Citrix Access Gateway Enterprise Edition 8

Contents

Introduction

This document shows the steps required to integrate PINsafe with the Citrix Access Gateway Enterprise Edition (Formerly Netscaler VPN) version 8.x to 9.1. Version 9.2 is covered in a separate document see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring PINsafe to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

To use the Single Channel Image such as the TURing Image, the PINsafe server must be made accessible. The client requests the images from the PINsafe server, and is usually configured using Network Address Translation, often with a proxy server. The PINsafe virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

Prerequisites

Access Gateway Enterprise Edition firmware version 8.x to 9.1.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

PINsafe 3.x

PINsafe server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the PINsafe server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or PINsafe files File:CAGEE_8_files.zip for versions 8 - 9.1

Baseline

PINsafe 3.5

Citrix Access Gateway Enterprise Edition 8.0. Also tested with 9.1.

Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the PINsafe server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside if they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the pinsafe modifications.

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

Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the virtual or hardware appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the PINsafe server to be accessible from the internet, usually with a NAT. See also Multiple Security Strings How To Guide

Login Page Customisation

SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

Navigate to the location of the pages to be modified, and make a local backup copy of them

```
>cd /netscaler/ns_gui/vpn
>cp index.html index.html.bak
>cp login.js login.js.bak
```

Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere regualarly to prevent work in progress being lost during development. How to manage these pages is covered later.

The index.html file now needs to be edited (or replaced). The tool vi can be used to do this but an application such as WinSCP will make this easier. The required files can be found in the prerequisites.

A pinsafe.js file that is a modification of the existing login.js file is required. Make a copy of login.js called pinsafe.js The showTuring function shown below needs to be added to this file. Note the sUrl setting needs to be changed to reflect the IP address and port number of the relevant PINsafe server. There are other changes that can be made, eg changing the prompt to read One-Time code instead of password.

For a virtual or hardware appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, a script must be created that runs at startup to copy the modified files back to this location. The nsafter.sh or rc.netscaler shell scripts can be created or modified to accomplish this. For example via ssh:

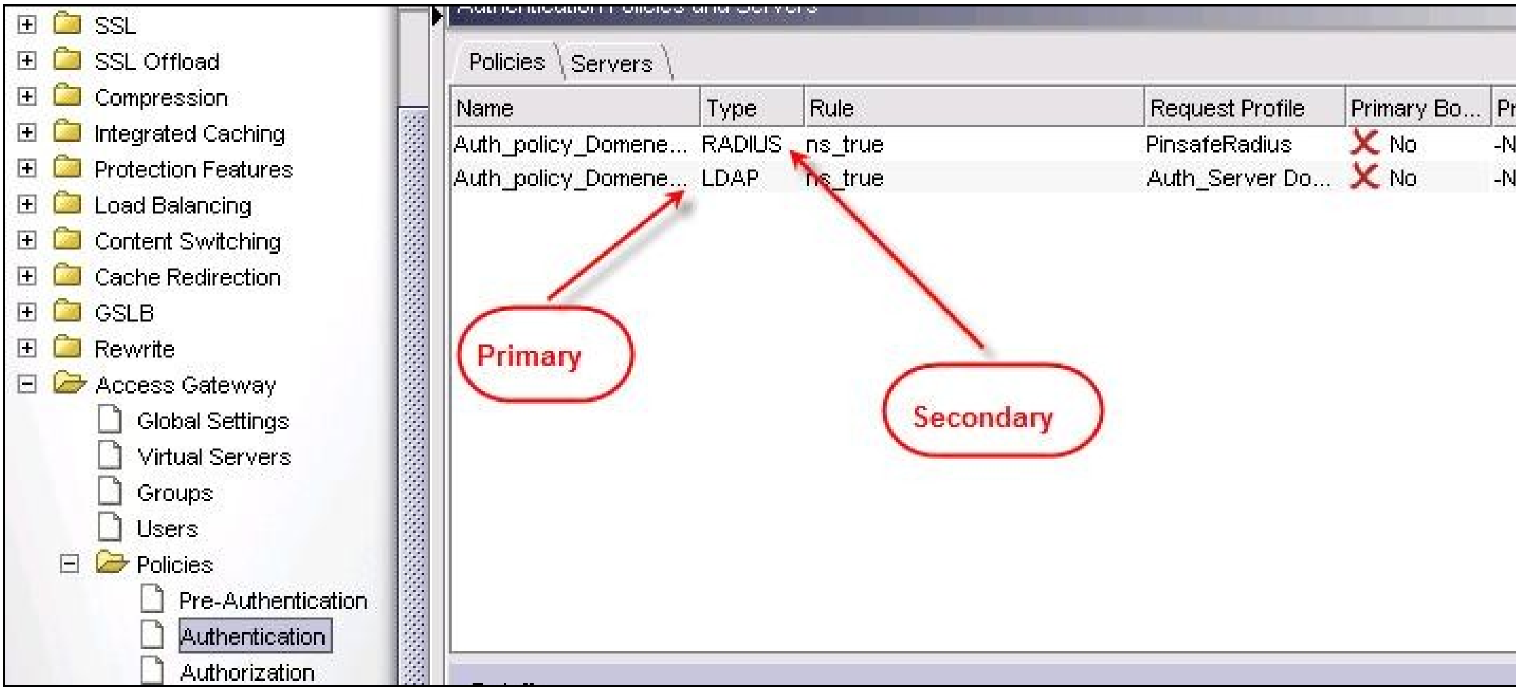
```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod /netscaler/ns_gui/vpn/pinsafe.js >> /nsconfig/rc.netscaler
```

Citrix Advanced Access Gateway Enterprise Edition RADIUS Cofiguration

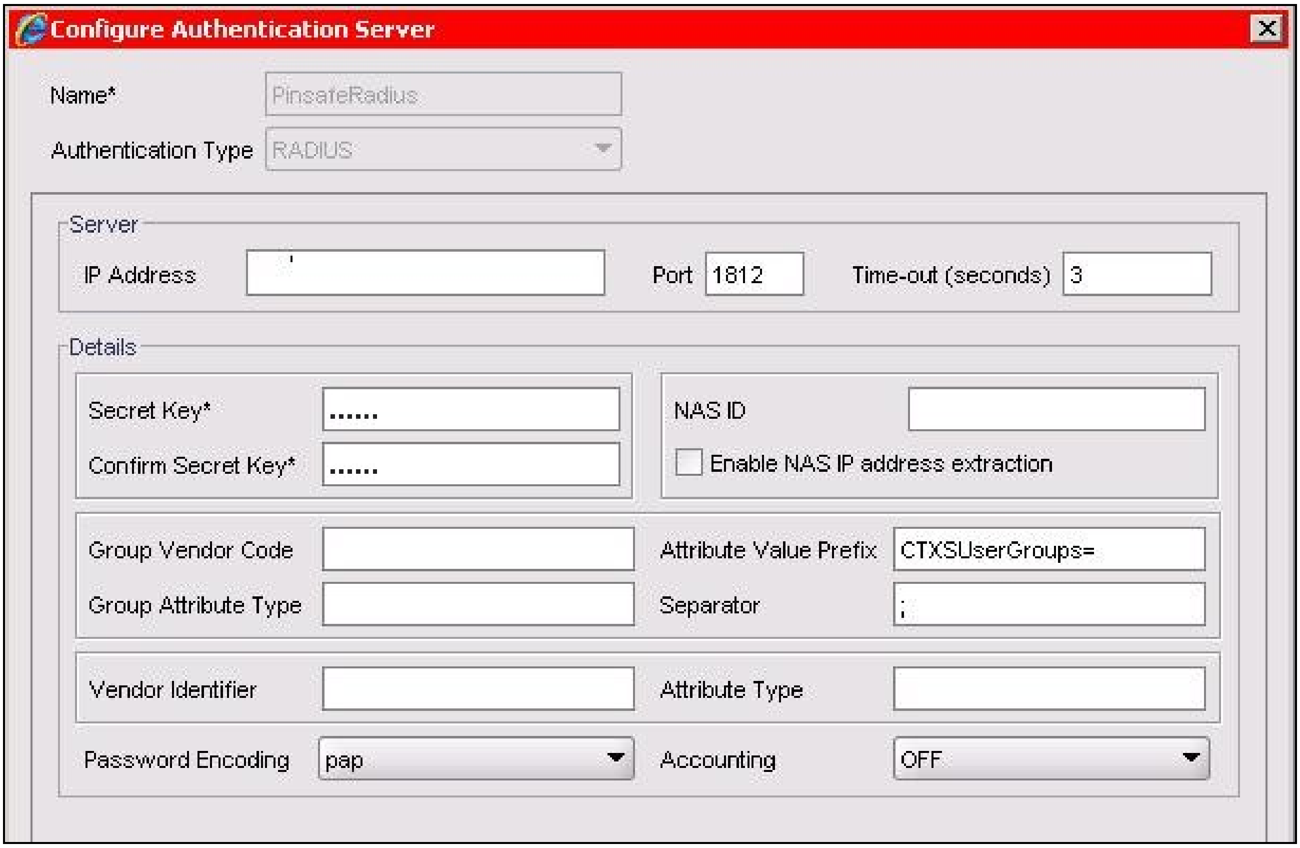
The CAGEE needs to be configured to use the PINsafe server as a RADIUS authentication server. Where a VIP is being used on the PINsafe server then configure the RADIUS request to be made against each of the PINsafe servers together with the use of Session Sharing.

PINsafe can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Create a new Authentication policy (under the Netscaler->System->Authentication menu). The policy must specify RADIUS and then the PINsafe server must be added as a RADIUS server.



Name	Type	Rule	Request Profile	Primary Bo...	Pr
Auth_policy_Domene...	RADIUS	ns_true	PinsafeRadius	✗ No	-N
Auth_policy_Domene...	LDAP	ns_true	Auth_Server Do...	✗ No	-N



Name* PinsafeRadius

Authentication Type RADIUS

Server

IP Address

Port 1812

Time-out (seconds) 3

Details

Secret Key* ......

Confirm Secret Key* ......

NAS ID

□ Enable NAS IP address extraction

Group Vendor Code

Attribute Value Prefix CTXSUserGroups=

Group Attribute Type

Separator ;

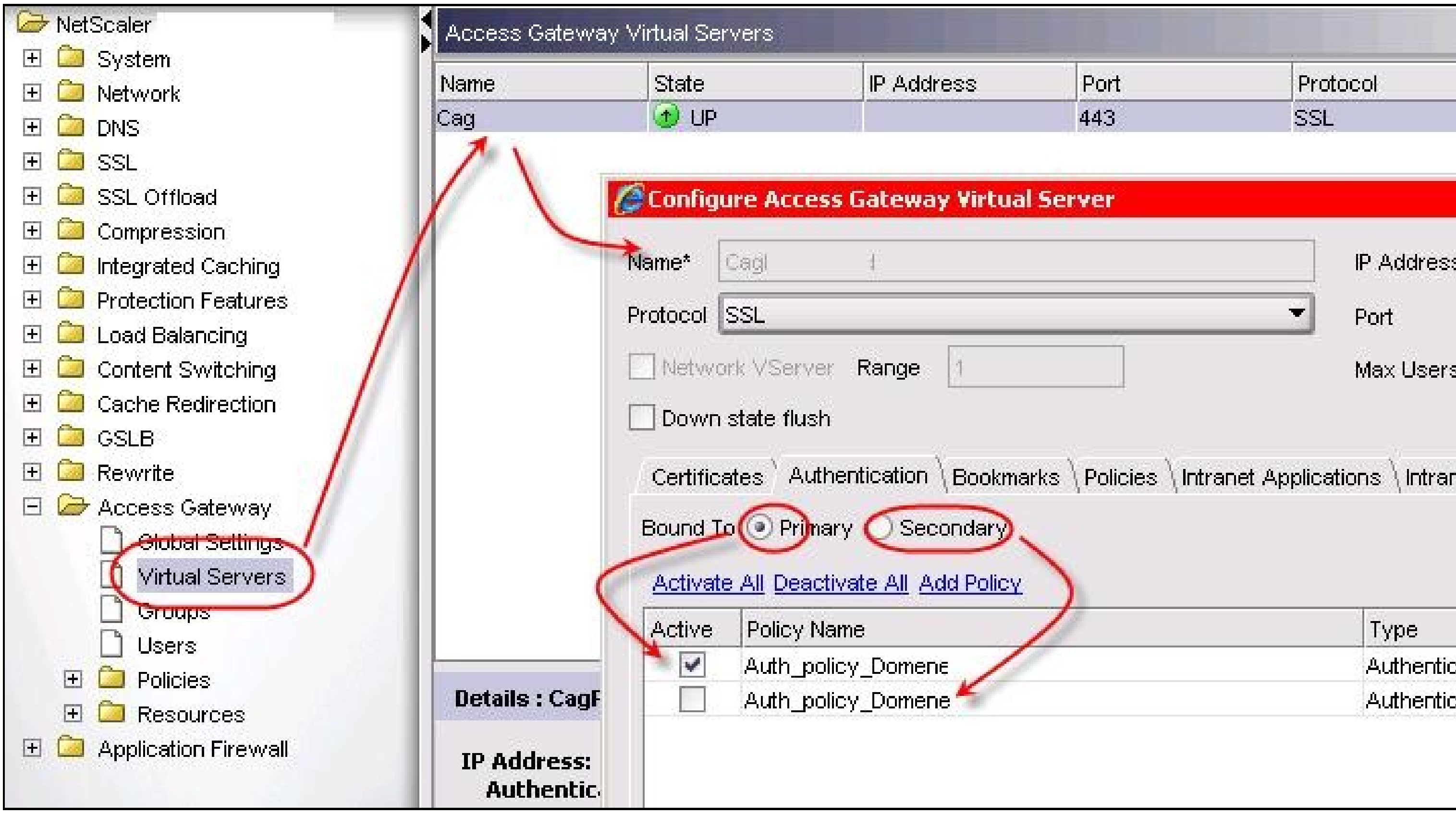
Vendor Identifier

Attribute Type

Password Encoding pap

Accounting OFF

On the SSL-> Virtual Server menu, the created policy must be activated. If just PINsafe authentication is required then you ensure that only the PINsafe policy is active. If you require AD and PINsafe authentication then you need to make active the PINsafe policy as the secondary. Save the settings.



Access Gateway Virtual Servers

Name	State	IP Address	Port	Protocol
Cag	UP		443	SSL

Configure Access Gateway Virtual Server

Name* Cagl

Protocol SSL

□ Network VServer Range 1

□ Down state flush

Bound To ● Primary ○ Secondary

Active	Policy Name	Type
☑	Auth_policy_Domene	Authentic
□	Auth_policy_Domene	Authentic

Additional Configuration Options

Challenge and Response

Citrix Access Gateway Enterprise Edition 9.1 supports RADIUS Challenge and Response

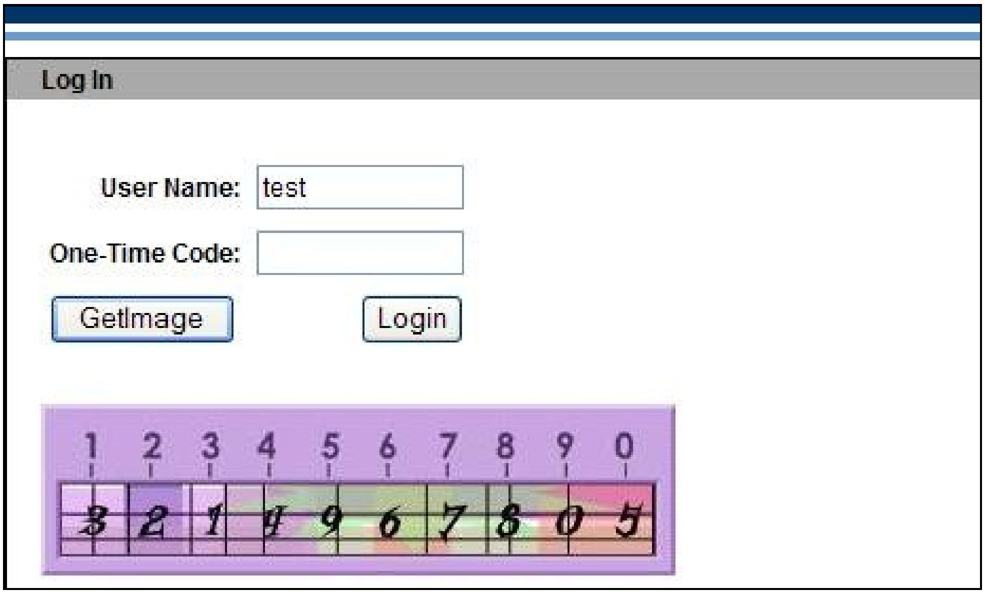
Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required.

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.



Log In

User Name: test

One-Time Code:

Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Image from PINsafe server absent

Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

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