Challenge response

Contents

Using PINsafe with RADIUS Challenge Response

Some One-time code based authentication systems may require two stages of authentication, eg first a username and password then username and one-time code. This article explains how such systems can be supported by PINsafe using Checkpoint secure client although Citrix Web Interface and other systems are known to support this model.

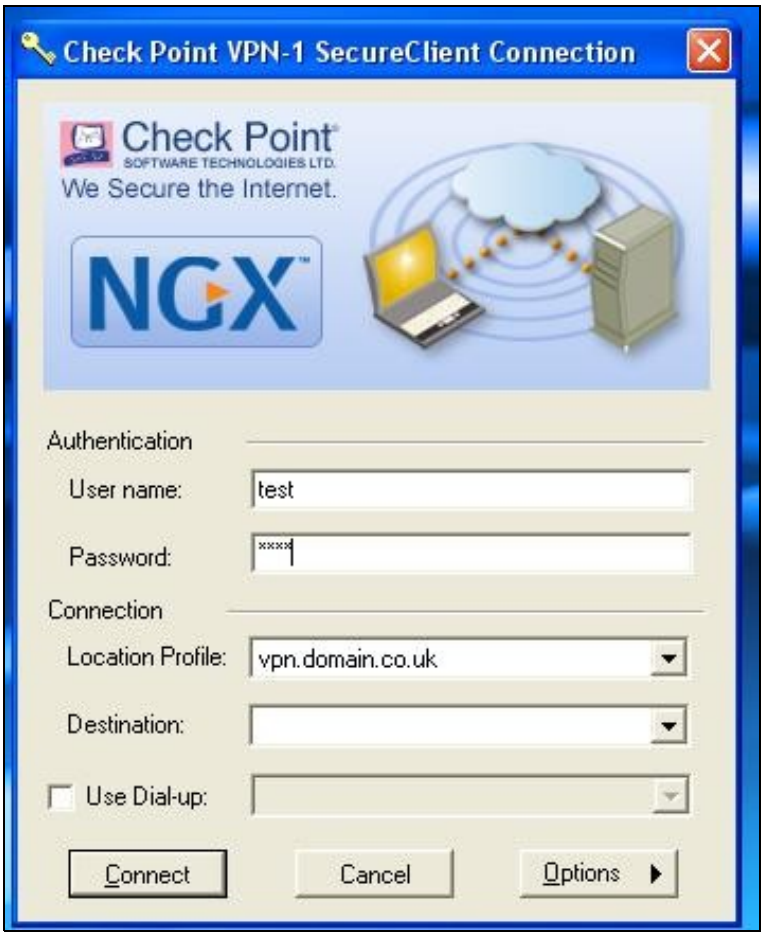
The Checkpoint solution was developed with the assistance of Network Integration.

This only applies to certain versions of PINsafe, eg Version 3.5 r3223 or later.

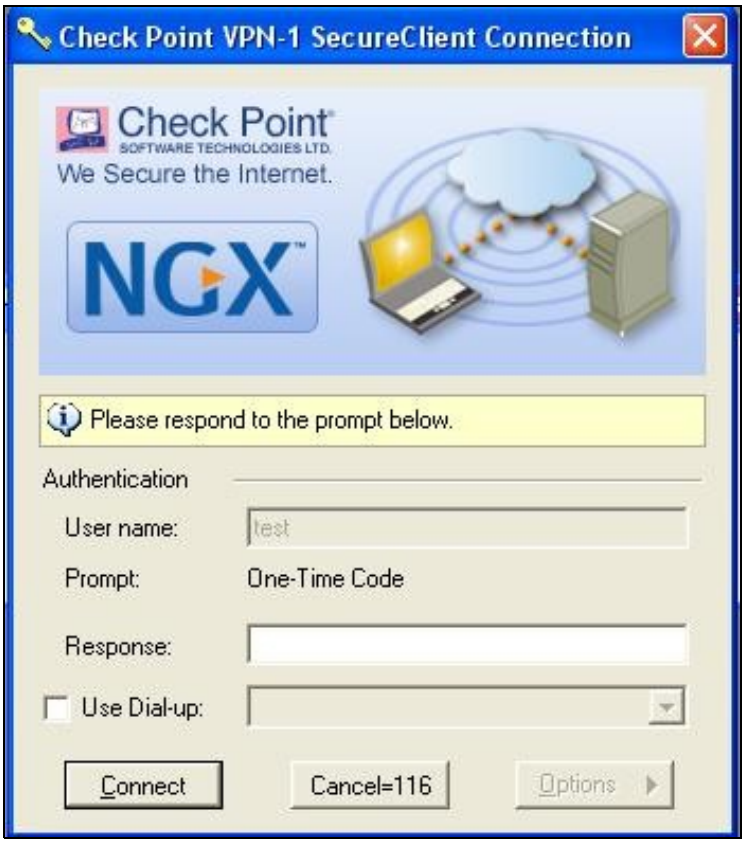
See Also [Challenge and Response How to Guide]

User Experience

The user starts their Secure client and is prompted for their username and static password.



If their username is correct, they then are prompted a with a second dialogue box for their one-time code. If PINsafe is set up for Dual Channel on-demand mode, at this stage their are sent a dual channel security string or one-time code



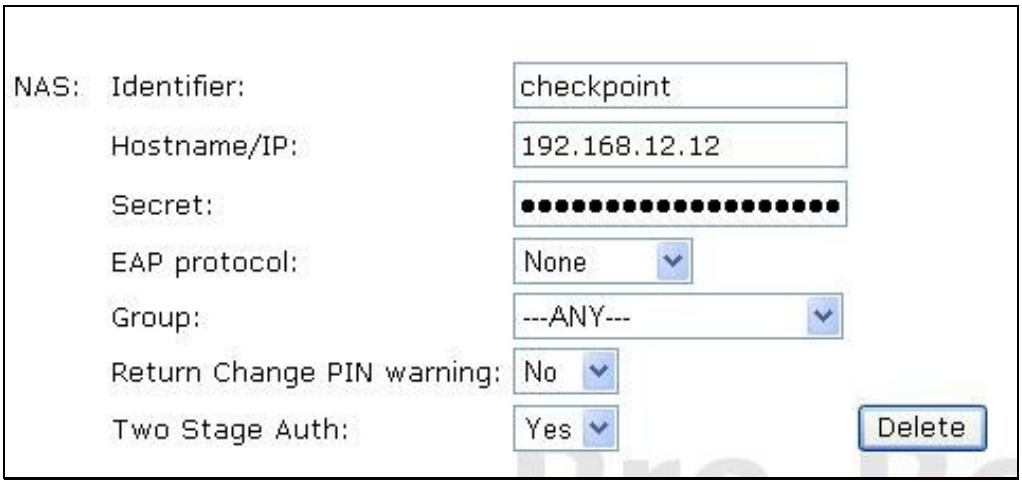
The user then enters their one-time code, eg based on the dual channel message that they have just received for on-demand mode or based on a security string already in their possession for dual channel auto-mode.

If this is correctly entered the user is authenticated.

Configuring PINsafe

To use this form of authentication you need to enable the PINsafe RADIUS server and then create a NAS entry for the VPN server, in this example the a Checkpoint VPN1 Server.

The NAS needs to be configured to use Two Stage authentication (auth) but not to Return a change PIN warning



With this configured, when a user attempts to authenticate via this NAS, PINsafe will assume that just the password has been submitted.

PINsafe will then check this password and, if it is correct, respond with a RADIUS challenge (One-time code) to the VPN server. This in turn causes the client to display the second dialogue prompt

Also, if the password is correct and PINsafe is set to Dual Channel On Demand, PINsafe will send out a dual channel message to the user in the appropriate format.

When the users submits their one-time code in this second dialogue box, PINsafe performs an authentication based on the password submitted initially and the one-time code just submitted.

Passwords

The first stage of this authentication model is to check the users password. This can be implemented in one of two ways.

- PINsafe can check against a password set for the user by PINsafe
- PINsafe can check the submitted password against the user's repository, eg Active Directory.

To use the second of these two options ensure that the Check Password with Repository option is selected on the Policy -> Password screen.