Cisco IPSEC Client Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
    - 5.1 Configuring the RADIUS server
    - 5.2 Enabling Session creation with username
        - 5.2.1 Setting up PINsafe Dual Channel Transports
    - 5.3 PINsafe Client Configration
        - 5.3.1 PINsafe Dual Channel Configuration
        - 5.3.2 PINsafe Single Channel Configuration
    - 5.4 Cisco VPN Server Configuration
    - 5.5 Cisco IPSEC Client Configuration
        - 5.5.1 Cisco IPSEC Client with Dual Channel Authentication
        - 5.5.2 Cisco IPSEC Client with Single Channel Authentication
        - 5.5.3 Cisco IPSEC client with OTC and AD password
    - 5.6 Additional Configuration Options
    - 5.7 Troubleshooting
    - 5.8 Known Issues and Limitations
    - 5.9 Additional Information

Introduction

The Cisco IPSEC client allows authentication using the following methods from Swivel:

- SMS Text
- Mobile Phone Client
- Token
- Taskbar Utility

This document outlines how to integrate PINsafe Turing image using the PINsafe Taskbar for Microsoft Windows, with the Cisco IPSEC VPN Client. If SMS use is only required then the below Taskbar steps are not required.

For the Cisco ASA PINsafe integration see Cisco ASA Integration

Prerequisites

PINsafe 3.x, 3.5 for RADIUS groups

Turing image available to user from across internet

Cisco IPSEC VPN Client

A Cisco Authentication device using PINsafe as a RADIUS server

PINsafe Taskbar for Microsoft Windows

Cisco IPSEC Client

Cisco documentation

Baseline

PINsafe 3.5

Cisco IPSEC VPN Client 5.0.02

PINsafe Taskbar 1.3.01

Architecture

The user starts the Cisco IPSEC VPN client which starts up the PINsafe Taskbar utility and generates a Turing image for the user to use for the authentication.

Swivel Configuration

Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

Enabling Session creation with username

To allow the TURing image, PINpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

Setting up PINsafe Dual Channel Transports

See Transport Configuration

PINsafe Client Configration

PINsafe Dual Channel Configuration

No specific client requirements for Dual Channel integration.

PINsafe Single Channel Configuration

Follow the installation notes to install the PINsafe Taskbar utility. Ensure that a Single Channel image can be generated. See Taskbar How to Guide. Note the intehgration has only been tested with the Turing Single Channel Image.

Cisco VPN Server Configuration

Configure the VPN server according to the Cisco Documentation, configuring the Cisco VPN server to use PINsafe as a RADIUS authentication server.

Cisco IPSEC Client Configuration

Cisco IPSEC Client with Dual Channel Authentication

No further configuration is required for the Cisco IPSEC client

Cisco IPSEC Client with Single Channel Authentication

Follow the Cisco installation notes. Then open the VPN Client Options menu and choose Application Launcher. The VPN Client displays a dialog, click on Enable and then enter the PINsafe Taskbar utility path and the required syntax:

Example: C:\Program Files\Swivel Secure Ltd\PINsafe Taskbar\PINsafeTaskbar.exe show

Click Apply to activate the application.

Note: The Cisco IPSEC VPN Client may need to be restarted.

Cisco IPSEC client with OTC and AD password

The Swivel server can be configured to use AD password and OTC. On the Swivel Administration console under RADIUS/NAS for the Cisco ASA set Check password with repository to Yes and apply the settings. The Password is entered first followed by the OTC, as passwordOTC. See also Password How to Guide.

Additional Configuration Options

Troubleshooting

Start the Cisco IPSEC VPN client, and click on connect. A Turing window should appear. A One Time Code can be obtained for authentication.

Check the PINsafe logs for Turing images and RADIUS requests.

No RADIUS connections seen

Check ports, Cisco uses 1645/1646 by default, Swivel uses 1812/1813 by default.

Cisco continues to use AD/other password instead of Swivel OTC

Rremove the Swivel RADIUS servers, apply the configuration then reenter them. Apply the configuration and then test to ensure RADIUS requests are seen in the Swivel logs.

Known Issues and Limitations

None

Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com