OpenVPN integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Integration
 4.1 PINsafe Integration
 4.2 OpenVPN Server Integration
 4.3 OpenVPN Client Integration

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:

RADIUS>Server	0	
Please enter the details for the	e RADIUS server.	
Server enabled:	Yes D	
IP address:		
Authentication port:	1812	
Accounting port:	1813	
Maximum no. sessions:	50	asus penganan yang berkenang sang s
Permit empty attributes:	No 3	
Additional RADIUS logging:	Both 3	
Enable debug:	No 👌	
Radius Groups:	No ()	
Radius Group Keyword:		
Session TTL:	60	
Use Challenge/Response:	No 👌	

Set the option Server Enabled to Yes

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

RAD	ius>nas 🛛		
	enter the details for any RADIUS interface.	v RADIUS network access	servers. A MAS
NAS:	Identifier:	openypn	
	Hostname/IP:	192.158.52.133	
	Secret:	000000000000000000000000000000000000000]
	EAP protocol:	None	
	Group:	PINsafeUsers 🕴	
	Authentication Mode:	Al	
	Vendor (Groups):	None	
	Change PIN warning:	No	
	Two Stage Auth:	No	Delete

- Identifier: Descriptive name of the openvpn server (hostname)
- Hostname/IP: Open/VPN Server IP address (as seen by PINsafe. Note if any NAT is required)
 Secret: Same secret password set in open/VPN 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 hingly 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:

DpenVPN Connection
Current State: Connecting
Fri Sep 23 18:27:22 2011 OpenVPN 2.1_rc19 i686-pc-mingw32 [SSL] [LZO2] [PKCS11] built on Jul 16 2009 OpenVPN - User Authentication Username: Password: OK
Disconnect Reconnect Hide

OpenVPN-GUI for Windows

carmen_out: Usuario y clave Por favor ingrese su combinación de usuario y clav
para el VPN.
Usuario:
lawrence
Clave:
🗌 Guardar en Llaveros
Cancelar OK

Tunnelbick for Mac OSX