yubico
the key to the cloud

Setup guide for OpenVPN with YubiRADIUS for Linux

A configuration guide to integrate OpenVPN in your OpenLDAP environment.

Yubico AB

January 15, 2012

Introduction

Yubico is the leading provider of simple, open online identity protection. The company's flagship product, the YubiKey®, uniquely combines driverless USB hardware with open source software. More than a million users in 100 countries rely on YubiKey strong two-factor authentication for securing access to computers, mobile devices, networks and online services. Customers range from individual Internet users to e-governments and Fortune 500 companies. Founded in 2007, Yubico is privately held with offices in California, Sweden and UK.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Trademarks

Yubico and YubiKey are trademarks of Yubico Inc.

Contact Information

Yubico Inc
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
USA
info@yubico.com

Contents

© 2012 Yubico. All rights reserved.

1 Background

This document will guide you through the configuration of OpenVPN with YubiRADIUS to allow user authentication with Yubikeys.

The common username/password prompt has been proven unreliable over time and a more secure mechanism of authentication is needed. The Yubikey represents the newest and most advanced two-factor authentication token on the market to increase the security of your computer network. A two-factor authentication mechanism requires something you know “a password”, and something you have “the Yubikey”. A user authenticated with this mechanism is more “trustworthy” and more protected against account hijacking.

At the end of this document you will be able to login in your account/network using OpenVPN and authenticate the users with two-factor strong authentication provided by Yubikey.

© 2012 Yubico. All rights reserved.

2 References

This user guide is based on the material available on yubico.com and openvpn.net. Please refer to the list below to read the full documentation.

1. **YubiRADIUS** documentation. Available at: http://www.yubico.com/support/documentation/

2. **YubiRADIUS** virtual appliance. Download from: http://www.yubico.com/products/services-software/yubiradius/download/

3. **OpenVPN** documentation. Available at: http://openvpn.net/index.php/open-source/documentation.html

4. **OpenVPN** client / server. Download from: http://www.openvpn.net

5. **VMware** client. Download from: https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_view_clients/1_0

6. **VMware** client documentation. Avilable at: http://www.vmware.com/support/viewclients/doc/viewclients_pubs.html

3 Prerequisites

This section will present the prerequisites for this set up.

This configuration requires two machines, a client and a server. The server will run the YubiRADIUS Virtual Appliance and the client will run Linux Ubuntu 12.10 with kernel 3.5.0-21. The server and client machine don't need to be on the same LAN but the client must be able to reach the server. This setup requires also two Yubikeys.The Yubikeys are sturdy two-factor authentication tokens that will allow us to securely identify against the YubiCloud or the Yubico Validation Server. You can buy a Yubikey on http://store.yubico.com.

~~3.1~~ YubiRADIUS

Download the YubiRADIUS Virtual Appliance (YRVA) from http://www.yubico.com/products/services-software/yubiradius/download/ . If this URL is not working please navigate www.yubico.com as it may have been moved or updated. In this documentation we will download the VMware YRVA image and execute it with VMware client version 5.0. This machine will be our server.

~~3.2~~ OpenVPN

Download and install OpenVPN on both client and server machine. On Ubuntu 12.10 this can be done using the command:

```
user1@example.com$ sudo apt-get install openvpn
```

At this time, current version is OpenVPN 2.2.1 i686-linux-gnu. You can check your OpenVPN version by typing the following command:

```
user1@example.com$ openvpn –version
```

~~3.3~~ YubiKeys

In this suggested setup we are going to use two Yubikeys Those tokens are already shipped pre-configured in slot one with a Yubico OTP. The first key will be used as primary key for logging into our network, while the second Yubikey will be used as a backup in case the first Yubikey is lost or stolen. Yubikeys are melded in a very stiff plastic material which makes them extremely resistant and thus they are very hard to break. If you would like additional information on how to configure your Yubikey please follow the personalization guide available at http://www.yubico.com/support/documentation/. This link will provide you with the documentation for the cross-platform personalization tool http://www.yubico.com/wp-content/uploads/2012/10/Cross-Platform-YubiKey-Personalization-Tool-3.0.1-User-guide-v5.pdf.

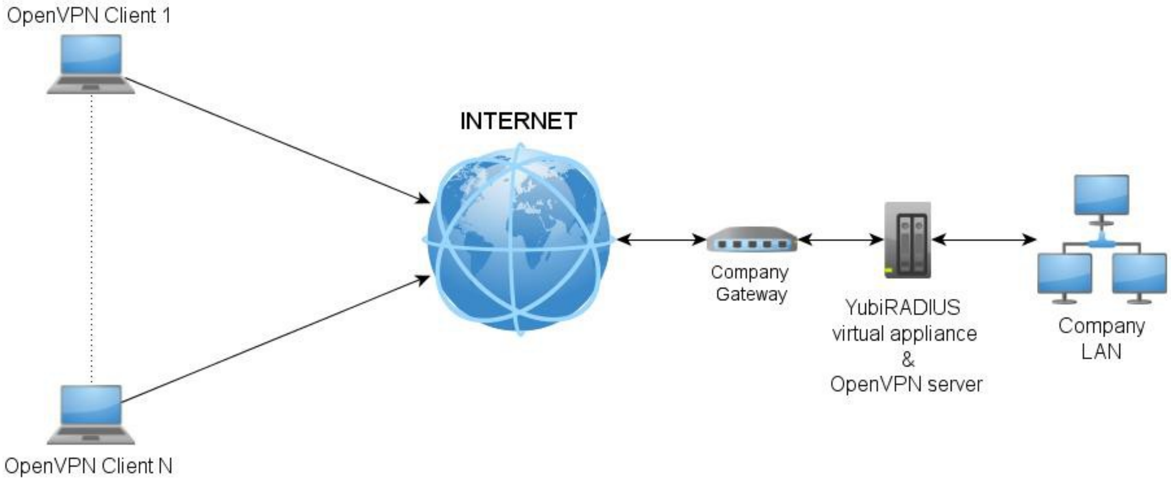
~~3.4~~ Virtualization Framework

The YubiRADIUS 3.6 is available in two different virtual appliance formats. The VMware format and the Open Virtualization Format (OVF). In this setup we are going to use the VMware format.

To run the virtual appliance we are going to need the VMware client available both for Windows and Linux. The current version of VMware client is 5.0 and it is available for download here: https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_view_clients/1_0.

4 System overview

Figure - Network topology for our sample configuration



Our system has three main components: the OpenVPN client, the OpenVPN server and the YubiRADIUS virtual appliance.

In our scenario the company ACME has employees all around the world and needs a secure mechanism to authenticate his workforce and allow them access to the private LAN

To achieve this, ACME installs a virtual network with OpenVPN and relies on the YubiRADIUS virtual appliance and the Yubikey for handling the users' authentication.

© 2012 Yubico. All rights reserved.

5 Generic setup

This chapter illustrates a generic setup. The server machine will run the YubiRADIUS virtual appliance version 3.6 and OpenVPN server. One (or more) machine will act as OpenVPN client. The client will authenticate to the server using a Yubikey, a two-factor strong authentication token. Each client needs its own Yubikey, therefore if we have one hundred clients we will need one hundred Yubikeys.

~~5.1~~ YubiRADIUS configuration guide

The complete configuration of YubiRADIUS is out of the scope of this document; however the basic steps needed to setup this example configuration are described in the following sections.

Please, refer to the complete documentation for YubiRADIUS available at http://www.yubico.com/support/documentation/ if you need more information.

5.1.1 User import and Yubikey binding

If you are new to YubiRADIUS, you may want to import the default users pre-configured for the virtual appliance. You can achieve this through the Webmin interface. Open your web-browser, and point it to 127.0.0.1 .

In this example, to access the Webmin interface use the following credentials:

username: root

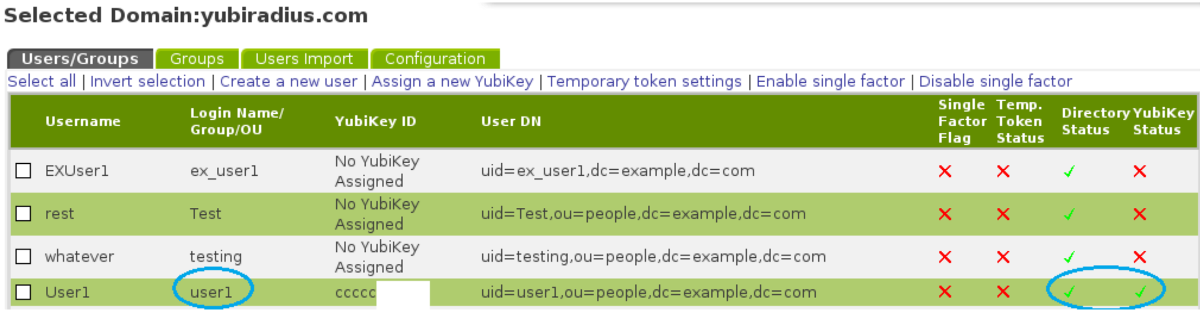
password: yubico

Create an example domain and import the example users preconfigure in OpenLDAP.

Once you have imported the users, you will need to bind a Yubikey to them. In Figure 2 you can see how a correctly configure user should look.

You can notice that User1, has YubikeyStatus = **Enabled** and has one YubikeyID associated with his account. To bind a key to a specific user, click the link “Assign a new YubiKey”.

Figure - user configuration



Selected Domain:yubiradius.com

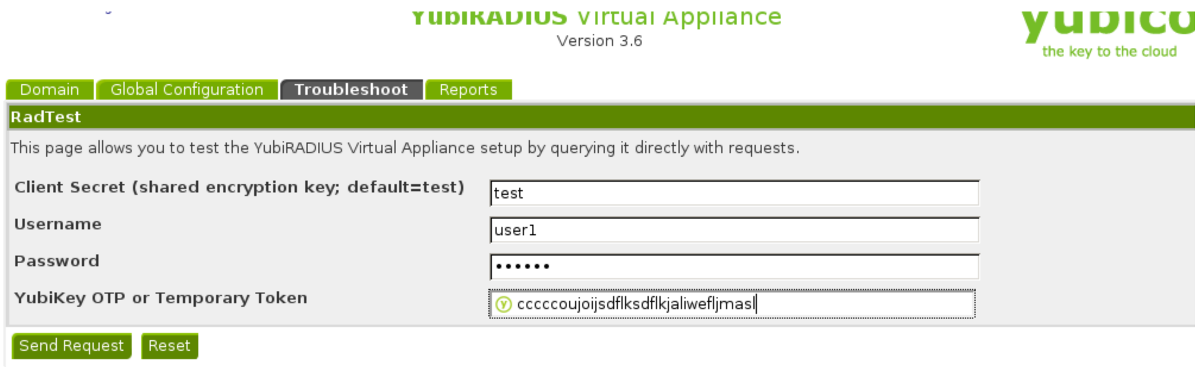
Users/Groups
Groups
Users Import
Configuration
Select all | Invert selection | Create a new user | Assign a new YubiKey | Temporary token settings | Enable single factor | Disable single factor

	Username	Login Name/ Group/OU	YubiKey ID	User DN	Single Factor Flag	Temp. Token Status	Directory Status	YubiKey Status
□	EXUser1	ex_user1	No YubiKey Assigned	uid=ex_user1,dc=example,dc=com	✗	✗	✓	✗
□	rest	Test	No YubiKey Assigned	uid=Test,ou=people,dc=example,dc=com	✗	✗	✓	✗
□	whatever	testing	No YubiKey Assigned	uid=testing,ou=people,dc=example,dc=com	✗	✗	✓	✗
□	User1	user1	ccccc	uid=user1,ou=people,dc=example,dc=com	✗	✗	✓	✓

5.1.2 Validating the Yubikey

The next step is to be sure that the validation server is configured correctly. To achieve this, access the troubleshoot menu from the YubiRADIUS Virtual Appliance link in the left panel.

Figure - authentication test



RadTest

This page allows you to test the YubiRADIUS Virtual Appliance setup by querying it directly with requests.

Client Secret (shared encryption key; default=test)	test
Username	user1
Password	••••••
YubiKey OTP or Temporary Token	cccccoujoijsdflksdflkjaliwefljmasl

Press the “Send Request” button and check for a successful response. If the check fails, you probably have misconfigured the validation server in the Global Configuration menu.

At this point you can also use the “radtest” tool to check if the configuration is working.

5.1.3 PAM configuration

PAM configuration can be tricky. The following sections will help you through the installation of PAM and the configuration of the necessary files to have your OpenVPN & YubiRADIUS working correctly.

5.1.4 Install libpam-yubico & libpam-radius-auth

There is an Ubuntu PPA (Personal Package Archive) for yubico-pam that can be installed using the following commands on reasonably modern Ubuntu / Debian platforms:

```
user1@example.com$ add-apt-repository ppa:yubico/stable

user1@example.com$ apt-get update

user1@example.com$ apt-get install libpam-yubico

user1@example.com$ apt-get install libpam-radius-auth
```

Please always refer to the up-to-date instruction available on GitHub: https://github.com/Yubico/yubico-pam/blob/master/README for the installation.

5.1.5 PAM configuration for Radius and OpenVPN

There are three files that you want to configure in PAM in order to have your system run correctly. Those files are: /etc/pam.d/openvpn, /etc/pam.d/radiusd and the /etc/pam_radius_auth.conf. The following sections will describe how to properly configure those files to setup correctly the environment.

5.1.6 Configuration file Radiusd

Create/edit a file named radiusd in /etc/pam.d directory. The file must look like the one presented below:

```
user1@example.com:/etc/pam.d# cat radiusd

# /etc/pam.d/radiusd - PAM configuration for FreeRADIUS
```

```
#README# the following text should be on the same line#
auth    required    pam_python.so    /usr/share/ykpam/pam_yubiserver.py
ropval_url=http://localhost/wsapi/ropverify.php?id=%d&otp=%s
send_password    ykotp_re=.*([CBDEFGHIJKLNRTUVcbdefghijklnrtuv]{44})$
hotp_re=null

#this is a new line
auth sufficient pam_yubico.so id=16 debug authfile=/etc/pam.d/yubimap

account     required         pam_permit.so          debug
session     required         pam_permit.so
```

5.1.7 Configuration file pam_radius_auth.conf

The file pam_radius_auth.conf is located in the /etc/ directory. You need to configure this file if you have more than one server running because they need to share the same secret. In this example my server *127.0.0.1* and *other-server* share the same secret: test

`user1@example$ cat pam_radius_auth.conf`

```
# server[:port]   shared_secret      timeout (s)
127.0.0.1             test               1
other-server          test               3
```

~~5.2~~ OpenVPN configuration guide

If you do not have yet configured your OpenVPN server, please follow the official guide at http://www.openvpn.net since this configuration is out of the scope of this documentation. If you are new to OpenVPN here is a short list of hints:

- Look for the sample configuration files to understand how a ".conf" file should look like,

- Generate the keys using the easy-rsa method first on the server,

- Check the configuration files included in this guide to understand what files you need to generate and include in the configuration,

- If nothing works, don't panic! Usually nothing works at the beginning, visit our Forum http://forum.yubico.com and/or Google search for your error, chances are that someone else already had the same issue.

5.2.1 Configuration file *openvpn*

Create/edit a file named OpenVPN in /etc/pam.d directory. The file must look like the one presented below:

`user1@example.com:/etc/pam.d# cat openvpn`

```
#openvpn configuration for pam

account      required    pam_radius_auth.so
account      required    pam_radius_auth.so
```

```
      auth          required    pam_radius_auth.so no_warn try_first_pass
```

5.2.2 Server Configuration

If you already have OpenVPN server configured the setup will be very quick. Simply add the following three parameters in your Server.conf file (usually located in /etc/openvpn).

```
plugin /usr/lib/openvpn/openvpn-auth-pam.so openvpn

client-cert-not-required

username-as-common-name

reneg-sec 0
```

5.2.3 Client configuration

We now move to the client configuration for our OpenVPN solution. You can configure your client with any text editor such as Emacs or vi.

We need to add the following parameter in order to enable client authentication with a username and password prompt.

```
# enable client authentication with username and password
auth-user-pass
```

© 2012 Yubico. All rights reserved.

6 Test case

In this chapter it is shown how to connect using OpenVPN. Please refer to our forum community at http://forum.yubico.com if you have further question or problems.

~~6.1~~ Starting the OpenVPN server

Execute the OpenVPN dameon with the following command:

```
user1@example.com$ /etc/init.d/openvpn restart
```

~~6.2~~ Starting the OpenVPN client

Execute the OpenVPN client with the following command:

```
user1@example.com$ oepnvpn /etc/openvpn/client.conf
```

~~6.3~~ Logging in with the Yubikey

The OpenVPN software will now prompt the user with a username and password prompt. The first step to login is to enter your username and press “Enter”.

The second step is to type in your password and touch your Yubikey button. **Do not press “Enter” right after typing in the password!** You need to concatenate your password with an OTP generated by your Yubikey. The server will then extract the OTP and validated it against the validation server of your choice.

If you will successfully log in you will be able to access your server through the virtual network you just created.

7 Troubleshooting

If you experience any problem with OpenVPN you should check the log file. Configure your client and server in verbose mode with the parameter:

```
# Set log file verbosity.
verb 6
```

To configure the logfile locations use the following directives within the server / client configuration files:

```
#logfile location
status ./openvpn-status.log
log /var/log/openvpn.log
```

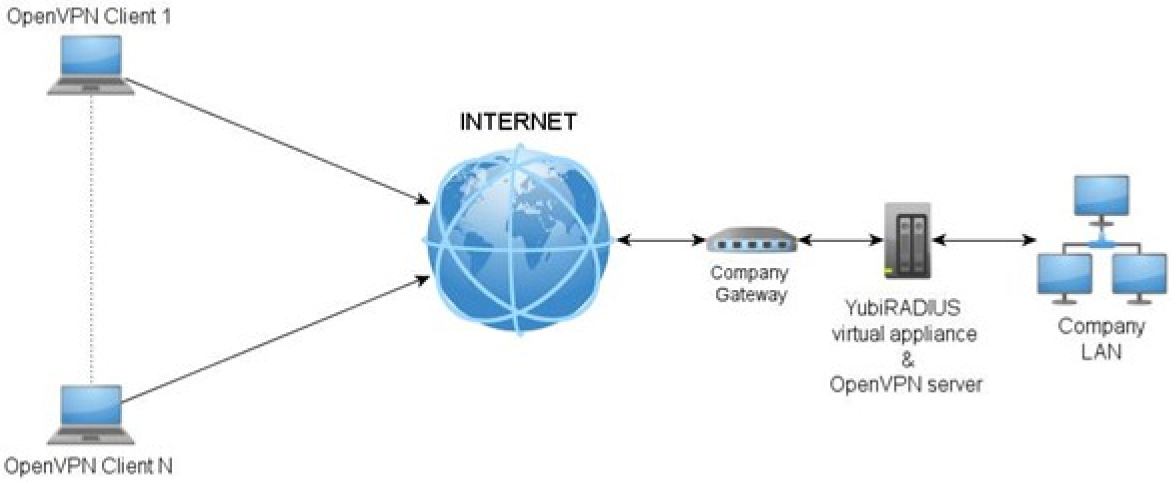
If you experience problem with YubiRADIUS and importing users from OpenLDAP, please refer to the official YubiRADIUS documentation at http://www.yubico.com/support/documentation/ and interact with our forum Tech Community at http://forum.yubico.com.

© 2012 Yubico. All rights reserved.

8 Appendix: Example setup

This guide will help you set up a client / server network with OpenVPN and YuibiRADIUS and Yubikey as two-factor authentication token. The sample network is shown in Figure .

Figure - Example of a network topology



~~8.1~~ OpenVPN server configuration file

```
user1@example.com:/etc/openvpn$ cat server.conf

port 1194
proto udp
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/rva354.crt
key /etc/openvpn/rva354.key  # This file should be kept secret
dh /etc/openvpn/dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
verb 6
plugin /usr/lib/openvpn/openvpn-auth-pam.so openvpn
client-cert-not-required
username-as-common-name
reneg-sec 0
# You may try to enable this in some cases
;script-security 2
```

~~8.2~~ OpenVPN client configuration file

```
user1@example.com:/etc/openvpn$ cat client.conf

client
dev tun
proto udp
entries to load balance         # between the servers.
remote 192.168.1.153 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/client1.crt
key /etc/openvpn/client1.key
ns-cert-type server
comp-lzo
# Set log file verbosity.
verb 6
# enable client authentication with username and password
auth-user-pass
# You may try to enable this in some cases
;script-security2
```

~~8.3~~ Configuration file pam radiusd

```
user1@example.com:/etc/pam.d# cat radiusd

# /etc/pam.d/radiusd - PAM configuration for FreeRADIUS

#README# the following text should be on the same line#
auth    required    pam_python.so    /usr/share/ykpam/pam_yubiserver.py
ropval_url=http://localhost/wsapi/ropverify.php?id=%d&otp=%s
send_password    ykotp_re=.*([CBDEFGHIJKLNRTUVcbdefghijklnrtuv]{44})$
hotp_re=null

#this is a new line
auth sufficient pam_yubico.so id=16 debug authfile=/etc/pam.d/yubimap

account      required          pam_permit.so          debug
session      required          pam_permit.so
```

~~8.4~~ Configuration file pam openvpn

```
user1@example.com:/etc/pam.d# cat openvpn

#openvpn configuration for pam

account      required    pam_radius_auth.so
account      required    pam_radius_auth.so
auth         required    pam_radius_auth.so no_warn try_first_pass
```

© 2012 Yubico. All rights reserved.