



External Authentication with Check Point NGX

Authenticating Users Using SecurAccess Server by SecurEnvoy

Compiled By:	Chris Presland	v1.0
Date	29th September	
Revision History	Phil Underwood	v1.1

This document describes how to integrate Checkpoint VPN with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Checkpoint VPN provides Client - Secure Remote Access to corporate network and application resources.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Checkpoint VPN) from any device, without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)
SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

Checkpoint VPN can be configured in such a way that it can proxy the Authentication request of the users to an external directory (such as Radius). This is how the Checkpoint VPN was configured. All authentication requests were forwarded to SecurEnvoy Authentication server. Both Checkpoint and SecurEnvoy utilize a web GUI for configuration. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below

Checkpoint

Checkpoint NG software
Software Revision Version 8.5.1

Microsoft

Windows 2000 server SP4
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed

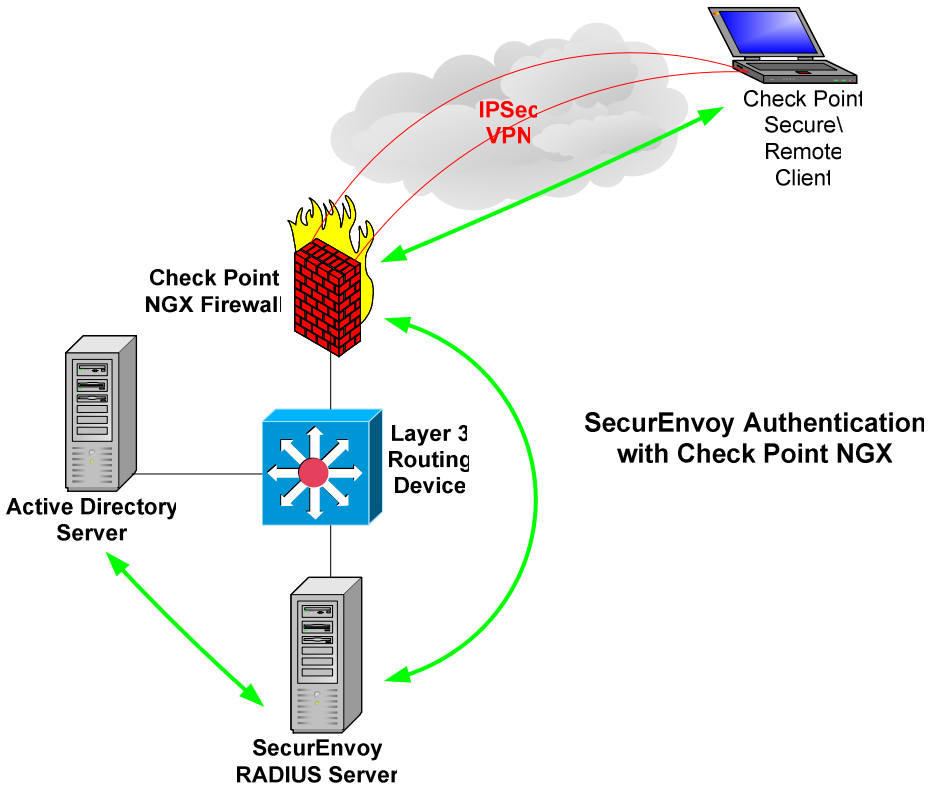
SecurEnvoy

SecurAccess software release v2.7 0100

SecurEnvoy SecurAccess Server and Check Point NGX (VPN Client –Secure Remote)

The integration guide explains how to authenticate Remote Access VPN clients against SecurEnvoy authentication server. The Radius component of SecurEnvoy takes the authentication request from the Checkpoint firewall; it is then passed to the SecurEnvoy authentication server which in real time retrieves user account and encrypted passcode data from Microsoft's active directory. All configuration and testing was completed within a test environment.

The deployment and topology design is outlined below.



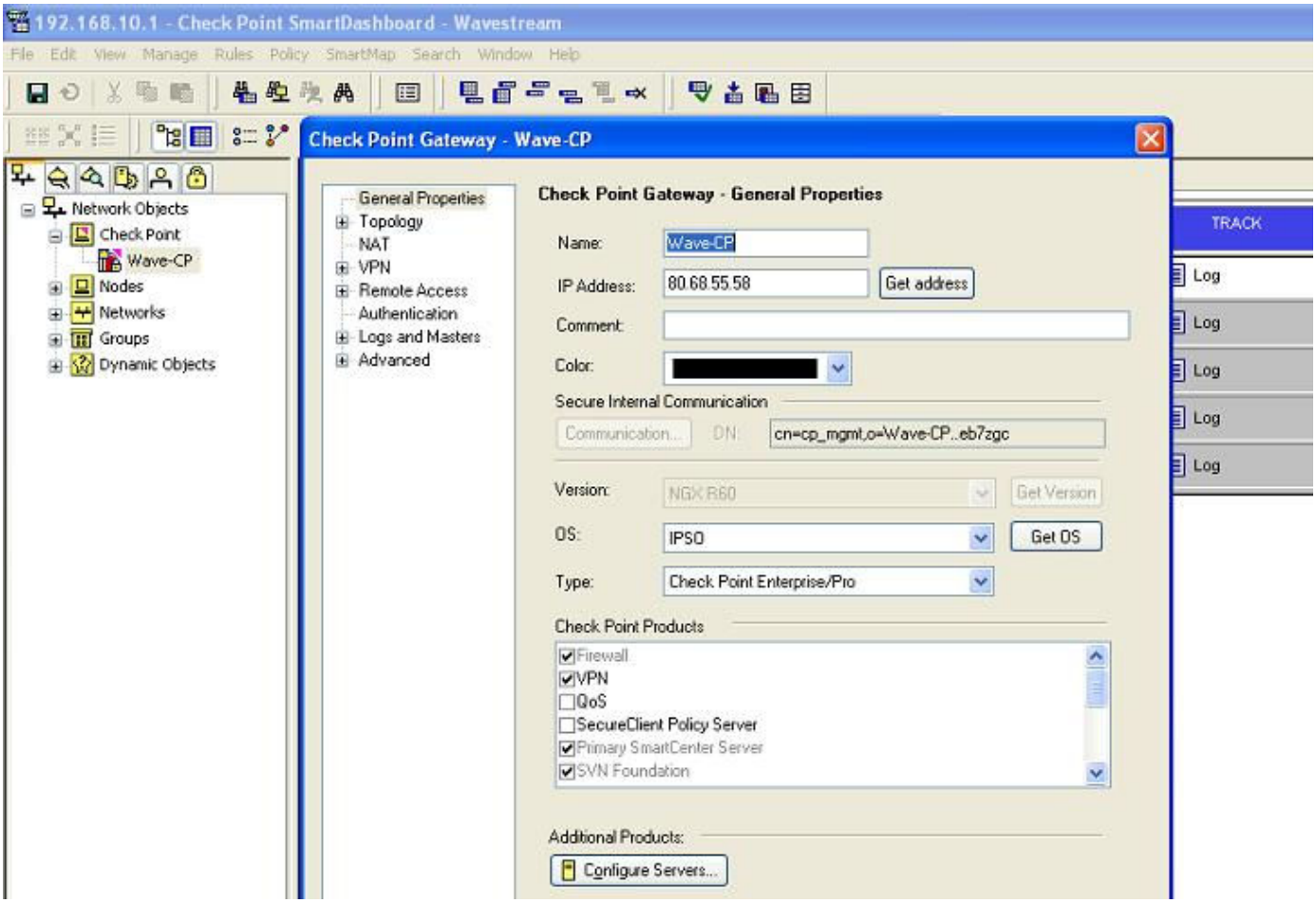
A Check Point Remote Access VPN client was setup and tested using static passwords. This was to facilitate the changes that would be required if deploying SecurEnvoy authentication from an existing traditional password model. These tests were carried out using Check Point NGX Enterprise/Pro with VPN, running on the latest version of IPSO, configured on a Nokia IP 380 Platform.
The SecurEnvoy SecurAccess server was installed on a fully patched, Windows 2000 Server, acting as both the authentication server and a RADIUS server.

Verify that the Check Point firewall is currently VPN "Enabled"; this is accomplished by checking that the VPN module is installed. Launch the Checkpoint management interface.
Go to "Network Objects"

"Check Point" and selecting the Checkpoint firewall you wish to configure.

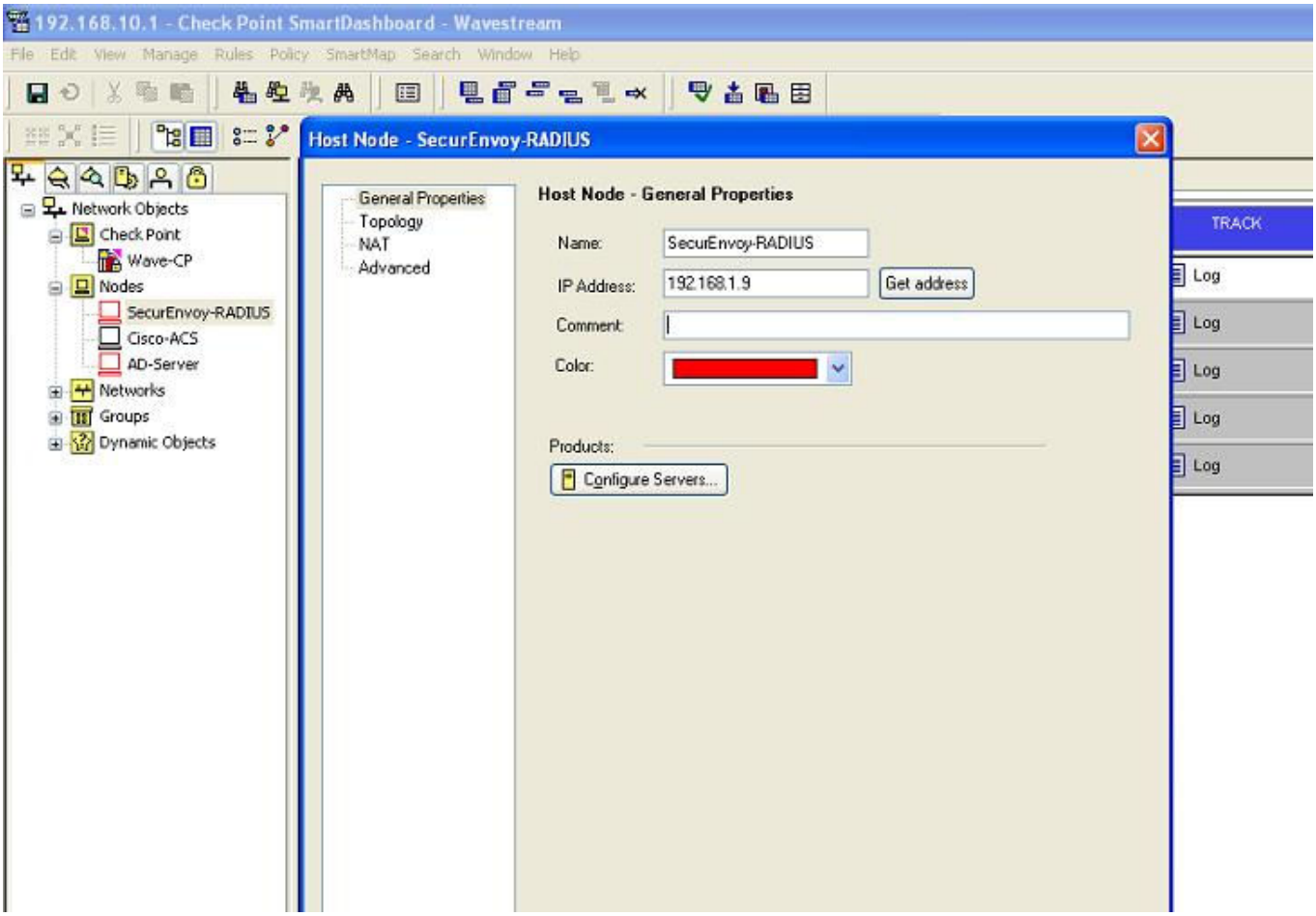
"Properties"

The VPN check box should be enabled.



The next step is to add the SecurEnvoy RADIUS Server as a host object, define it as a valid machine on the network.

Go to "Network Objects"
"Right-Click" Node → New node to add.
Populate the required information.
See diagram below.

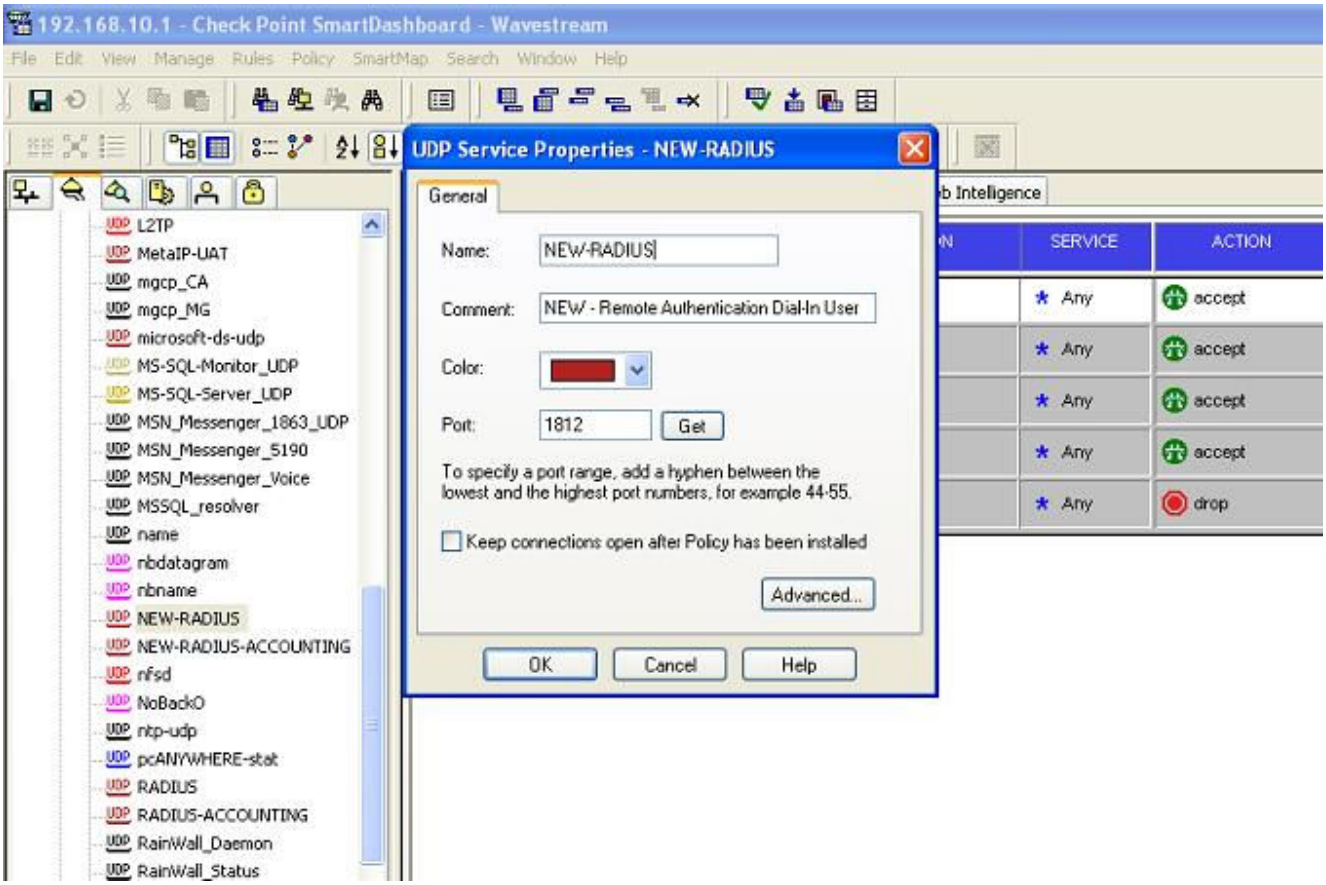


Click "ok" and "Save" to complete.

Check that the Check Point firewall uses the correct RADIUS Protocol details for communication between itself and the SecurEnvoy RADIUS Server.

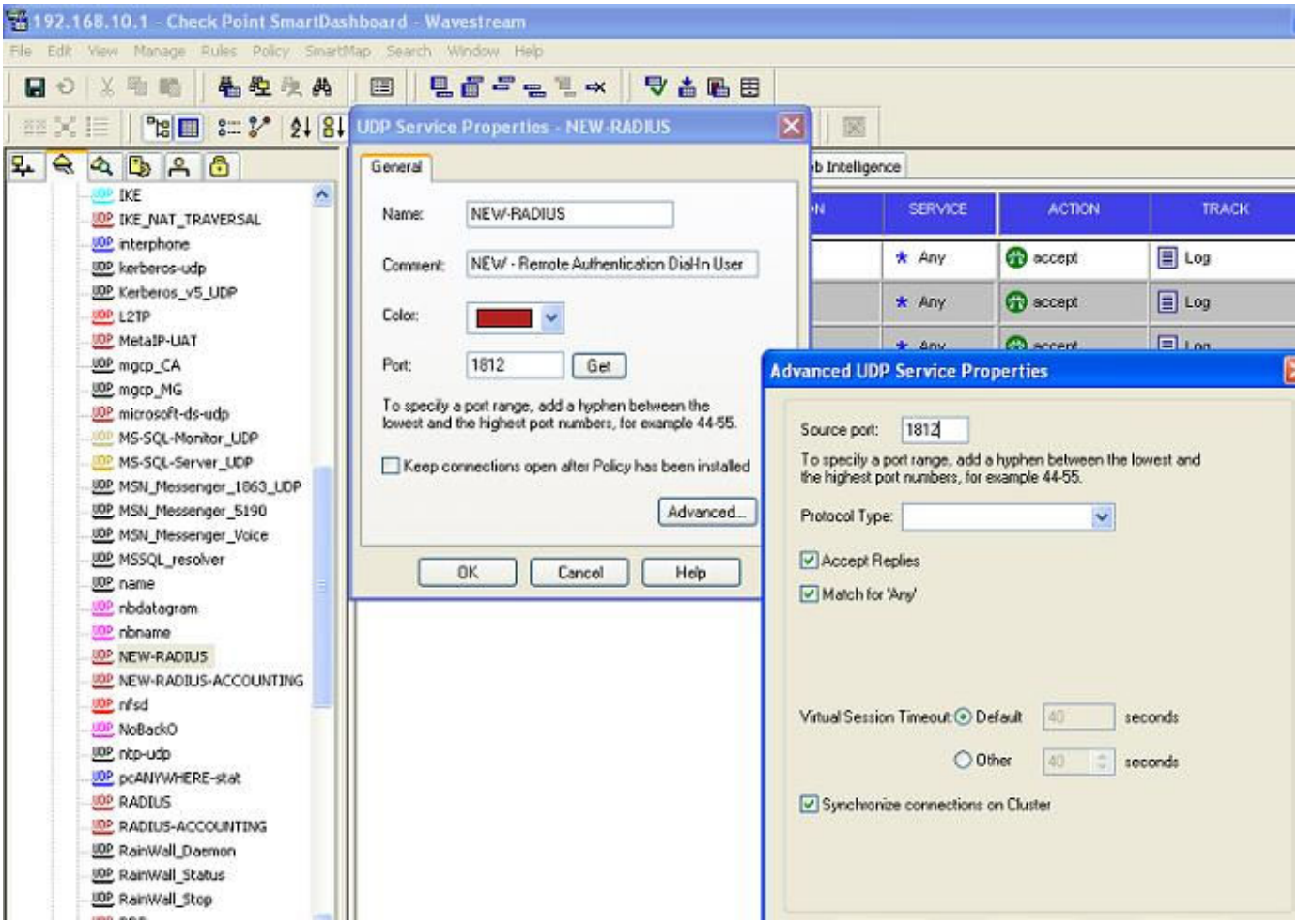
The SecurEnvoy RADIUS Server is configured by default to communicate on Port 1812, using Protocol UDP. It can be configured to use another port by running "regedit" on the SecurEnvoy server.
Go to "HKLM\SOFTWARE\SecurEnvoy\Radius Server select port and change this port to reflect your network design, typically this will be port 1645 UDP. Stop and restart the SecurEnvoy Radius service to make the new changes valid.

Under the "Services" tab, select "UDP" as the Protocol type, and browse to "New-RADIUS".
On the properties of "New-RADIUS", make sure that it is set to "Port 1812".
See diagram below.



Select the "Advanced…" tab and make sure that the Source port is set to "1812". Also make sure that the "Accept Replies" check-box has been enabled.
See the following diagram.

Advanced UDP Service properties

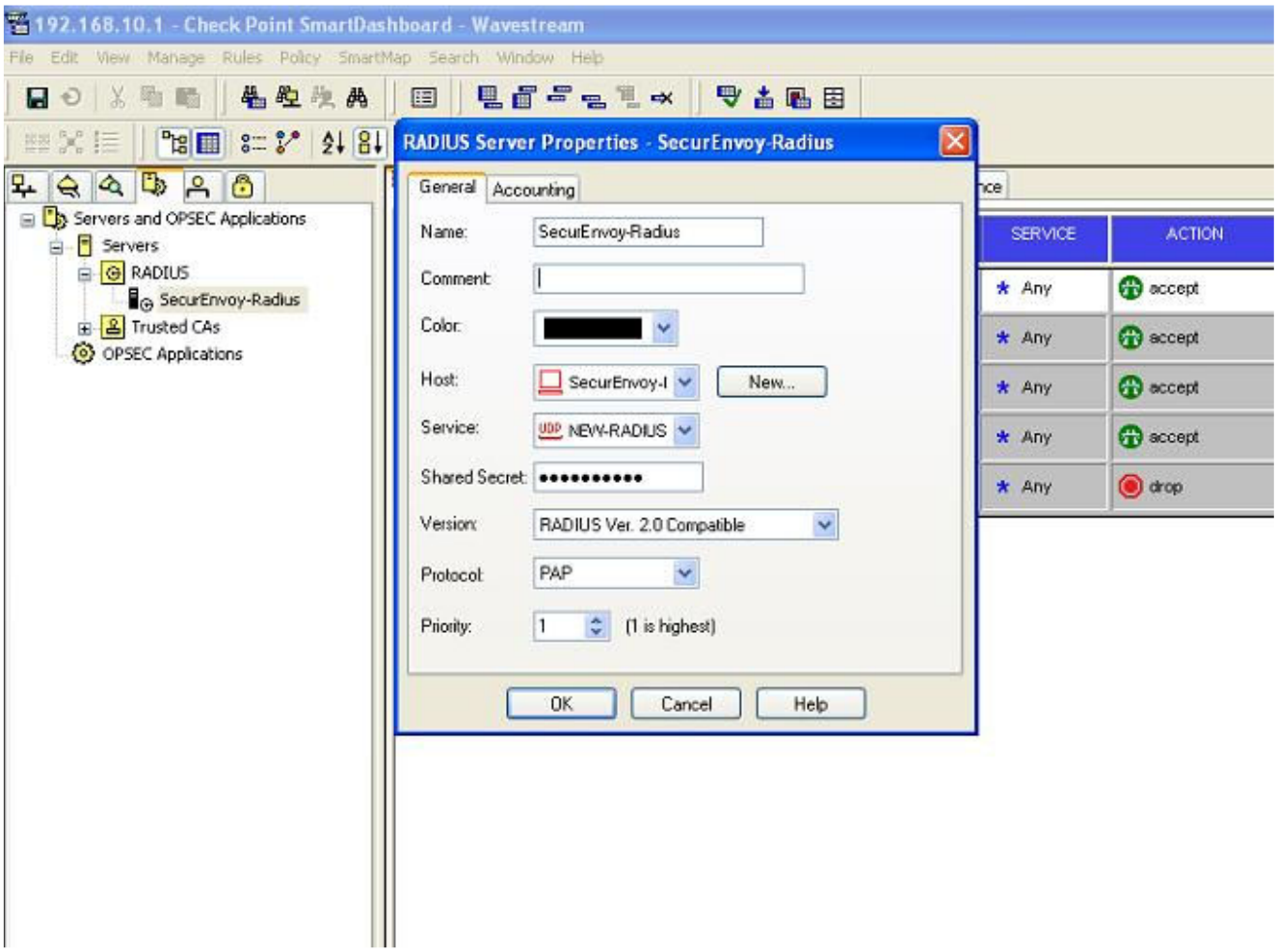


Select "ok" to save and "ok" again to exit. Then select "Save".

Now specify the specific SecurEnvoy RADIUS server and the details regarding version and protocol types supported.

Under the "Servers and OPSEC Applications" tab,
select "Radius" → New RADIUS… and then add in the new RADIUS server details.
Select the "SecurEnvoy-Radius" host you created earlier, set the Service type to use "udp NEW-RADIUS", and specify the common "Shared Secret" key to be used.
(The "Share Secret" key is configured on both the Check Point firewall and SecurEnvoy RADIUS Server). Make sure the Protocol type is set to "PAP".

Radius Server Properties

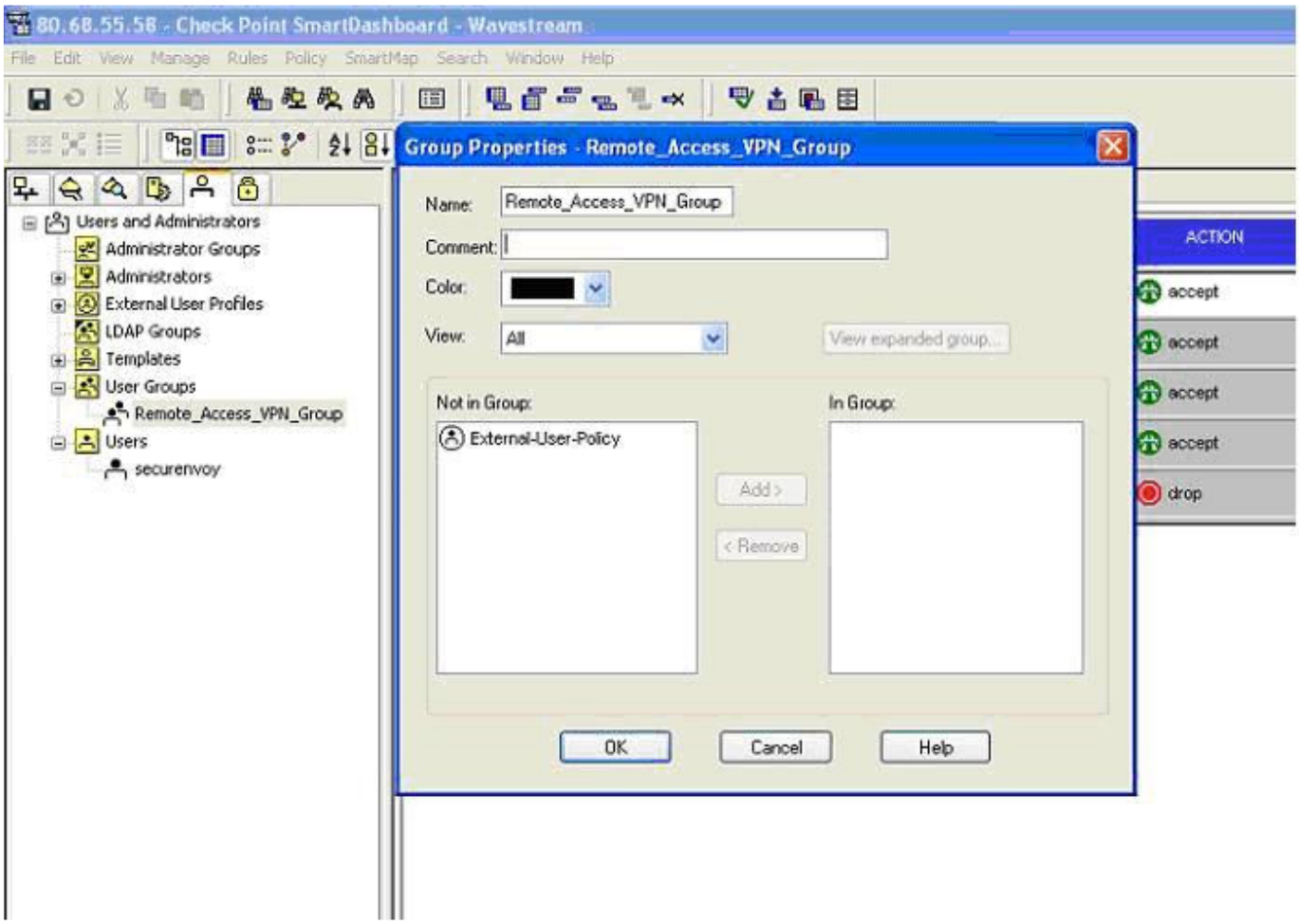


Select "ok" and then "Save" to complete.

From the "Users and Administrators" tab, "Right-Click"
"User Groups" → New User Group…
create a "Remote_Access_VPN_Group" for external users.

This group is used as a Global Authentication Group for "Check Point Secure/Remote Client" Remote Access VPN users.
See following diagram

Group Properties_VPN_Group



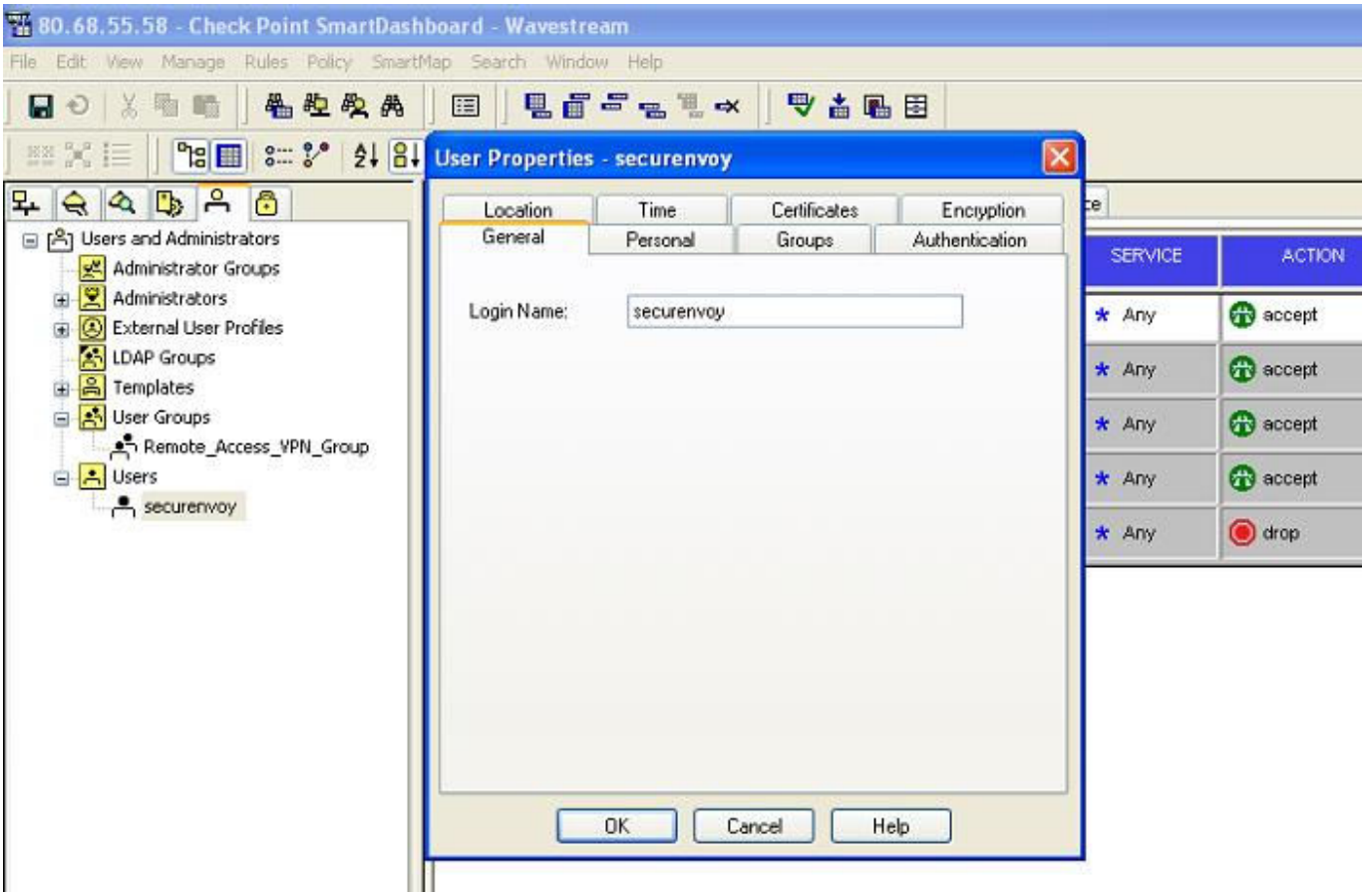
Select "ok" and "Save" to complete.

There are many ways of setting up VPN users in Check Point NGX. In this example, we are going to create a local user account, add it to the "Remote_Access_VPN_Group", and set it to authenticate against the external "SecurEnvoy-Radius" server.

Select "Users" → New User…

Create a VPN user account "securenvoy", which we can then associate with the "Remote Access VPN Group". Set the "Login name" details for the user.

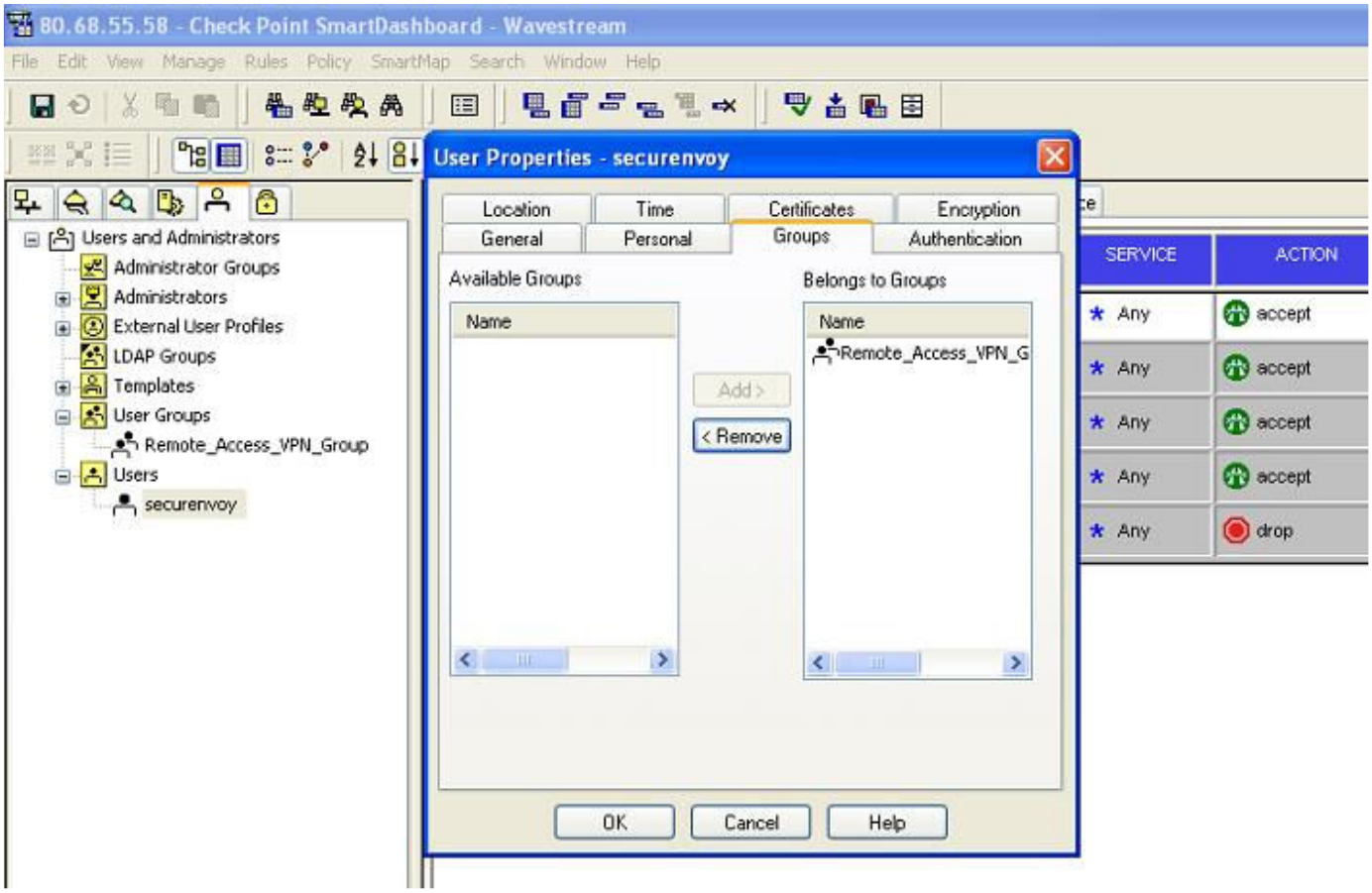
Typically this would be the same as the Active-Directory Domain user account.



On the "Groups" tab,

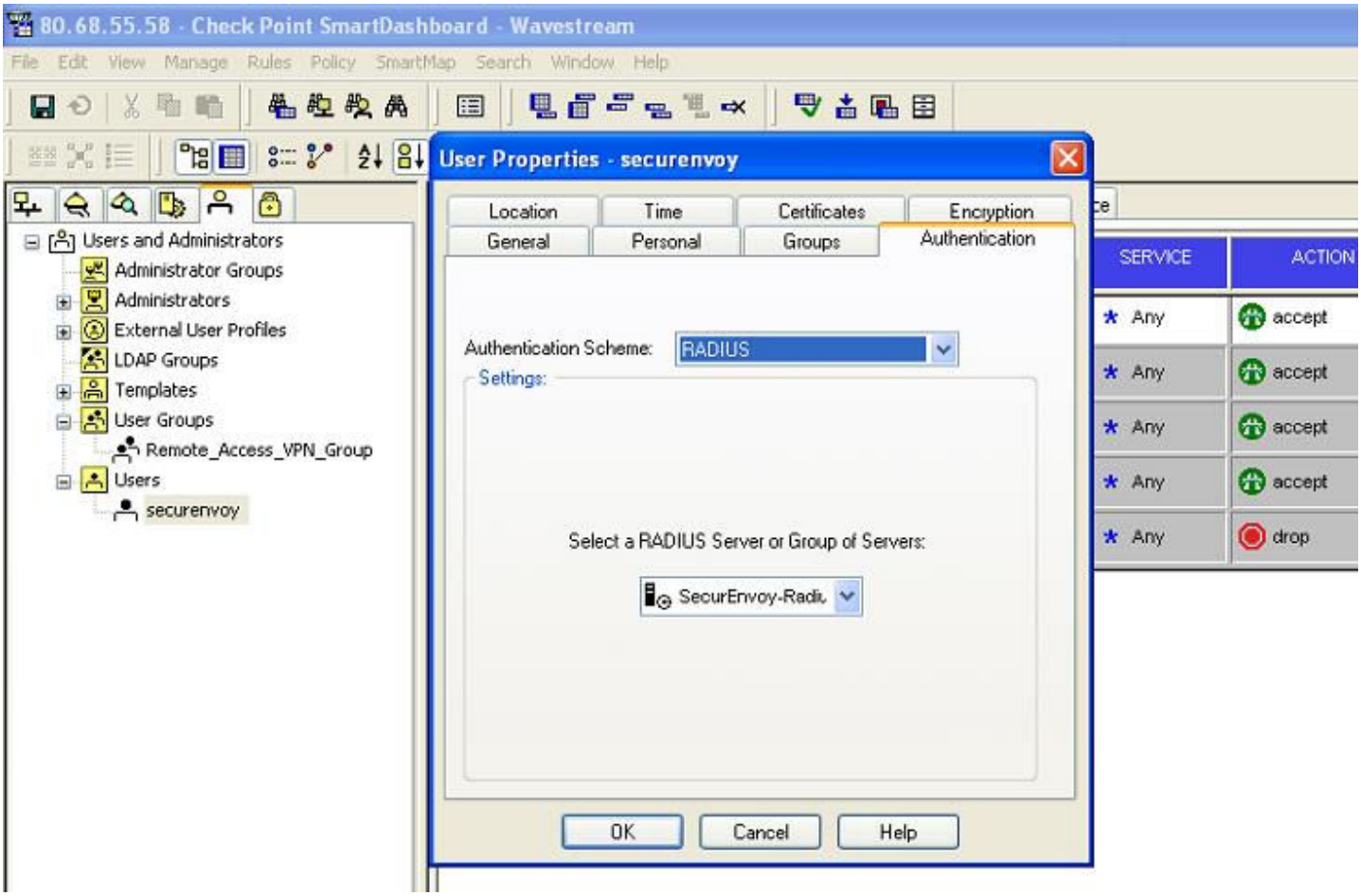
Select the "Remote_Access_VPN_Group"

As the group you want the account to become a member of.



On the "Authentication" tab,

set the Authentication Scheme to "RADIUS" and below that select the RADIUS Server "SecurEnvoy" as the chosen RADIUS Authenticator for this user.



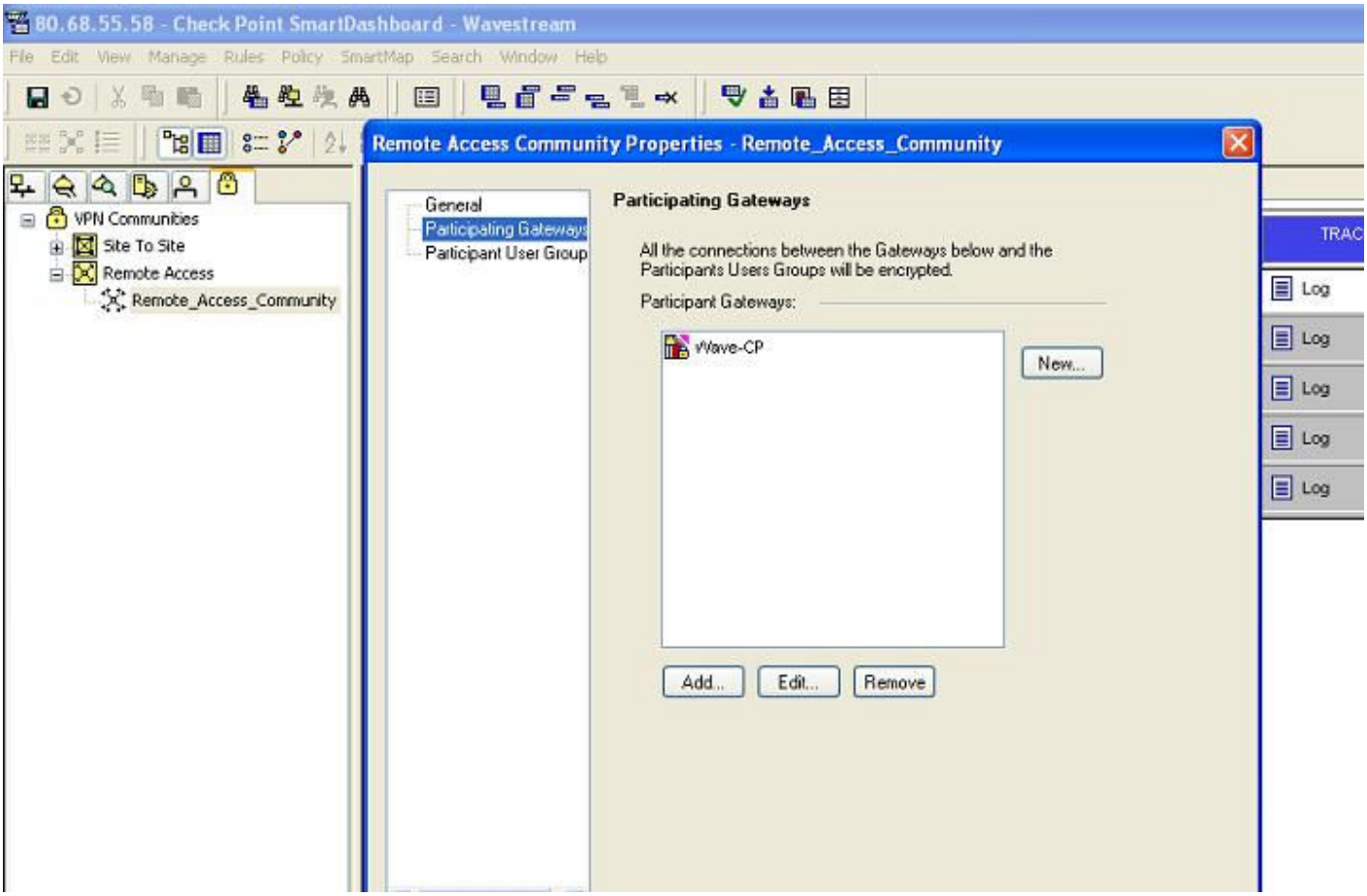
Select "ok" and then "Save" to complete.

Select the "VPN Communities" tab,

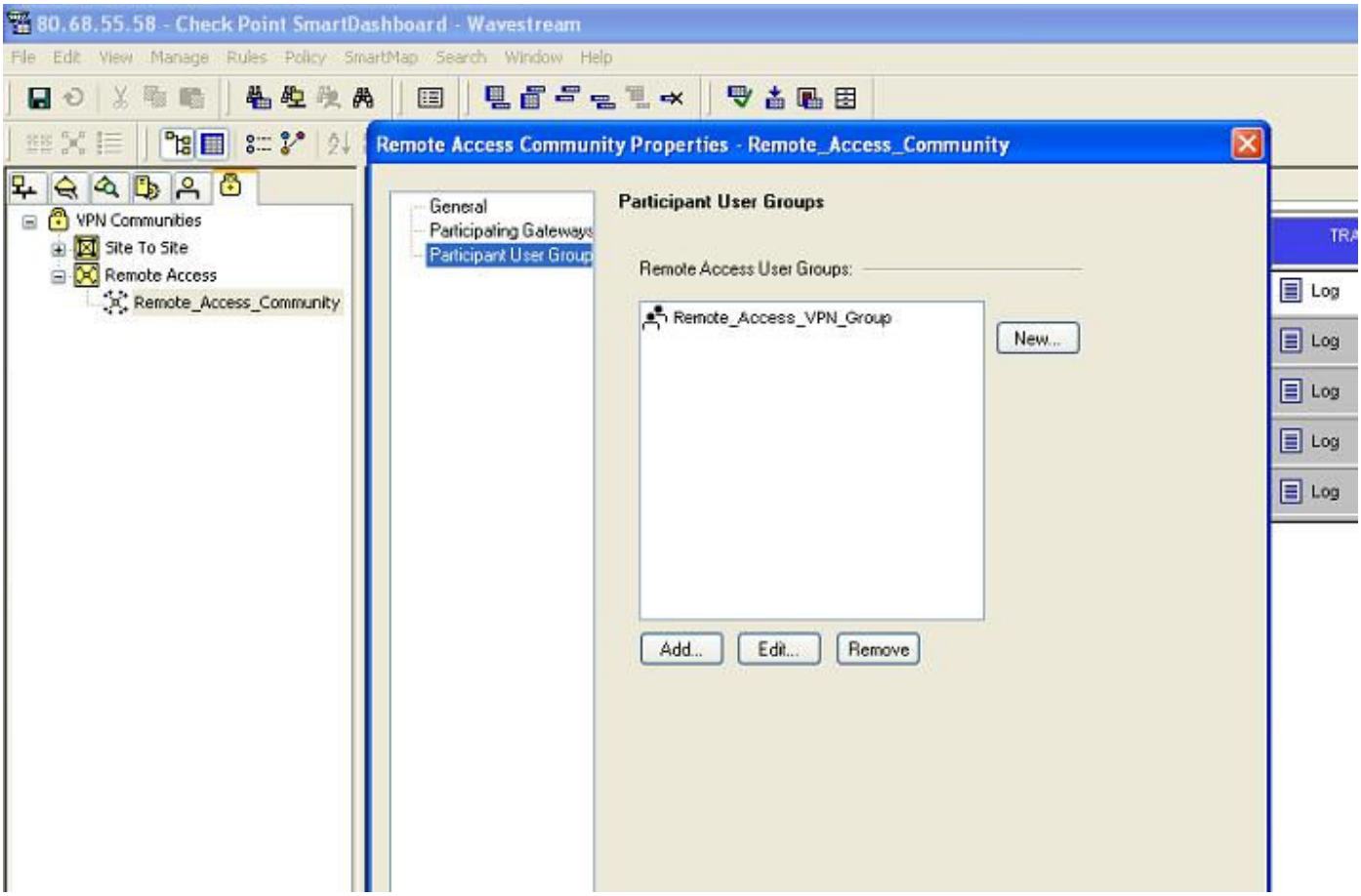
Then "Right-Click" Remote Access,

→ New Remote Access Community, and configure.

On the "Participating Gateways" tab, select your Check Point NGX node.

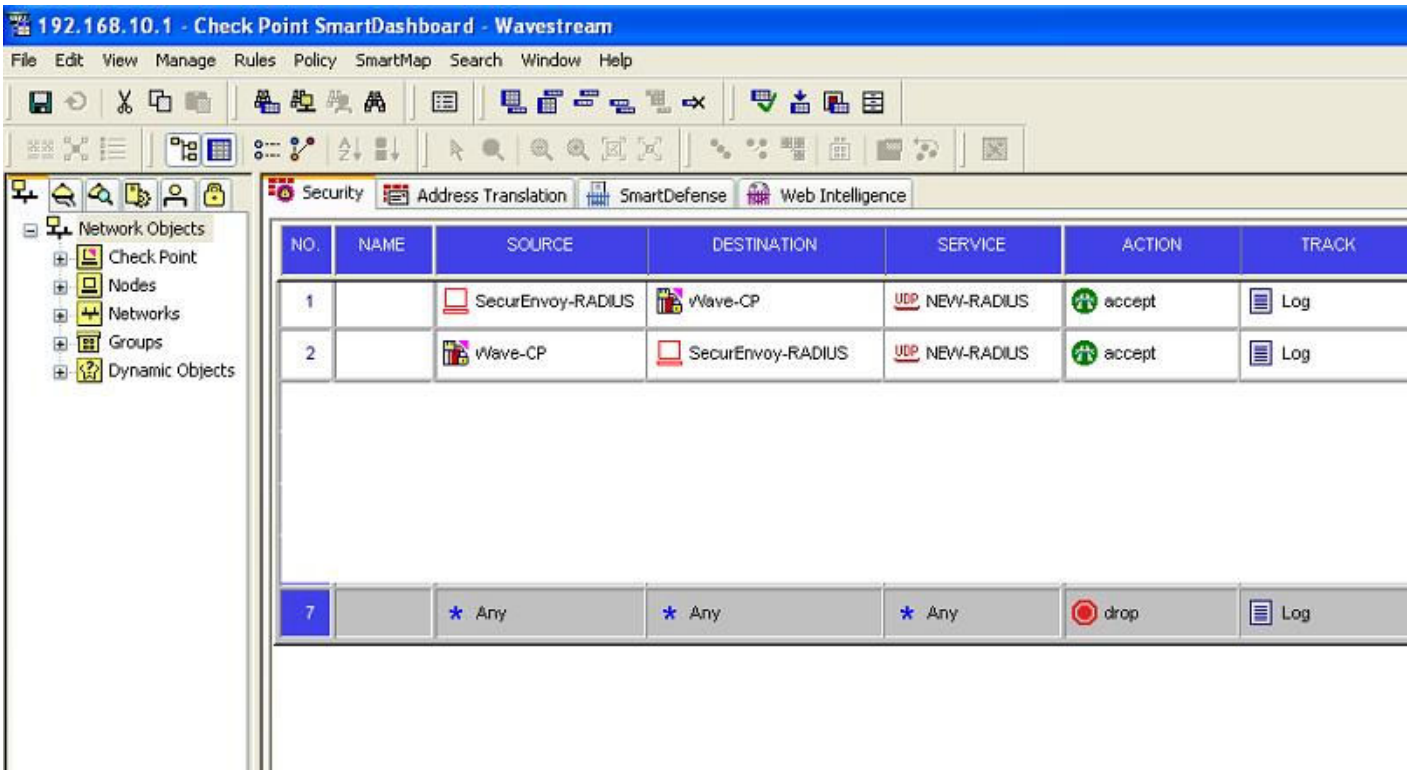


Then, on the “Participating User Groups”, select the “Remote_Access_VPN_Group” you created earlier, And add this group into the Check Point “VPN Communities” properties.



Select “ok” and “Save” to complete.

Depending on your current Check Point firewall rule-base configuration, you may need to add in a rule "Permitting" "NEW-RADIUS" communication between the "SecurEnvoy-RADIUS" server and the Check Point NGX firewall.

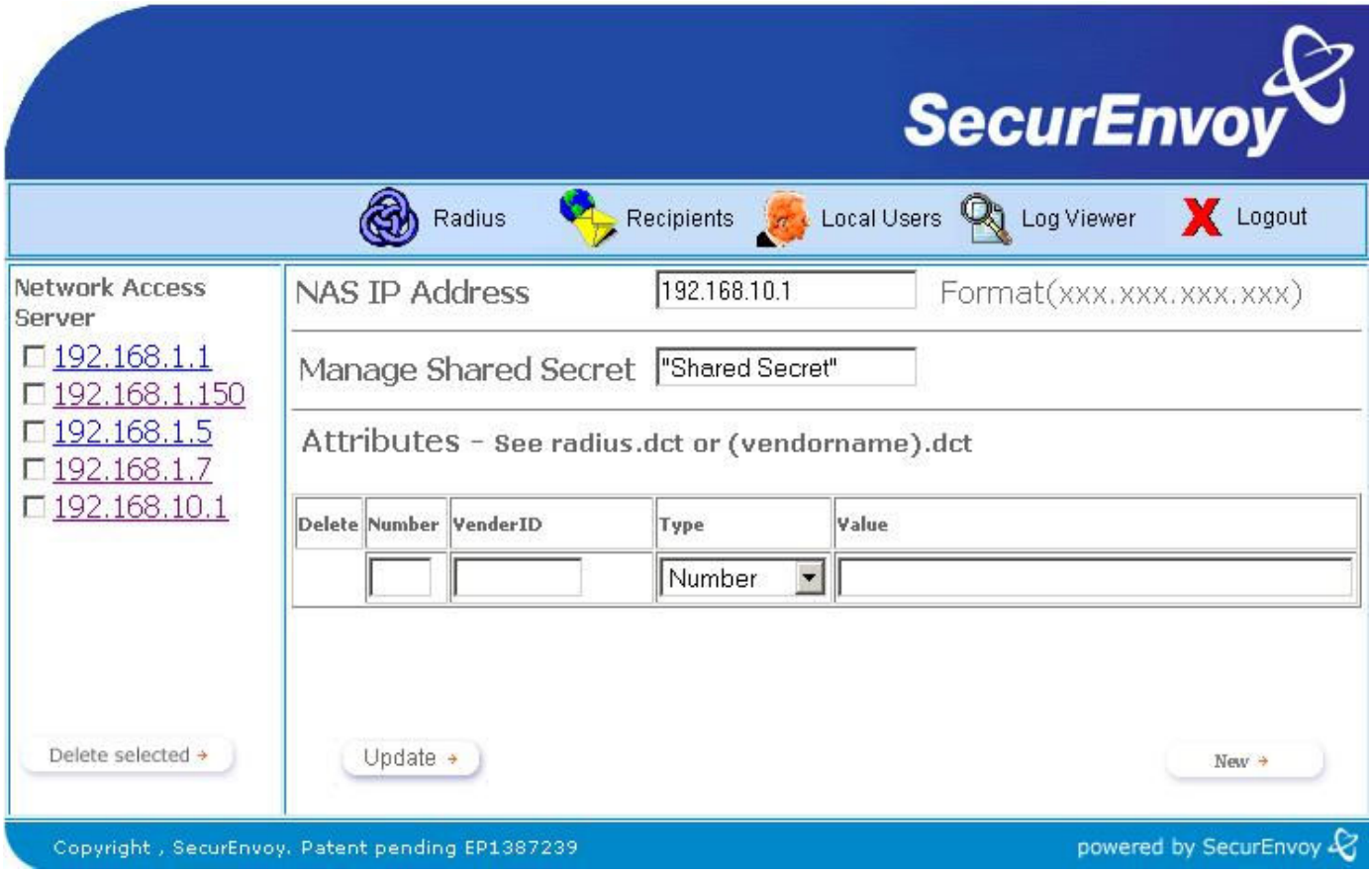


Once the above details have been configured, and the policy has been saved, it can be pushed to the relevant Check Point Enforcement Modules.

Next step is to configure the Check Point NGX Firewall as an "Agent" RADIUS Server within the SecurEnvoy Administration interface.

Launch the SecurEnvoy Admin GUI, from the shortcut or remote web admin connection. Once logged-in to the SecurEnvoy Admin GUI,

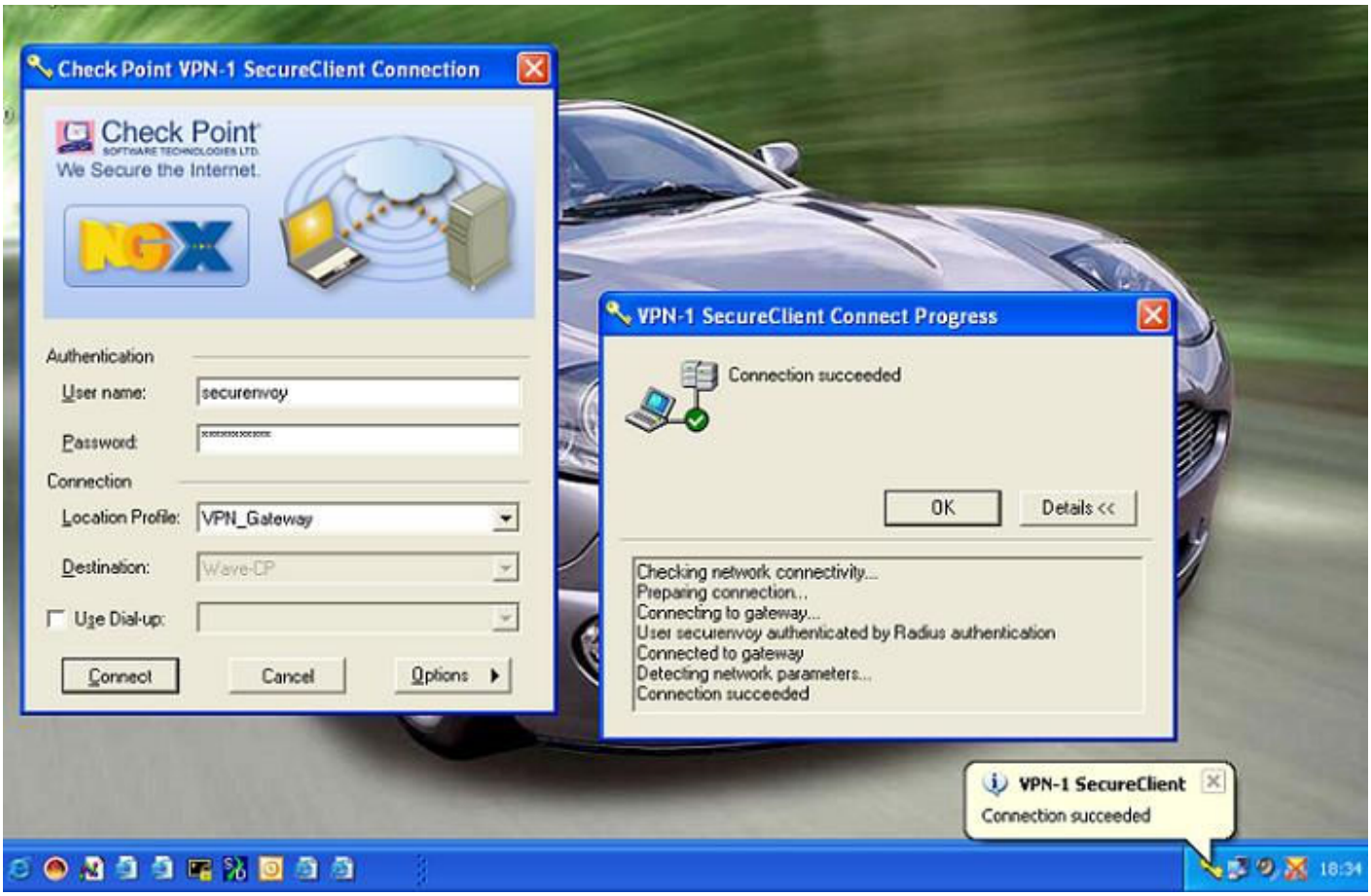
Select "RADIUS", and then enter in the details of the Check Point Firewall, including the "Shared Secret" key, which is identical on both the Check Point Firewall, and the SecurEnvoy RADIUS Server itself.



Select "Update" to complete the changes.

Test the RADIUS Authentication setup against SecurEnvoy by connecting to the Check Point NGX Gateway using the Check Point Secure/Remote VPN client installed on a Company Laptop of a Remote User.

Begin by starting up your NGX VPN client. Then supply the correct credentials for your login.



The "securenvoy" user credentials have been successfully passed against our internal RADIUS server,
And the VPN connection is setup, allowing me local access to the internal company network.