OpenVPN integration

Contents

Introduction

This article describes how to integrate an existing OpenVPN server with PINsafe, to allow VPN authentication with a Username and One Time Code (OTC) using SMS, mobile phone clients, and the Taskbar. The Single Channel TURing image is not directly displayed within the login.

Prerequisites

- Linux OpenVPN server installation.
- PINsafe installation with network port UDP 1812, accessible from OpenVPN server device.
- OpenVPN Client

Baseline

The Swivel integration was tested with the following versions

Linux OpenVPN server CentOS/RHEL openvpn-2.2.0-3.el6.rf.x86_64

OpenVPN Client 2.1 rc19

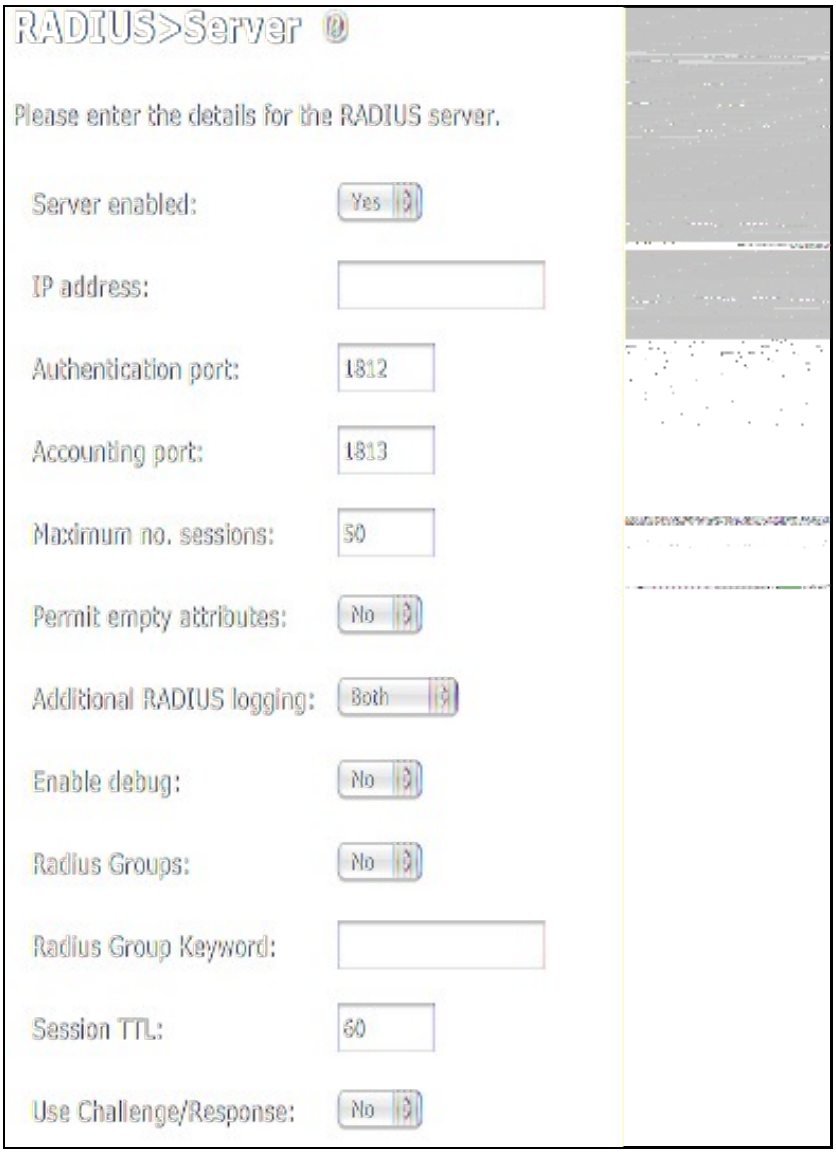
Swivel 3.8

Integration

PINsafe Integration

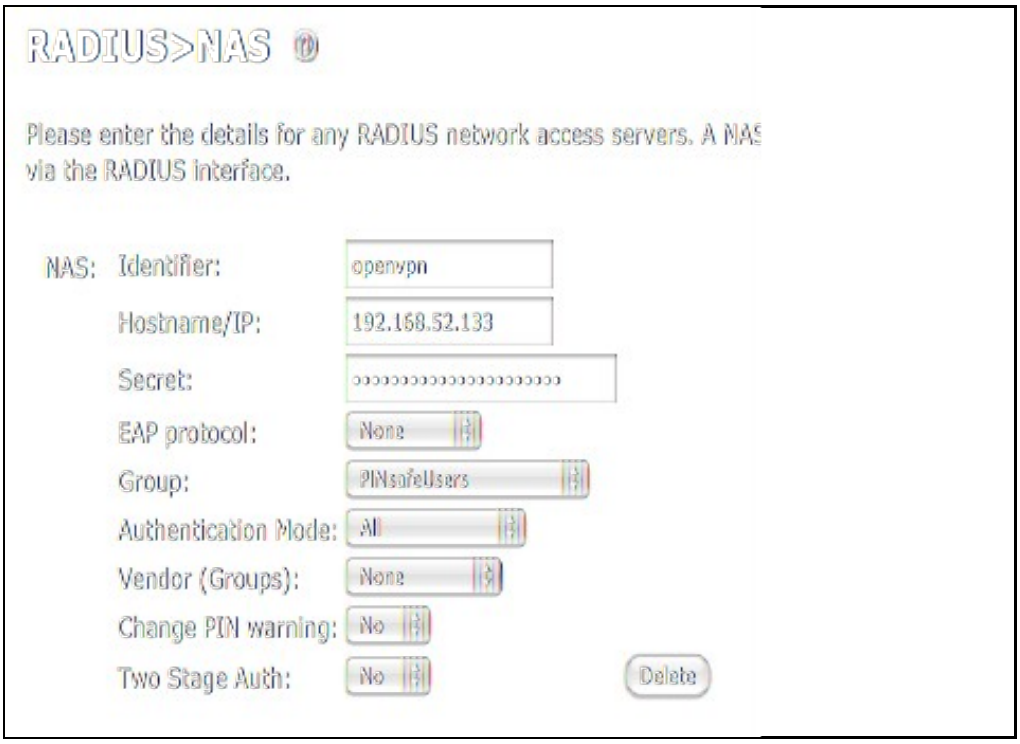
On the Swivel appliance

1.-) Configure and enable RADIUS Server:



Set the option *Server Enabled* to Yes

2.-) Create a new NAS (Network Access Server)



- **Identifier:** Descriptive name of the openvpn server (hostname)
- **Hostname/IP:** OpenVPN Server IP address (as seen by PINsafe. Note if any NAT is required)
- **Secret:** Same secret password set in openVPN file /etc/pam_radius.conf
- **Group:** The PINsafe group permitted to authenticate

OpenVPN Server Integration

In the **OpenVPN Server device** (assumed to be a RHEL/CENTOS), the package **pam_radius** RPM should be installed.

To achieve that run the command *"yum install pam_radius"*.

Edit the openvpn configuration file. By default this file should be **/etc/openvpn/openvpn.conf**.

Add the line:

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

IMPORTANT UPDATE In OpenVPN Server openvpn-2.2.1-1.el6.x86_64 the plugin location changes to **/usr/lib64/openvpn/plugin/lib/openvpn-auth-pam.so**. It is hihgly recommended to perform a search for file **openvpn-auth_pam** to ensure everything will work smooth.

Edit the file **/etc/pam_radius.conf** and add a line with next format:

```
IP_Pinsafesecret   timeout
```

where:

IP_Pinsafe is the IP address where PINsafe installation is.

secret is the password that will be used for the RADIUS communication with PINsafe RADIUS Server.

timeout is the time in seconds that will be defined to wait until a connection attempt with pinsafe server is terminated.

```
Example: "192.168.52.25 secret 10"
```

Edit the file **/etc/pam.d/openvpn** and add after lines at the beginning with

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

On the **OpenVPN server** a service restart will be needed:

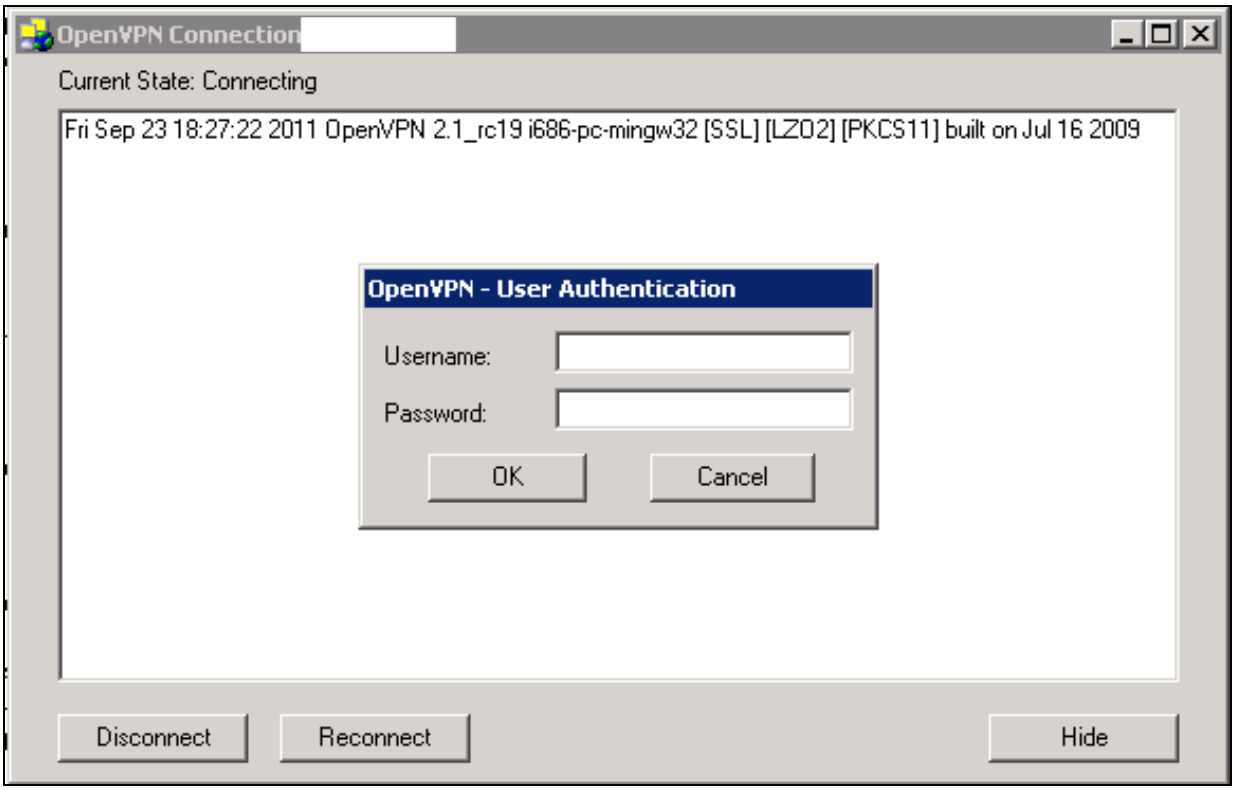
```
"/etc/init.d/openvpn restart" or "service openvpn restart"
```

OpenVPN Client Integration

On the client **OpenVPN configuration file**, add the following line:

```
"auth-user-pass"
```

When the client application starts it will prompt with a window before starting the connection for authentication information:



OpenVPN-GUI for Windows

Tunnelbick for Mac OSX