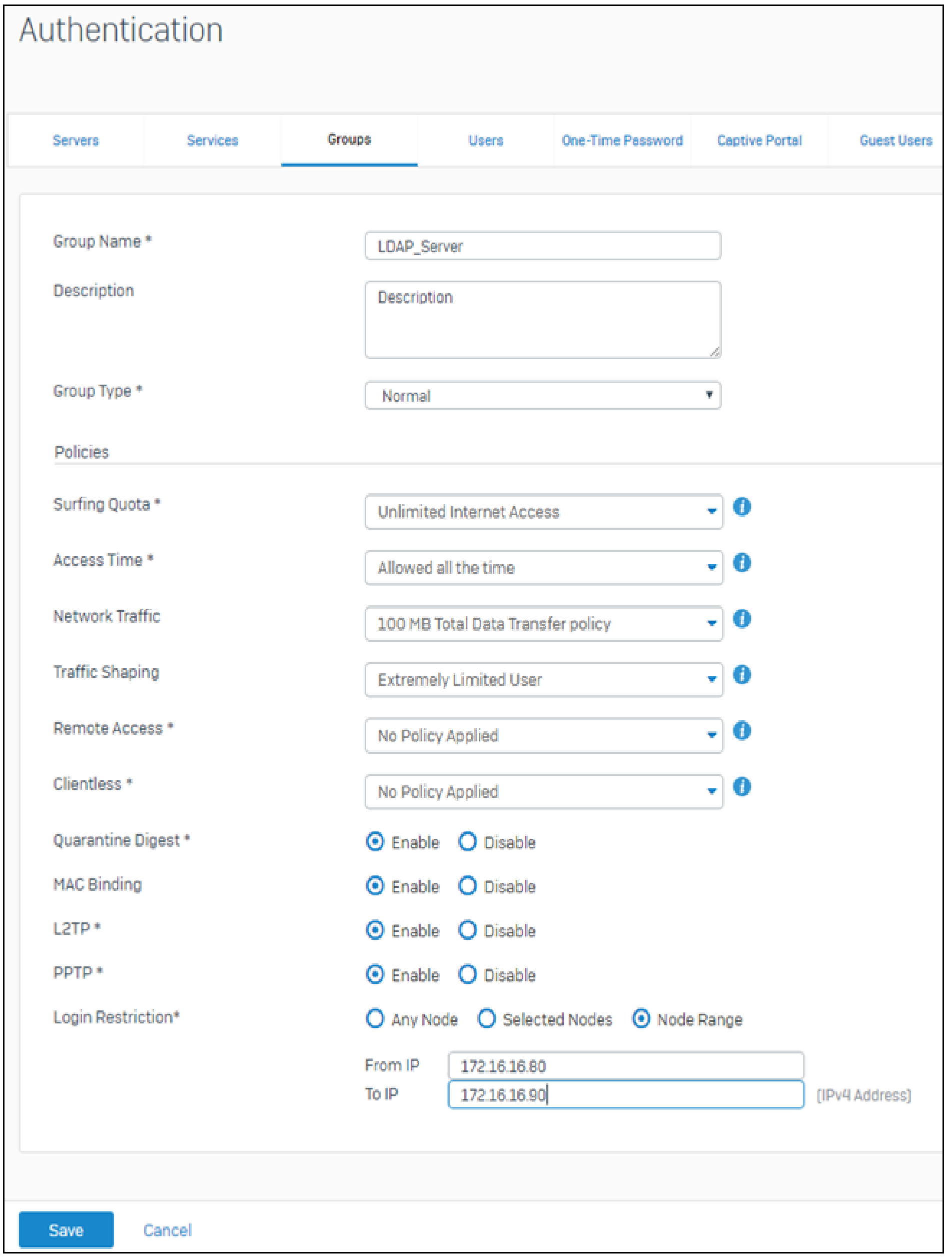
By default LDAP users are added to the Default group of SF-OS. If you do not want to add them to the Default group, create a new LDAP group in SF-OS. The group is synchronized with the LDAP server at the time of each user's first login.

- Go to **Configure** > **Authentication** > **Groups** and click **Add**.
- Set **Group Type** to **Normal** to log in using the client device; or to **Clientless** to perform access control through IP address.
- You can create, or choose the Policies.
- To override a user's group policy, create or choose **Remote Access** and **Clientless** policies.

Note: **Remote Access**: To deny SSL VPN access, select No Policy Applied.

- **Login restriction** allows access from any or specified nodes.

Click **Save**.



Group Name * LDAP_Server

Description: Description

Group Type * Normal

Policies

Surfing Quota * Unlimited Internet Access

Access Time * Allowed all the time

Network Traffic 100 MB Total Data Transfer policy

Traffic Shaping Extremely Limited User

Remote Access * No Policy Applied

Clientless * No Policy Applied

Quarantine Digest * ● Enable ○ Disable

MAC Binding ● Enable ○ Disable

L2TP * ● Enable ○ Disable

PPTP * ● Enable ○ Disable

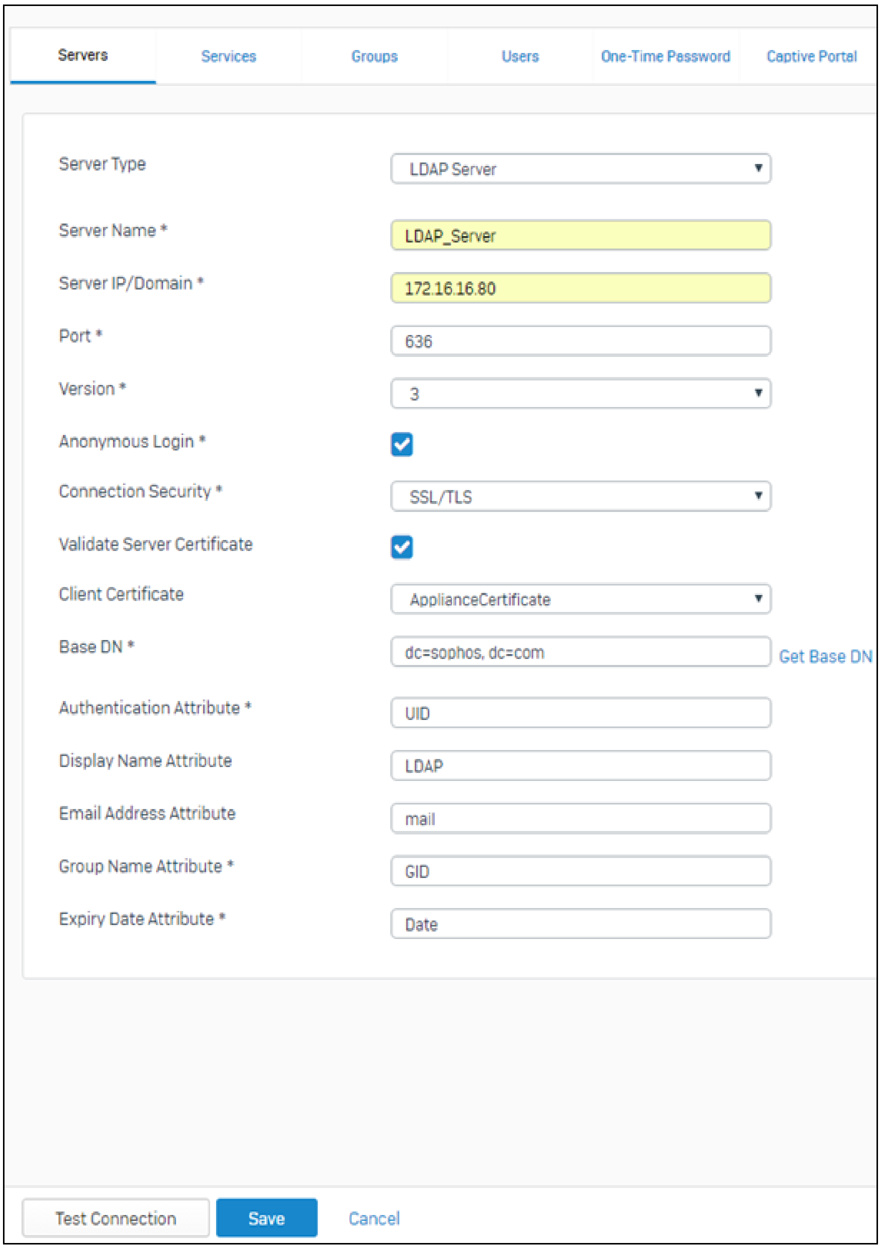
Login Restriction* ○ Any Node ○ Selected Nodes ● Node Range

From IP 172.16.16.80

To IP 172.16.16.90 [IPv4 Address]

Step 2: Configure LDAP authentication

- Go to **Configure** > **Authentication** > **Servers** and click **Add**.
- Set **Server Type** to **LDAP Server**.
- The default **Port** is based on the **Connection Security** that you select. Change the port number, if required.
- For **Connection Security** options **SSL/TLS** or **STARTTLS**, select **Validate Server Certificate**, if required.
- **Client Certificate** is set to the default certificate, change if required.
- Click **Get Base DN** to retrieve it from the LDAP directory.
- To use an attribute other than the default UID, enter the **Authentication Attribute**.



Server Type	LDAP Server ▾
Server Name *	LDAP_Server
Server IP/Domain *	172.16.16.80
Port *	636
Version *	3 ▾
Anonymous Login *	☑
Connection Security *	SSL/TLS ▾
Validate Server Certificate	☑
Client Certificate	ApplianceCertificate ▾
Base DN *	dc=sophos, dc=com
Authentication Attribute *	UID
Display Name Attribute	LDAP
Email Address Attribute	mail
Group Name Attribute *	GID
Expiry Date Attribute *	Date

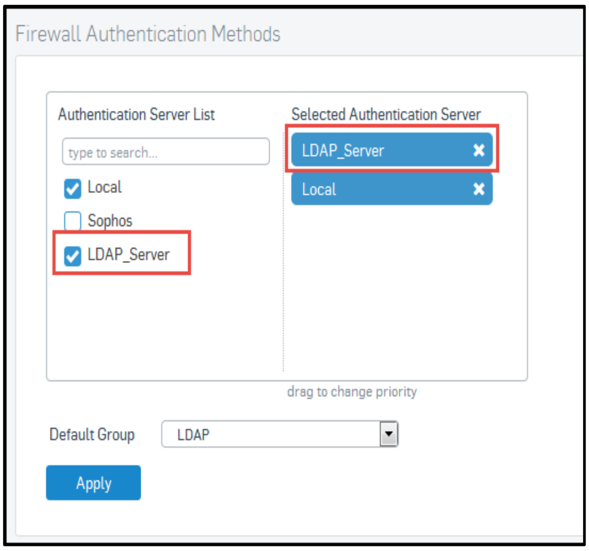
Note:

For **Connection Security** option **Simple**, **username** and **password** are communicated in plain text between **SF-OS** and **LDAP**.

Click **Save**.

Step 3: Select LDAP as Authentication Server

- Go to **Configure** > **Authentication** > **Services**
- Within **Firewall Authentication Methods**, go to the **Authentication Server List** and select the **LDAP Server** you have configured in Step 2.
- In the **Selected Authentication Server** list, drag the selected **LDAP server** to the top. This **LDAP server** will act as the primary authentication server.



Firewall Authentication Methods

Authentication Server List

type to search...

☑ Local

□ Sophos

☑ LDAP_Server

Selected Authentication Server

LDAP_Server ✖

Local ✖

drag to change priority

Default Group: LDAP

Click **Apply**.

Results

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

Copyright Notice