Cyberoam UTM SSL VPN

Contents

Introduction

This document describes steps to configure a Cyberoam UTM firewall with integrated SSL VPN and PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility. It is not possible to embed the graphical single channel image directly into the login page.

Prerequisites

Cyberoam CRxxx (except CR15i and CR15wi as these do not have SSL VPN support)

Cyberoam Firmware 10.x

PINsafe 3.x

Baseline

Cyberoam CR25i firmware 10.01.0 build 739

PINsafe 3.8

Architecture

The Cyberoam CR25i makes authentication requests against the PINsafe server by RADIUS. PINsafe can also verify the AD or other supported repository password where required.

Swivel Configuration

Configuring the RADIUS server

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

If Tight Integration is to be used with RADIUS groups then ensure RADIUS Groups is set to YES.

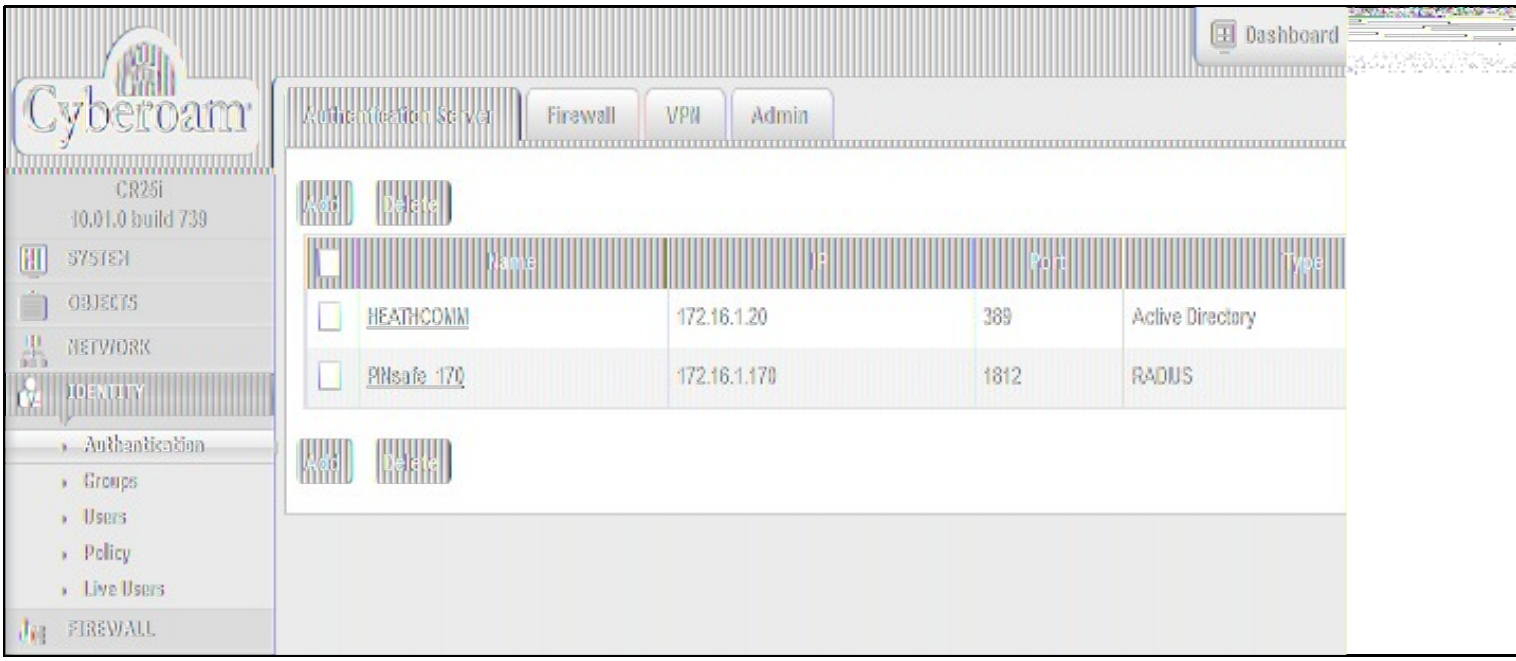
PINsafe Dual Channel Authentication

See Transport Configuration

Cyberoam CR25i Configuration

Define a RADIUS server on the Cyberoam

On the Cyberoam CR25i Administration console select Identity, then Authentication and the Authentication Server Tab, then click on Add.



Enter the PINsafe RADIUS server authentication details as follows:

- Server Type: RADIUS Server
- Server Name: Descriptive name for the PINsafe server
- Server IP: PINsafe server IP address
- Authentication Port: usually 1812
- Shared Secret: A secret password also entered on the PINsafe RADIUS NAS entry
- Integration Type: Loose Integration or Tight Integration as described below:

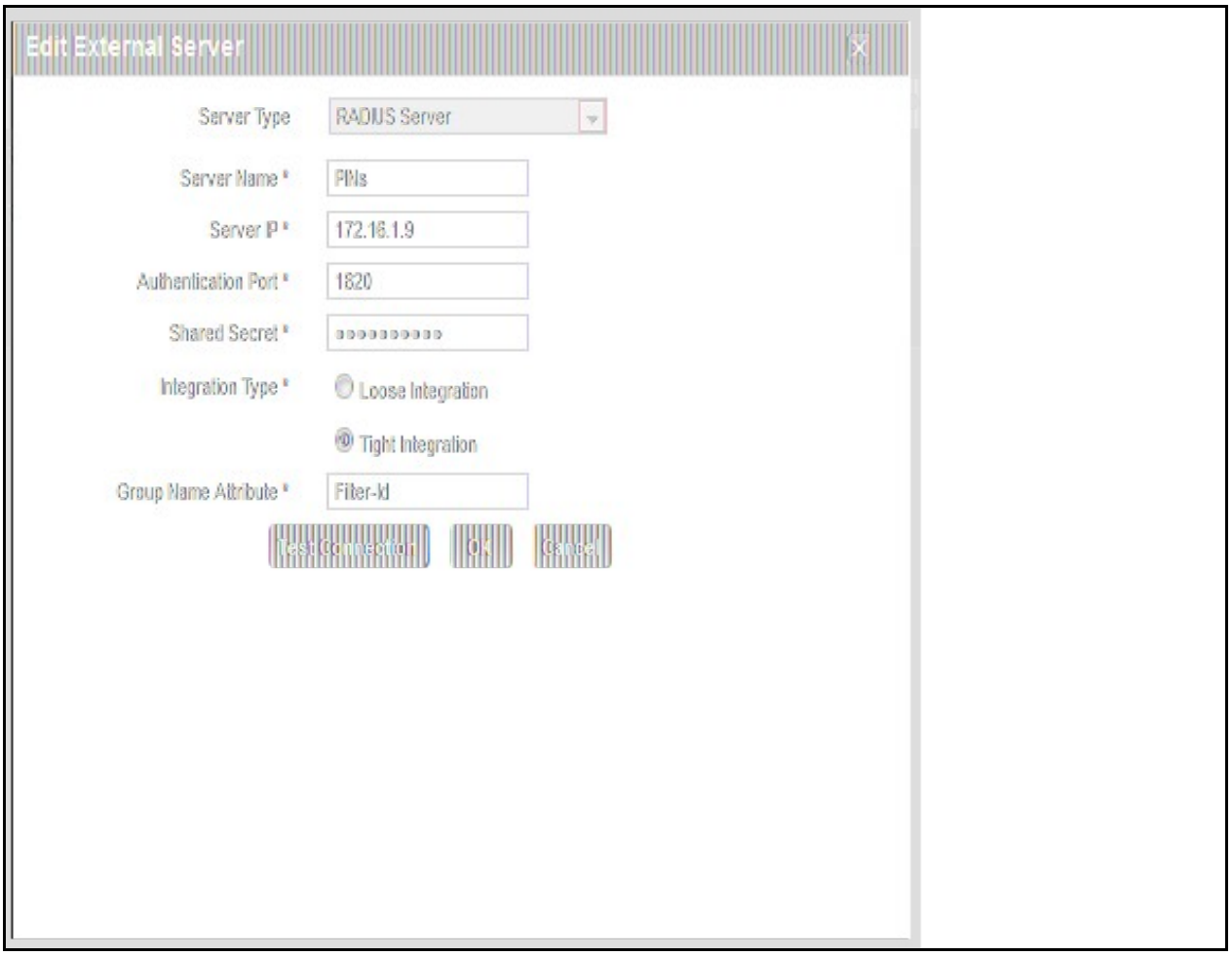
Loose Integration

With loose integration, Cyberoam does the Group management and does not synchronize groups with RADIUS server when user tries to logon. By default, users will be the member of Cyberoam default group irrespective of RADIUS Server group. Administrators can change the group membership. If Loose Integration is used, new users will be added to the default user group on the Cyberoam.

Tight Integration

With Tight integration, Cyberoam synchronizes groups with the PINsafe RADIUS Server every time the user tries to logon. Hence, even if the group of a user is changed in Cyberoam, on each subsequent login attempt, the user logs on as the member of the same group as configured on the PINsafe RADIUS Server. In this case group membership of each user is as defined in the RADIUS Server. The PINsafe RADIUS server needs to be configured to use RADIUS groups.

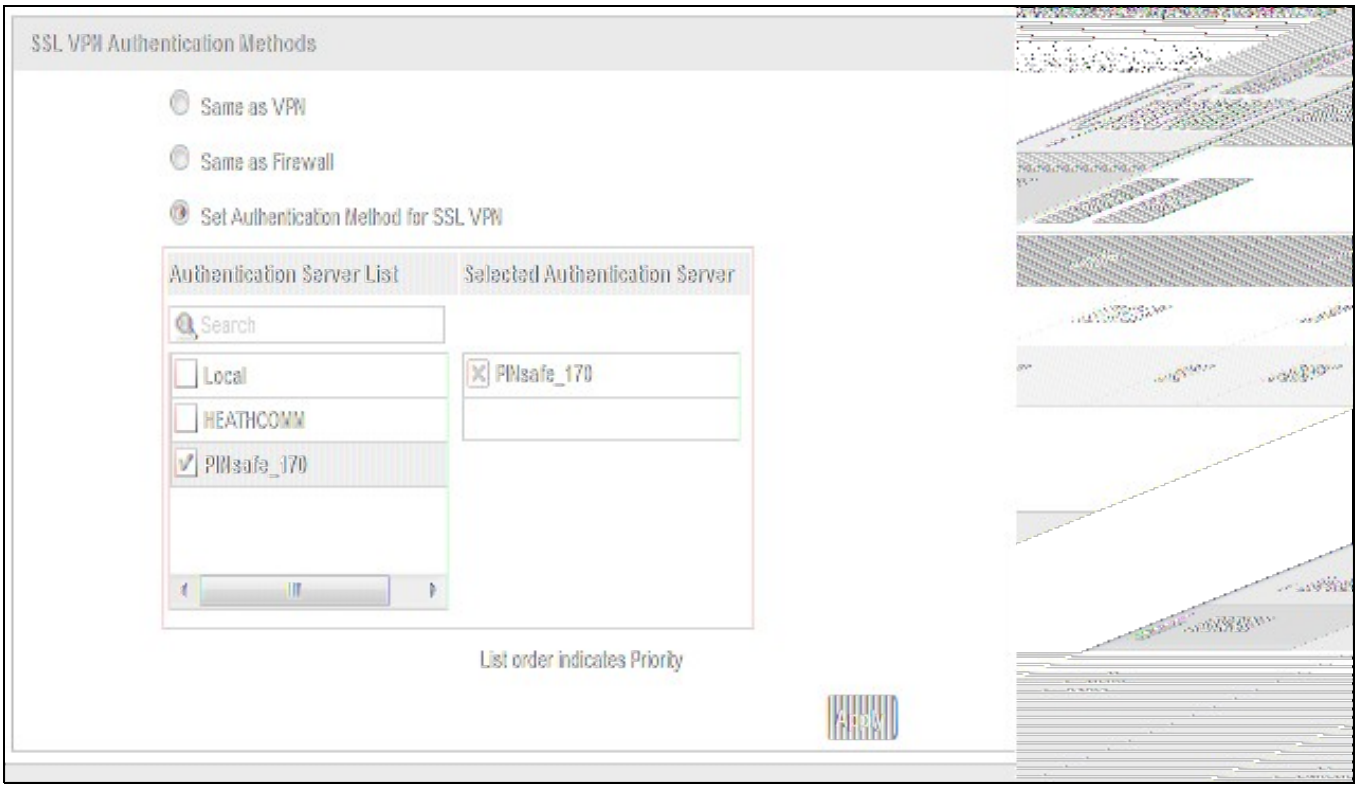
Note: when creating a SSL VPN policy, a user needs to login to the Captive Portal first, which creates the RADIUS user on the Cyberroam. They can then login to the SSL VPN portal



Cyberoam SSL VPN Authentication Methods

On the Cyberoam Administration console select Menu Identity, then Authentication then the VPN tab and select the Set Authentication Method for SSL VPN. All authentication servers that have been configured on the unit is shown on the left side. So the PINsafe RADIUS server added in the previous step should show up here. Tick the server to select it. It will then be shown in the list on the right side. It is possible to select more than one server if you have an active/active PINsafe configuration.

Note is is not possible to check authentication against multiple authentication types, the first authentication method that matches the user will be used. To configure authentication with multiple authentication servers see Additional Cyberoam Configuration Options below.



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. Browse to the SSL VPN login page, 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 SSL VPN 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.

Additional Cyberoam Configuration Options

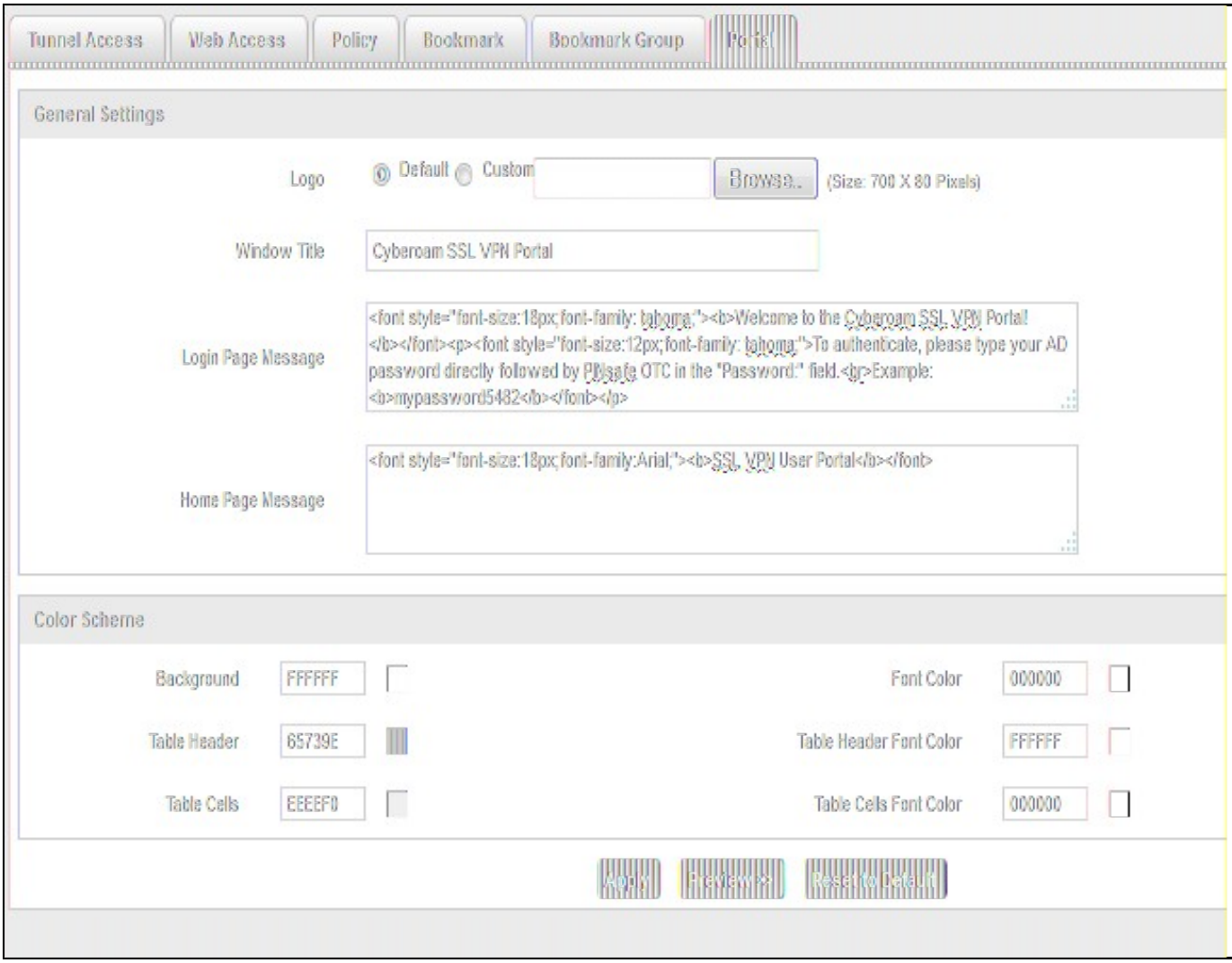
Configuring Authentication with AD Password and OTC

PINsafe can be configured to Check the password of supported repositories such as Active Directory. To do this the Check Password with repository must be enabled on the PINsafe server. PINsafe 3.7 and earlier have this as a global setting affecting all users, to select this option on the PINsafe Administration Console select Policy then Password, for PINsafe 3.8 onwards, it is defined by each NAS, under RADIUS then NAS. For more information see the Password How to Guide

The Password must be entered followed directly by the OTC on the login page by the user, e.g. passwordnnnn

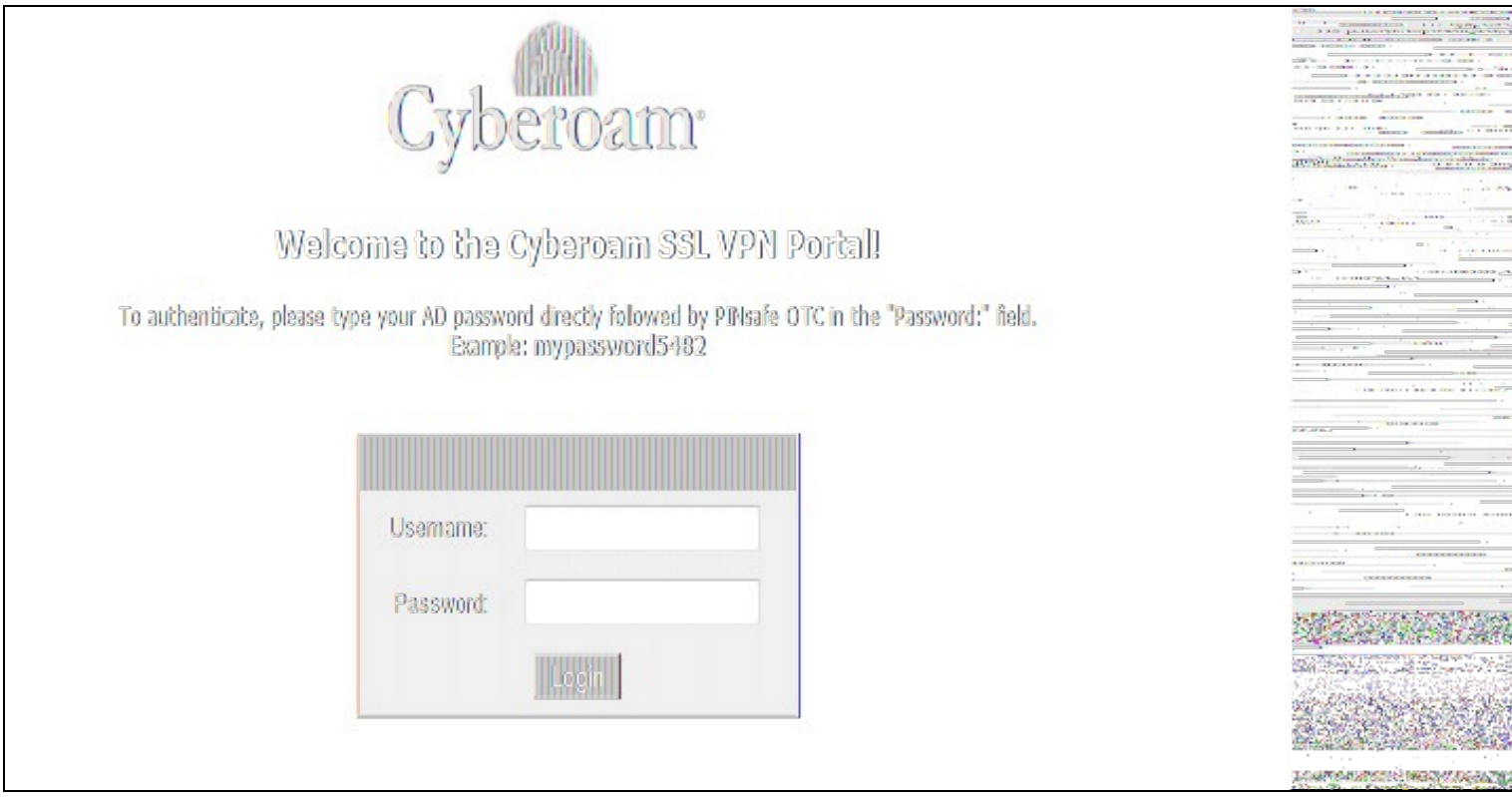
Modifying the Cyberoam login page

The Cyberoam login page can be modified to display different text and colours. To do this, on the Cyberoam Administration console select VPN, then SSL then select the Portal Tab. The below example shows modification for explianing how to add AD password and One Time Code.



Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. The below example shows the combination of AD password with OTC for authentication.



Troubleshooting

Check the PINsafe logs for RADIUS requests.

Known Issues and Limitations

Dual Channel authentication and Taskbar only

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