Pulse Policy Secure

Multi Factor Authentication with Duo

Configuration Guide

Product Release	**9.0R1**
Document	**1.0**
Published	**May 2018**

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

Multi Factor Authentication with Duo

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA."

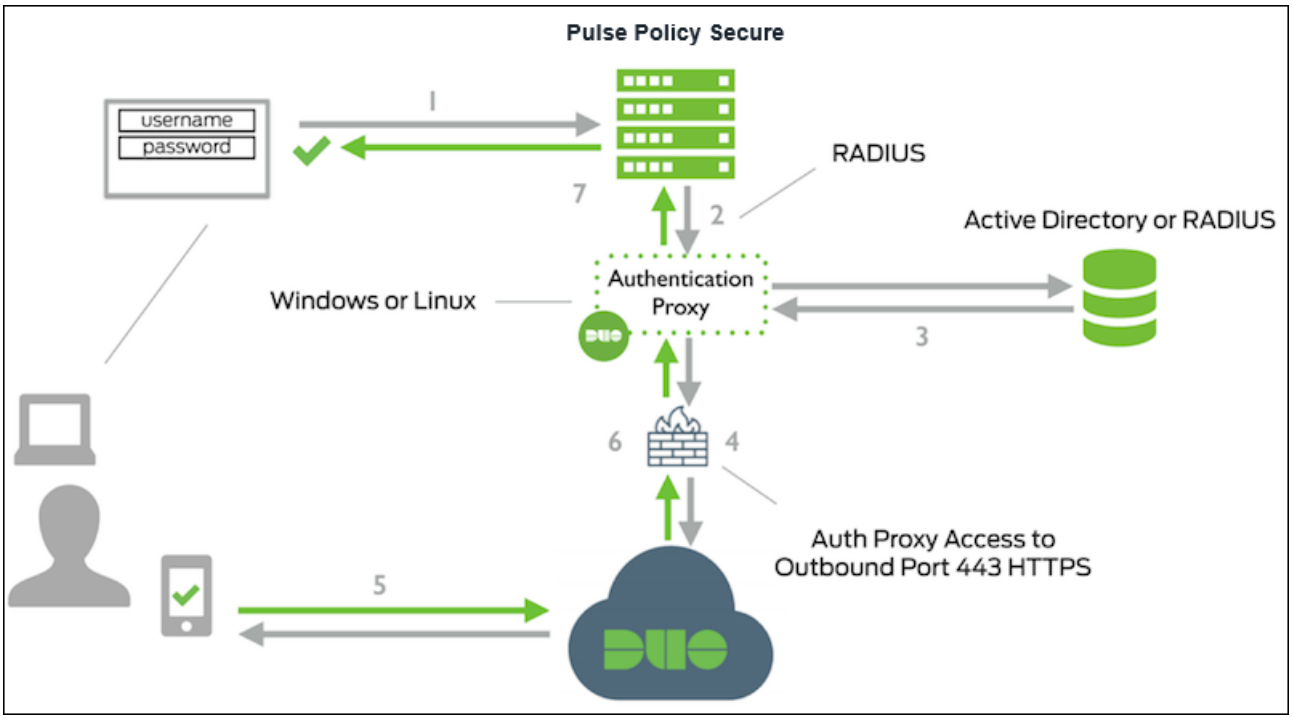
Introduction

Multi-factor authentication (MFA) adds a layer of security that allows companies to protect against the leading cause of data breach, which happens through compromised credentials. The MFA adds additional security where users must provide extra information or factors for authentication before accessing corporate applications, networks, and servers.

PPS integration with Duo security adds two-factor authentication to PPS login. It uses a combination of primary username and password along with secondary authentication based on push-notification approval to a mobile device or phone call or other supported authentication methods through Duo Security.

This document explains how PPS integrates with Duo Security to add two-factor authentication to PPS login.

Figure 1: Overview



1. Primary authentication is initiated to PPS.
2. PPS sends authentication request to Duo Security's authentication proxy.
3. Primary authentication is performed using Active Directory or RADIUS.
4. Duo authentication proxy connection is established to Duo Security over TCP port.
5. Secondary authentication through Duo Security's service.
6. Duo authentication proxy receives authentication response.
7. PPS access is granted.

Configuration

The goal is to configure two-factor authentication using RADIUS/AD as a Primary authentication server with Duo Security as a Secondary authentication server. It explains how to integrate MFA solution into the existing 802.1X connections and how-to setup the MFA realm.

This use case involves the following configuration:

- Configuring Duo RADIUS Proxy
- Configuring Duo Security
- Configuring PPS

Configuring Duo RADIUS Proxy

1. Install the Duo Authentication Proxy on Windows or Linux server and configure the authproxy.cfg file.

   Location of the configuration file.

   Windows (64-bit): C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg
   Linux: /opt/duoauthproxy/conf/authproxy.cfg

2. Configure the Proxy for Primary Authentication.

   If you have only RADIUS authentication server for primary authentication, then modify the authproxy.cfg file with below command. For example:

   ```
   [radius_client]
   host=1.2.3.4
   secret=radiusclientsecret
   ```

   If you have want to use Active Directory for primary authentication, then modify the authproxy.cfg file with below command. For example:

   ```
   [ad_client]
   host=1.2.3.4
   host_2=1.2.3.5
   service_account_username=duoservice
   service_account_password=password1
   search_dn=DC=example,DC=com
   security_group_dn=CN=DuoVPNUsers,OU=Groups,DC=example,DC=com
   ```

3. Setup the Authentication Proxy to work with PPS.

   Example configuration for AD.

   ```
   [radius_server_auto]
   ikey=DIXXXXXXXXXXXXXXXX
   skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   api_host=api-XXXXXXX.duosecurity.com
   radius_ip_1=5.6.7.8
   radius_secret_1=radiussecret1
   client=ad_client
   port=1812
   failmode=safe
   ```

Configuring Duo Security

1. Signup for a Duo account. Log in to the Duo Admin Panel and navigate to Applications.
2. Click Protect an Application and locate Juniper UAC (Older name for Pulse Policy Secure) in the applications list. Click Protect this Application to get your integration key, secret key, and API hostname.
3. Add the RADIUS server in PPS.
4. Configure a user realm in PPS.

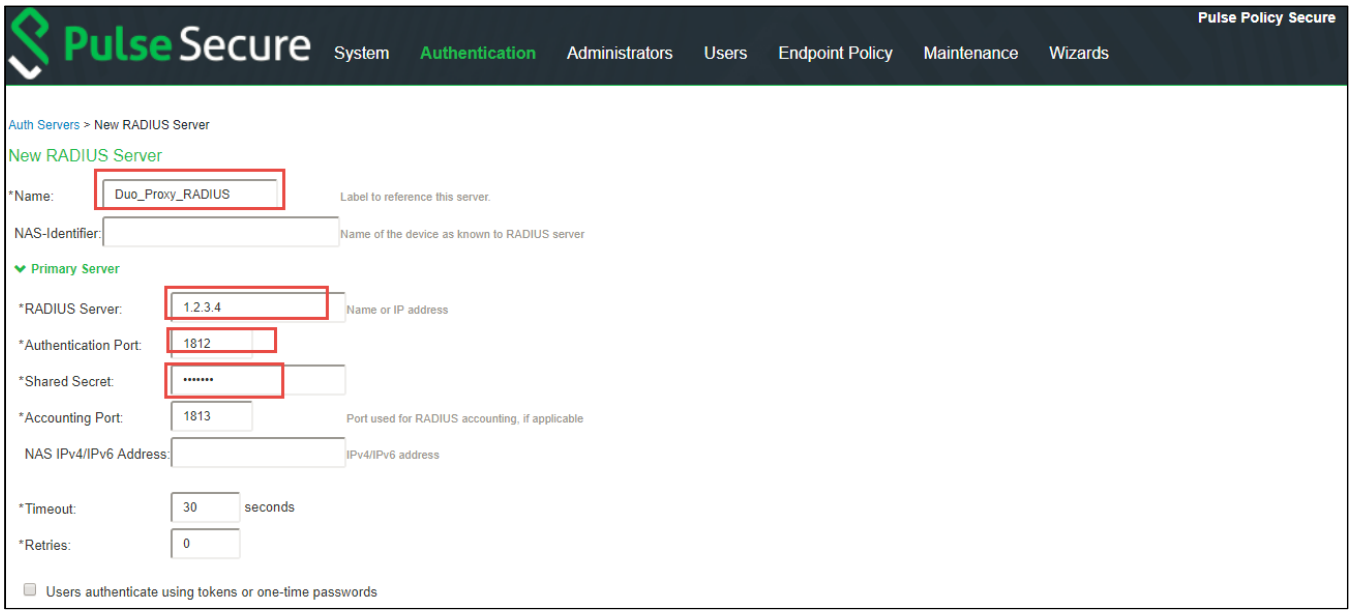
Note: This configuration applies to a RADIUS based MFA solution with Duo Security configured as a Secondary authentication server.

Configuring PPS

The configuration involves adding a RADIUS Server profile and then configuring a user realm.

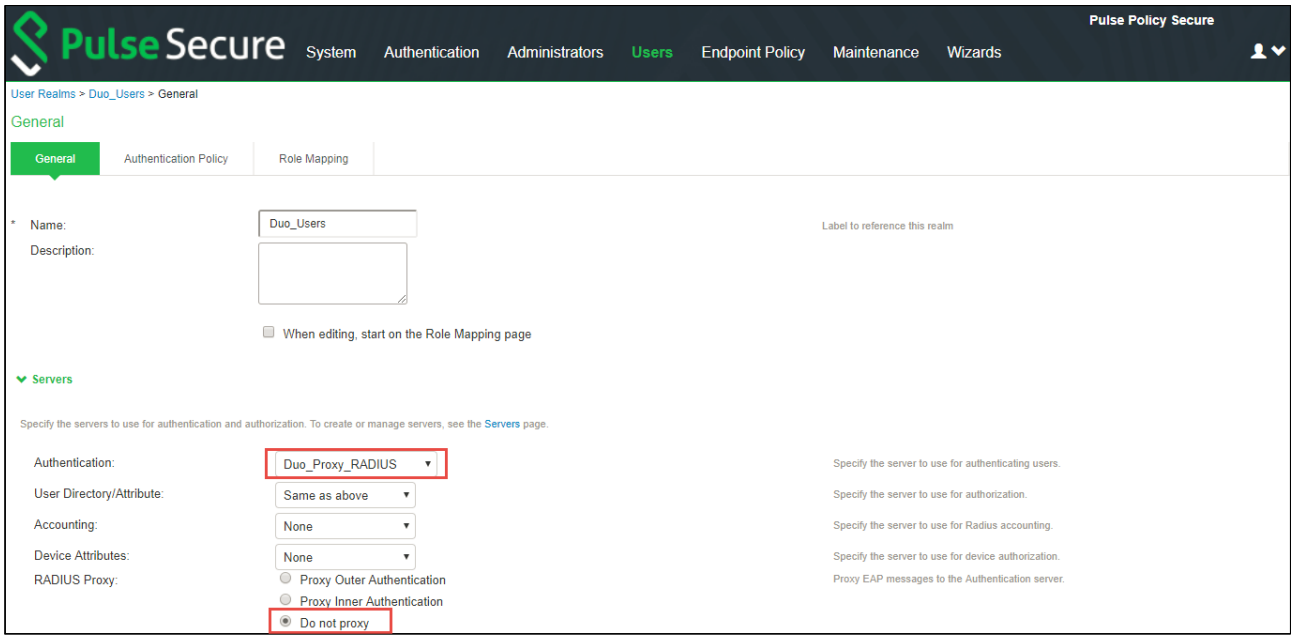
1. From the PPS Admin console, navigate to **Authentication > Auth. Servers**.
2. Select **RADIUS Server** from the **Auth Server Type** list, click **New Server**.
3. In the **Name** field, enter **Duo-Proxy-RADIUS.**
4. Under the **Primary Server** section, enter the following information:
    a. The IP address of your Duo Authentication Proxy.
    b. The RADIUS secret shared with your Duo Authentication Proxy.
    c. 1812 (or whichever port specified in your authproxy.cfg file).

Figure 2: RADIUS server



5. Configure User Realm for the Duo RADIUS server, navigate to **Users > User Realms** select **Duo-Proxy-RADIUS** (or whatever you named your new RADIUS server) in the Authentication drop-down.

   Figure 3: Authentication Realm



6. Click **Save Changes**.

Conclusion

You should now be able to properly authenticate devices based on the primary and secondary authentication server.

For troubleshooting you can verify the user access logs.

Figure 4: User Access Logs