Checkpoint SecureClient Integration

Checkpoint SecureClient

Integration Guide

Version 1.1 March 2010, Updated March 2014

Contents

Introduction

This document outlines the steps required to integrate the Checkpoint SecureClient VPN software with Swivel.

Swivel users can use Swivel?s Token, SMS, Mobile Phone Client, as well as the single channel TURing and Pinpad methods to retrieve a One Time Code or a Security string.

With Single Channel methods, the user must be presented with a TURing or Pinpad at sign-in time, so they can extract their OTC such as the TURing using the Taskbar.

The settings and software can be configured for larger deployments within an msi file to ease installation.

Prerequisites

Checkpoint SecureClient E75. This solution is not compatible with E80.

Swivel 3.x. Where the Single Channel image is to be used, this should be presented to the user through a Network Address Translation to the Swivel server.

Swivel SecureClient software

- The file extensions have been changed to prevent them being blocked by filters etc .dll files to .dlx, and .reg to .rex. These need to be renamed back again.

Baseline

Checkpoint SecureClient R60 and R77,

Checkpoint SecureClient E75.10 (tested for Token, SMS, Mobile App, Taskbar)

Checkpoint VPN server R75.45 (tested for Token, SMS, Mobile App, Taskbar)

Swivel 3.6, 3.9.7, 3.10

Architecture

The user connects to the Checkpoint VPN by using the SecureClient software. The Checkpoint is configured to use a Swivel server for radius authentication. Users are stored and maintained in Swivel.

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 Swivel Dual Channel Transports

See Transport Configuration

Configuring the Checkpoint VPN-1/Firewall-1

Checkpoint VPN-1/Firewall-1 configuration Overview

The steps for enabling SecureClient users on the Checkpoint VPN-1/Firewall-1 is outlined below. For further details refer to the VPN-1/Firewall-1 Administration Guides.

1. Install the SecureClient license.

2. Create SecureClient users.

3. Define a SecureClient authentication method using PINsafe as a RADIUS server

4. Create a SecureClient group.

5. Add SecureClient users to the SecureClient group.

6. Define a Remote Access Community and participants.

7. Create SecureClient rule for the Remote Access Community.

8. Create the Desktop Security Policy rules.

9. Install Security Policy.

Configure Checkpoint VPN-1/Firewall-1 to use the Swivel RADIUS server

Create a RADIUS server entry on the Checkpoint Policy Editor

Select Manage/Network Objects' then Click on New then Workstation. In the Workstation Properties window, enter the, Swivel server IP Address, choose 'Host' for Type. For the Comment enter enter "PINsafe authentication". When complete, click OK. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

Select Manage/Servers then click on New and from the menu select Radius. In the RADIUS Server Properties window enter the following:

Name RADIUS server name

Comment information e.g. PINsafe RADIUS server

Colour A colour for the object (we like orange!)

Host hostname of the Swivel server created above

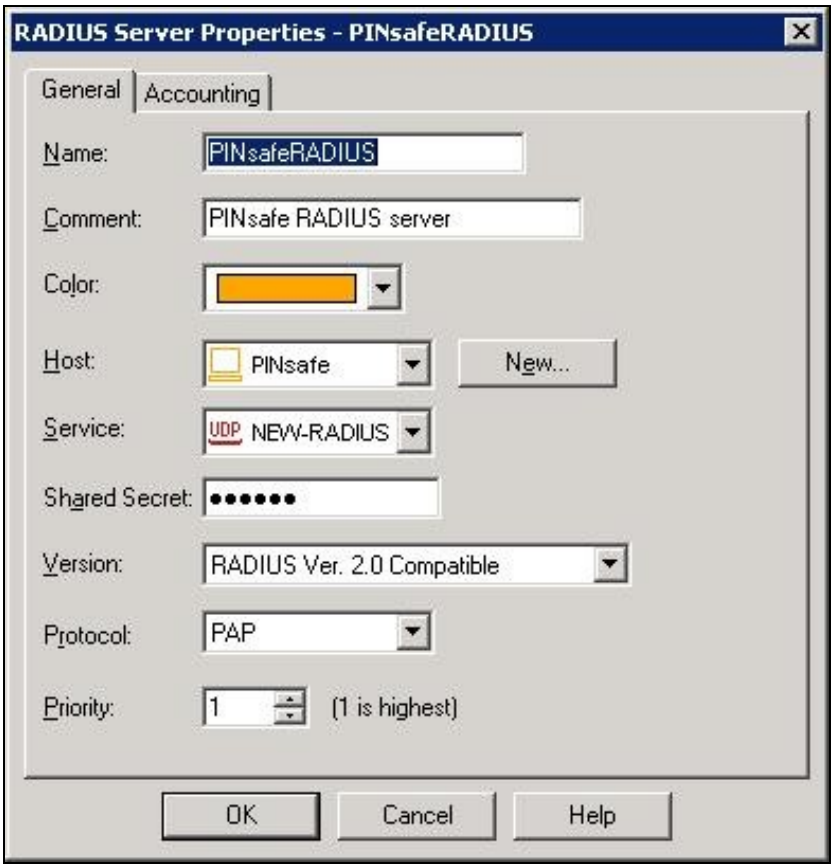
Service select New Radius (Uses port 1812)

Shared secret enter the shared secret that is also entered on the Swivel server

Version select the RADIUS version required

Protocol select the required RADIUS version

Priority The priority for authentication to multiple RADIUS devices



To configure External Checkpoint VPN-1/Firewall-1 users to authenticate by RADIUS

External User Profiles There are two different types of External User Profiles available in the Check Point VPN-1/Firewall-1 product, either match all users or match by domain, whereby users are differentiated by their domain name.

The steps below will configure an External Profile of Match All Users.

1. On the Checkpoint VPN-1/Firewall-1 configuration select Manage/Users and Administrators/New/Match All Users/Default.

2. The user generic* is created and greyed out.

3. Select the Authentication tab.

4. From the drop down box choose RADIUS as the user?s Authentication Method.

For further details on the available user authentication methods, configuration and setup, refer to the VPN-1/Firewall-1 Administration Guides.

The SecureClient is now ready for two factor authentication using standard SMS delivery or the Mobile Phone Client.

Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Open the Secureclient, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SecureClient login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

Modifying the Checkpoint SecureClient for Single Channel and Advanced SMS features

Note that all .dll files have been renamed to .dlx, and .reg files to .rex, to avoid problems with email filters. You will need to change the names back before deploying the files.

Stop the SecureClient or ensure it is not running.

Copy PINsafeAuthGUI.dll, and copy it to the SecuRemote\bin folder

Edit SecuRemote\database\userc.C. and add the below to the :options section

```
:guilibs (
: ("C:\Program Files\CheckPoint\SecuRemote\bin\PINsafeAuthGUI.dll")
```

)

Edit RegSettings.reg. to set the correct Swivel server and possibly the port and context. Double-click RegSettings.reg to install the registry settings the DLL needs.

The options are:

PINsafeServer: The IP address of the Swivel server. This should be a NAT address of the Swivel server and accessible from the client.

PINsafeProtocol: 1 for https, or 0 for http

PINsafePort: The port used to retrieve single channel images from the Swivel server, usually 8443 for a Swivel virtual or hardware appliance. For a software only install see Software Only Installation

PINsafeContext: The installation instance of the pinsafe server, usually pinsafe or proxy for a Swivel virtual or hardware appliance

PINsafeAllowSelfCert: 1 to allow self signed certificates on the Swivel server, 0 to not allow them to be used

PINsafeSecret:

PINsafeUser: The user for authentication can be pre-configured. Do not set this value if this is a template to be used for deployment to multiple users.

PINsafeChannelType: single or dual channel communications. Setting dual, requests an SMS security string by the on demand method. The On Demand authentication must be enabled on the Swivel server.

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="localhost"
"PINsafeProtocol"="1"
"PINsafePort"="8080"
"PINsafeContext"="pinsafe"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Swivel virtual or hardware Appliance Values:

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="External NAT IP of PINsafe server"
"PINsafeProtocol"="1"
"PINsafePort"="8443"
"PINsafeContext"="proxy"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Verify that winhttp.dll is present in C:\Windows\System32

Start SecureClient. Click connect. Under Options, Change Authentication to Secure Authentication API.

When you click Connect, you should now either see a dialog with a TURing on it, or "CONFIRMED" for dual channel, in which case a security string will be sent by the appropriate transport. The password field has been left in case you want a password as well as a OTC, but this can be removed if required. Enter the OTC, and hopefully it will authenticate.

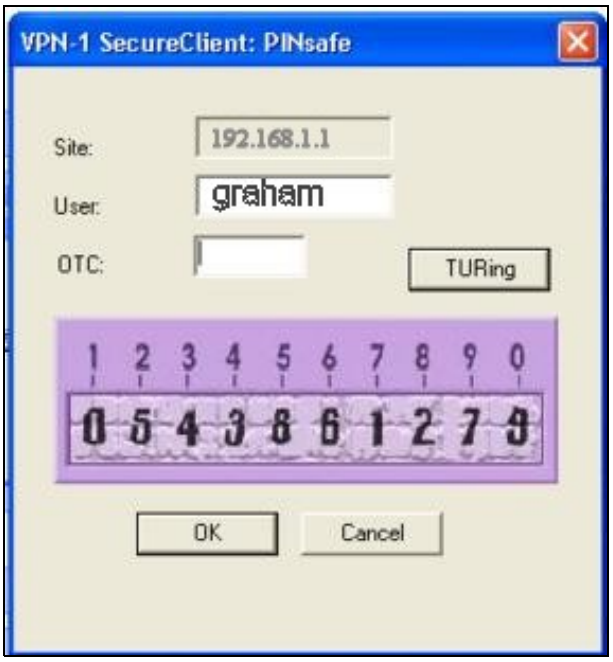
Removing the Swivel SecureClient

To remove the Swivel authentication remove the earlier added content in Edit SecuRemote\database\userc.C.

then restart the client

Verifying the Installation

Login using the Turing or SMS.



Bulk deployment

With a tested deployment, it is possible to take these settings and create a msi file that will install the Swivel SecureClient software.

For further information see [[1]]

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Check the Checkpoint Firewall Logs

radius not supported

This can be seen when using local policies, switch to a Global Policy for RADIUS authentication and test, or for individual users use RADIUS authentication.

Known Issues and Limitations

Checkpoint will not accept RADIUS passwords greater than 16 characters in length. If check password with repository is used, then the PIN length will also need to be taken into account, i.e. for a 4 digit PIN, this restricts the length to 12 characters. Two stage RADIUS authentication will bring this back to 16 characters.

Additional Information

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