External Authentication with Netscreen 25

Remote VPN

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

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

Juniper Remote Access VPN provides - Secure Remote Access to corporate network resources for all Client/Server applications.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Juniper Remote Access VPN), 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.

Juniper Remote Access 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 Juniper Remote Access VPN was configured. All authentication requests were forwarded to SecurEnvoy Authentication server. Both Juniper 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

Juniper

Netscreen Firewall VPN
Hardware Version: 4010(0)
Firmware Version: 5.1.0r3.0 (Firewall+VPN)

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

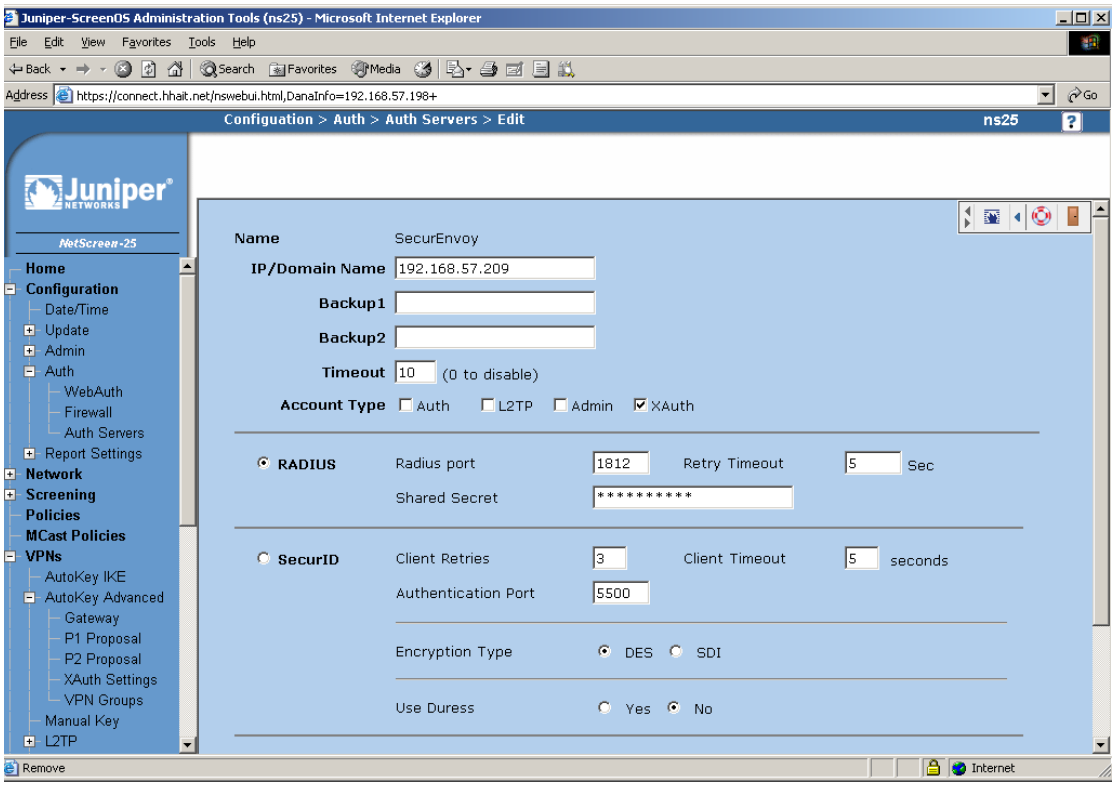
Log into the Juniper Networks Netscreen-25 Administrator Console. The administrator console can be reached via a web browser

In the Administrator Console, choose Configuration/Auth/Auth Server, click on new server.

Populate the fields to reflect the network setup.
The "Name" is a label used in the Juniper Networks Netscreen Firewall to refer to the SecurEnvoy Authentication server. It is NOT the name associated with a DNS entry. The "IP/Domain Name" should be either the IP address or the FQDN of the SecurEnvoy Server.

Select "Timeout" and enter a value of at least 10 seconds, set the account type to XAuth.

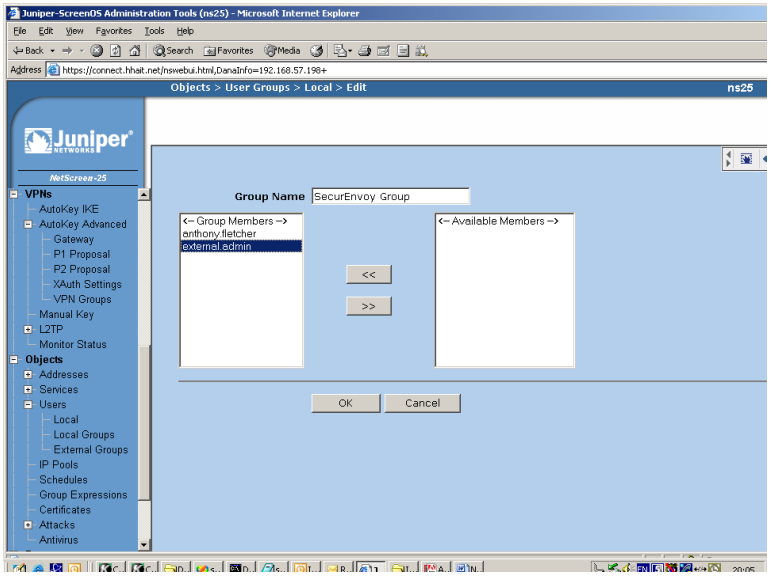
Select "Radius" and enter port and Pre-Shared key values, these values must be reflected within the configuration of the SecurEnvoy Radius settings (shown later).



Create a User Group and create Users who will have VPN access with SecurEnvoy authentication.

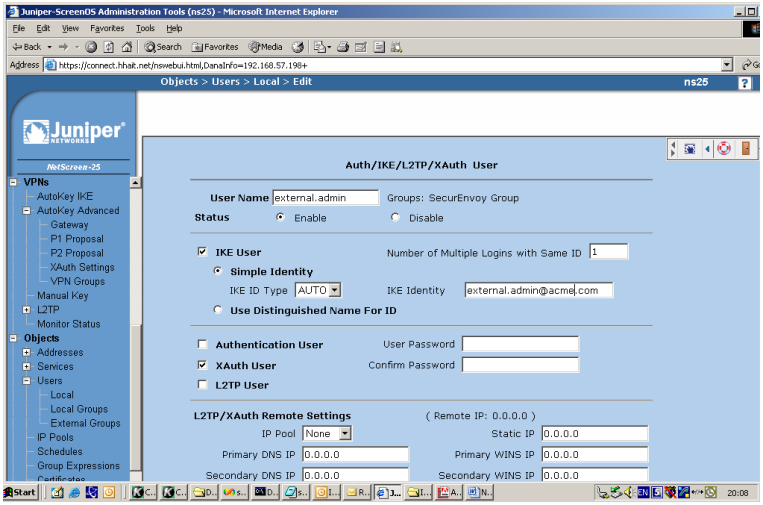
Go to Objects/User Groups/Local

Create a group Called SecurEnvoy Group and select members to be added to this group. Click Ok when completed.



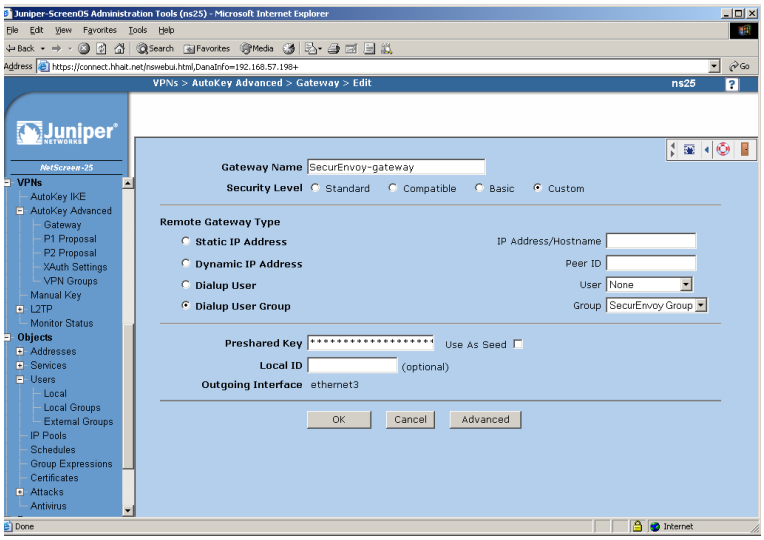
Note: Users must be create before they can be added to the User Group

Go to Objects/Users/Local
Create new user, enable and select them as an IKE user, populate which mechanism they will use for IKE identity.

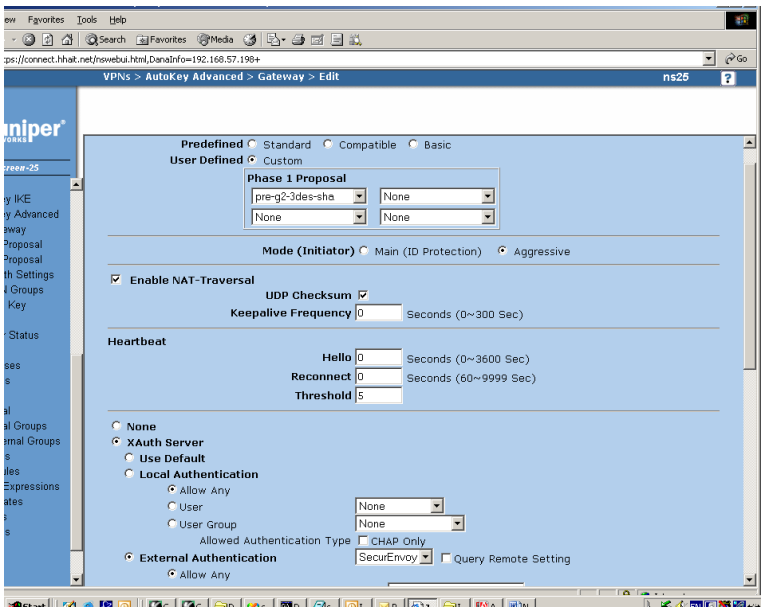


Click Ok when completed.

Establish the VPN settings
Go to VPN's/Auto Key Advanced/Gateway
Create a new VPN gateway enter SecurEnvoy Gateway as the name for this new entry select "custom" security level, select "dial-up user group" and select the group you defined earlier in the drop-down box "SecurEnvoy Group". Populate the pre-shred key for Phase 1 VPN configuration. This must match on both the VPN client and Netscreen 25. Then click on the Advanced button.



Continue building the VPN Gateway under "Advanced" by clicking on "user Defined" and selecting a series of Phase 1 Proposals. Check the Enable Xauth box. Select the External Authentication radio button and select the name given to your SecurEnvoy Server.

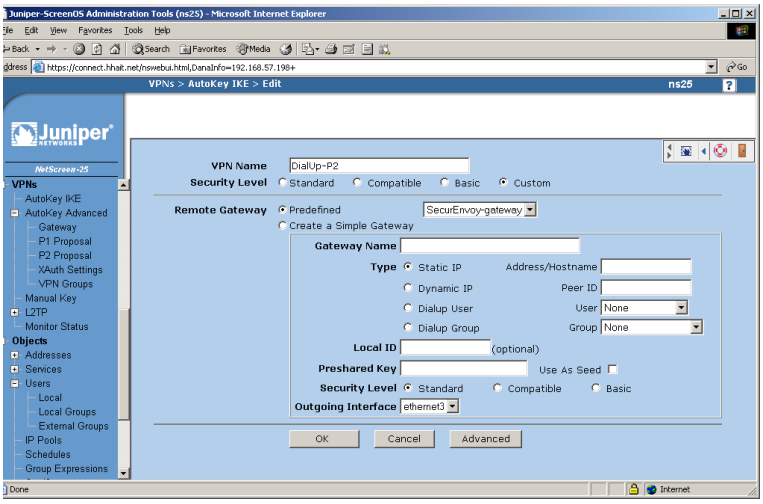


Click the "Return" button and then the "OK" button to conclude building the Gateway

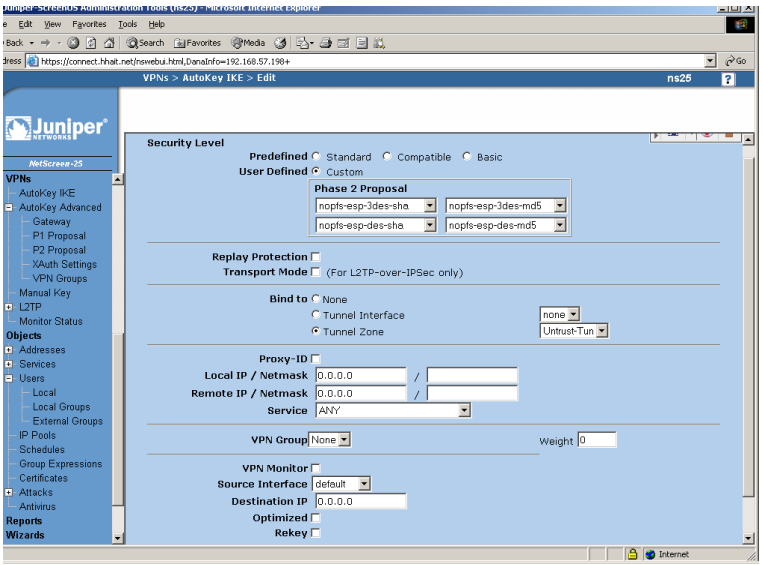
Continue with the VPN Setup

Go to VPN/AutoKey IKE.

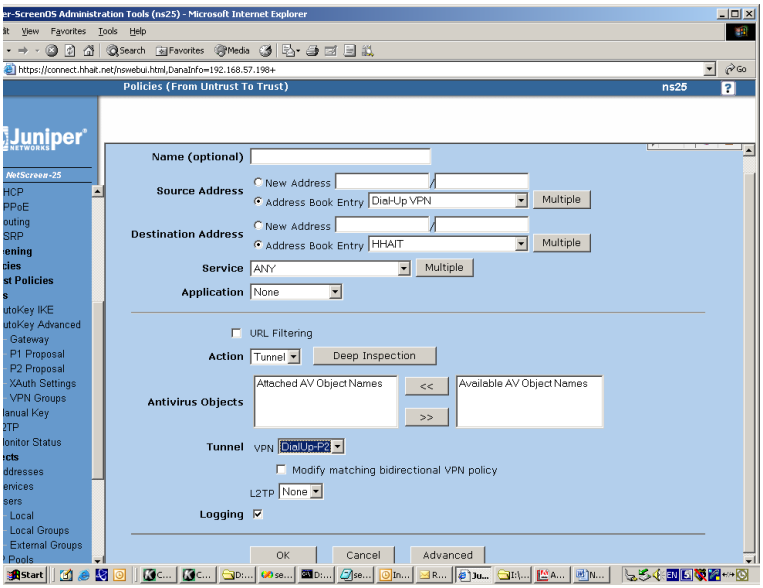
Click on the "New" button. Define a new VPN here by giving it a name, select "custom" for the security level, and choose Predefined for the Remote Gateway. Then select the gateway you just defined from the drop-down box "SecurEnvoy Gateway. Click on the "Advanced" button.



Continue defining the VPN under "Advanced" by defining a Phase 2 proposal. Select Tunnel Zone within the Bind to field.

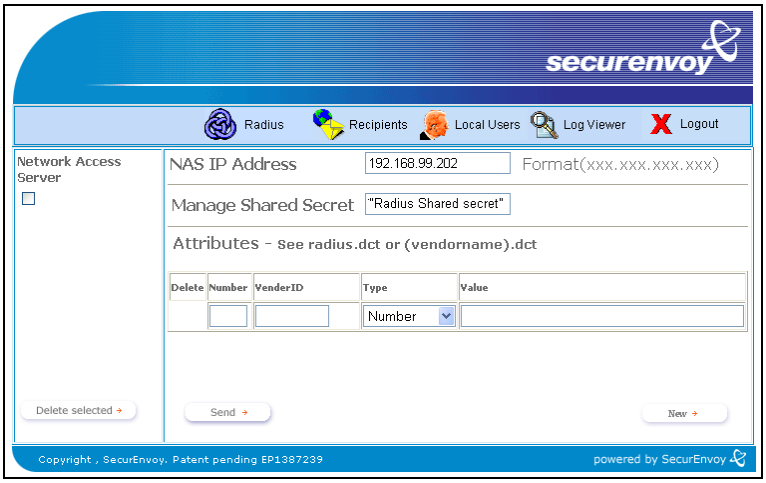


Create a Policy from Untrust to Trust. The source will be from the address book entry "Dial-Up VPN" and the Destination will be the trusted network. Under Action, choose tunnel. For the tunnel, chose the tunnel you defined in the prior step.



Click Ok when complete.

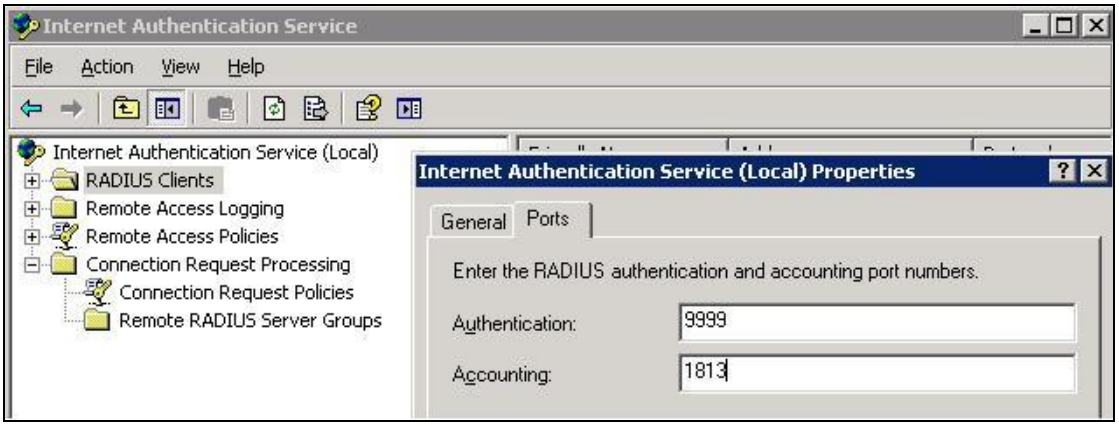
To set up Radius on SecurEnvoy SecurAccess, launch local Security Server Administration
Select Radius
Enter NAS IP address
Enter "Radius Shared Secret"
Click Send



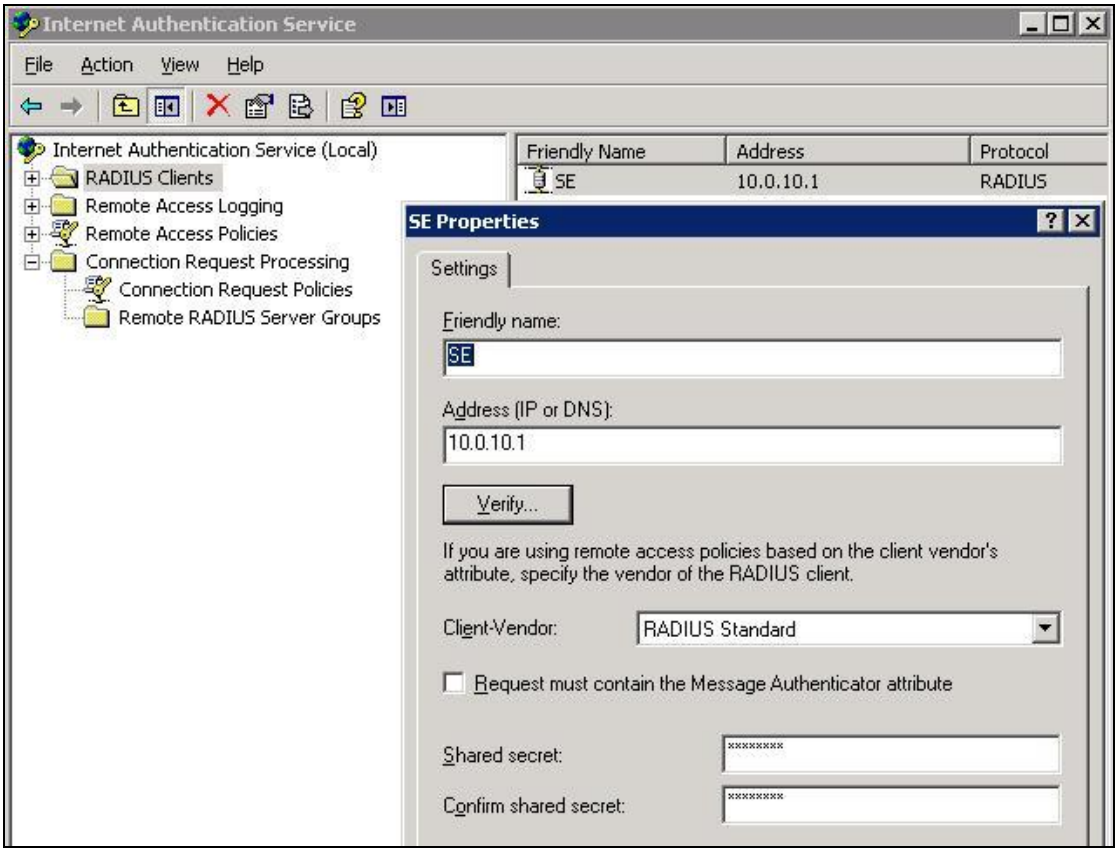
NOTE: Netscreen VPN requires a RADIUS accounting server or it will fail authentication! A Microsoft IAS service must be installed to act at the RADIUS accounting only.

Install Microsoft IAS, this is a windows service on Microsoft Windows 2000 and 2003 server. This has to be installed on the same server as the SecurEnvoy SecurAccess server.

Set up the IAS server so that the authentication port is an unused port as this service is not required, keep the accountancy port set to default.



Create a new Radius client entry for the Netscreen VPN Firewall, the Radius shared secret will be the same as the Radius shared secret for the SecurEnvoy Radius server.



Therefore the Radius authentication request will be answered by the SecurEnvoy server and the accountancy information will be logged by the Microsoft IAS server.

Test Authentication
Carry out a test authentication, launch VPN client Enter Username, Pin and Passcode into the relevant fields.