External Authentication with Cisco ASA

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	

Cisco ASA Integration Guide

This document describes how to integrate a Cisco ASA with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Cisco ASA provides Secure Remote Access and Firewalling to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cisco), 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 any LDAP server 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 in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilising the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seemless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, as does the Cisco ASA (ASDM). All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Cisco

Cisco ASA v7.2
Cisco VPN client software v5.0.02.0090

SecurEnvoy

Windows 2003 server SP1
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.2.503

© 2005 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites 3
1.1 Configuration of Cisco ASA 4
1.2 Configuration of Cisco ASA VPN configuration 4
2.0 Configuration of SecurEnvoy - PIN configuration 8
2.1 Configuration of SecurEnvoy - RADIUS configuration 8
3.0 Cisco VPN Client Configuration 9
4.0 Test logon 9
5.0 Troubleshooting RADIUS connection 10

1.0 Pre Requisites

It is assumed that the Cisco ASA has been installed and is authenticating VPN users with a username and password.

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Routing and Remote Access server(s), additional open ports will be required.

NOTE: *Add radius profiles for each Cisco ASA that requires Two-Factor Authentication.*

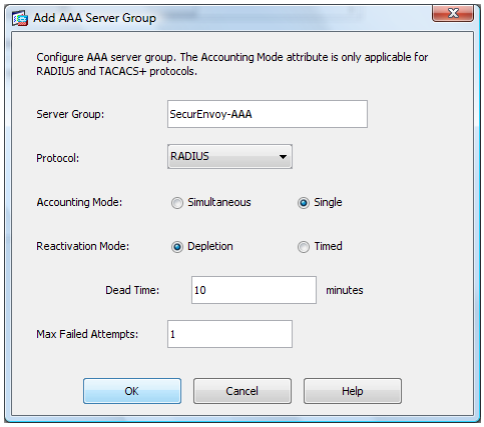
© 2005 SecurEnvoy Ltd. All rights reserved

1.1 Configuration of Cisco ASA

Launch the Cisco Adaptive Security Device Manager (ASDM), select Configuration in top toolbar, navigate to AAA setup, go to AAA server Groups and click ADD.

Enter name details and select the Radius protocol, set max failed attempts to 1.

Click Ok when completed.

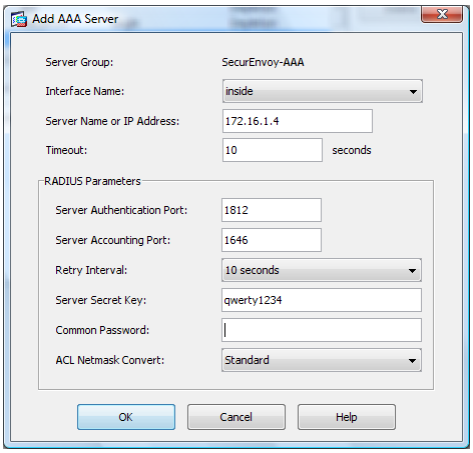


Navigate to AAA setup, go to AAA server and click ADD.

Enter details for interface, IP address of SecurEnvoy server. Set port to 1812 (this is the default port of SecurEnvoy Radius)

Enter Server Secret Key.

Click OK when completed.

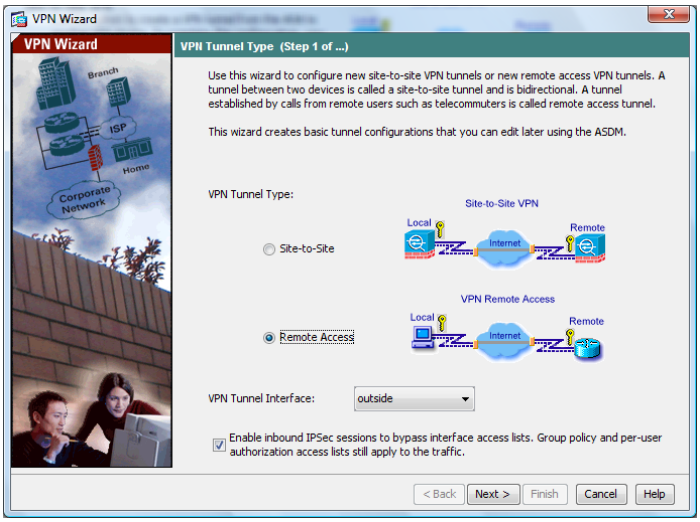


1.2 Configuration of Cisco ASA VPN configuration

Within the ASDM, navigate to the Feature pane (LHS) and select VPN and VPN wizard.

Select the interface you wish to have VPN services enabled upon.

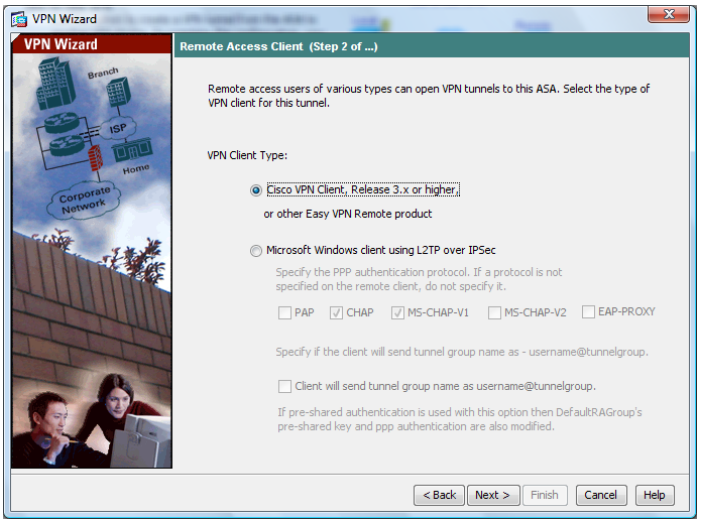
Click next.



© 2005 SecurEnvoy Ltd. All rights reserved

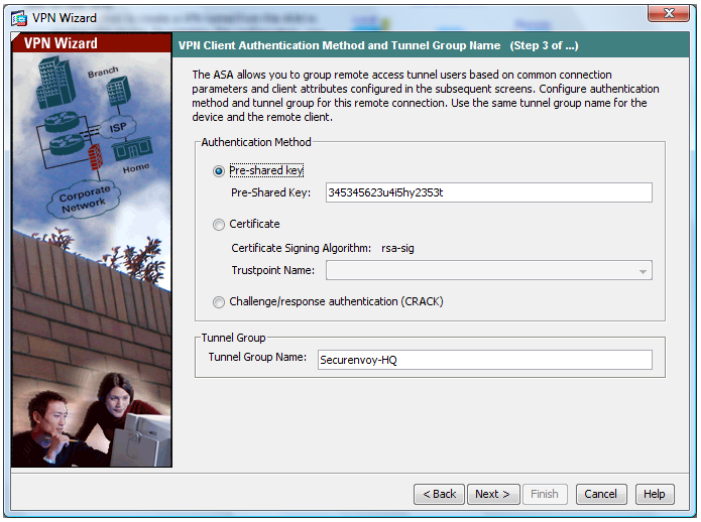
Select the VPN client software to be used. This example uses Cisco VPN client software.

Click next.



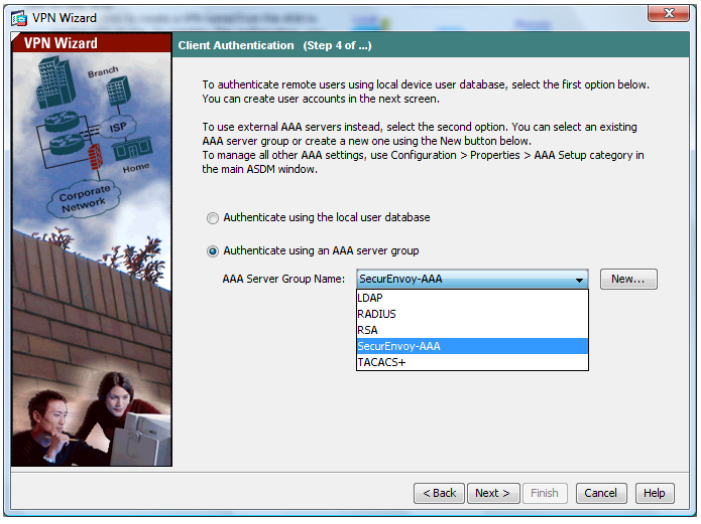
Select Pre-shared key and enter key information. This key will be required when configuring the VPN client.

Click next.



Select Authentication using AAA server group, select SecurEnvoy configured AAA server group.

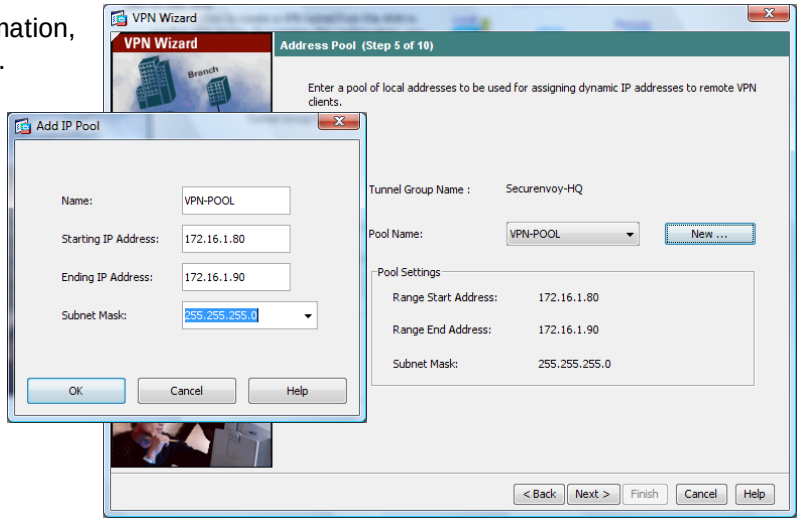
Click next.



© 2005 SecurEnvoy Ltd. All rights reserved

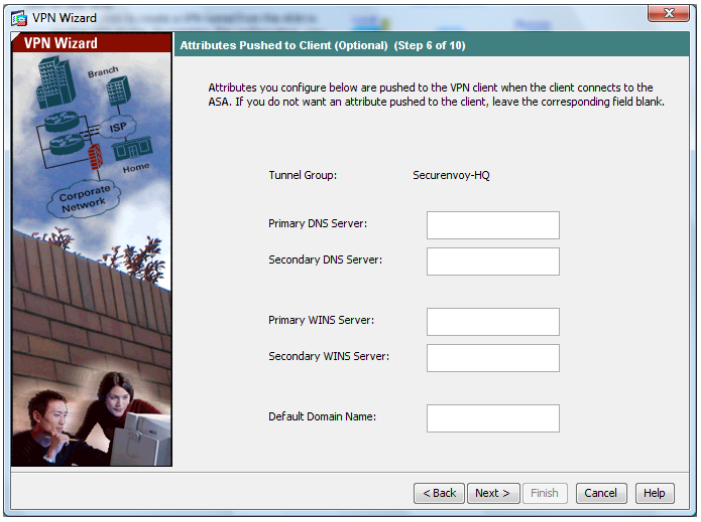
Select address pool information, add a new pool if required.

Click next.



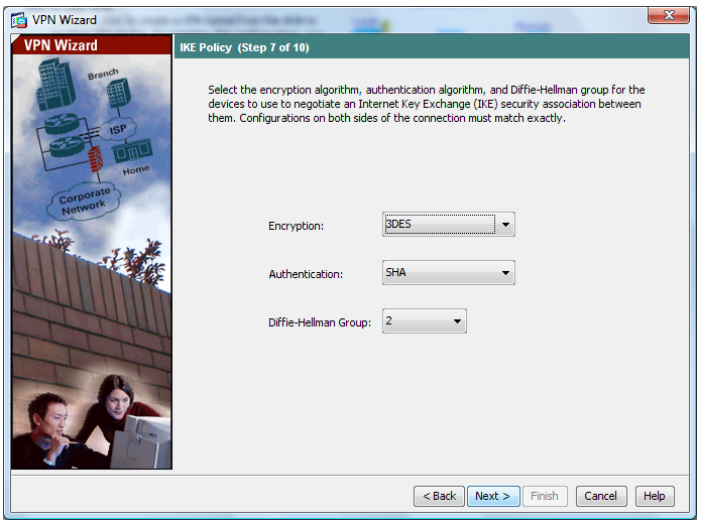
Enter IP information regarding DNS, WINS servers and default Domain.

Click next.



Select IKE policy information, this example used the default settings.

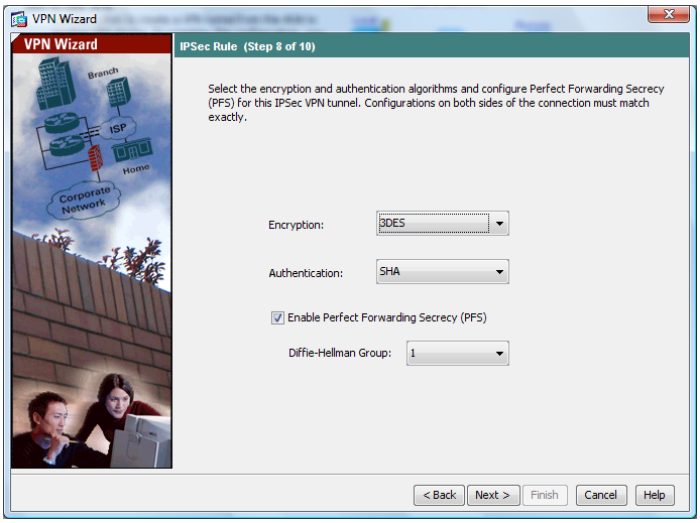
Click next.



© 2005 SecurEnvoy Ltd. All rights reserved

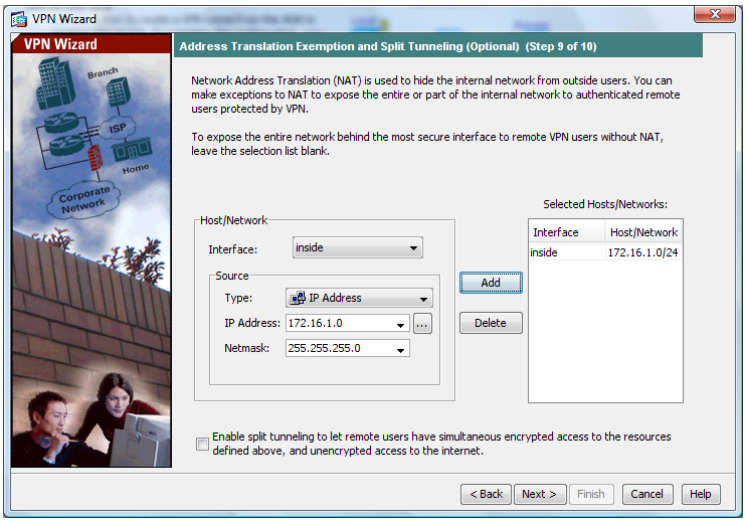
Enter details for the IPSec rule information. This example used the default settings

Click next.



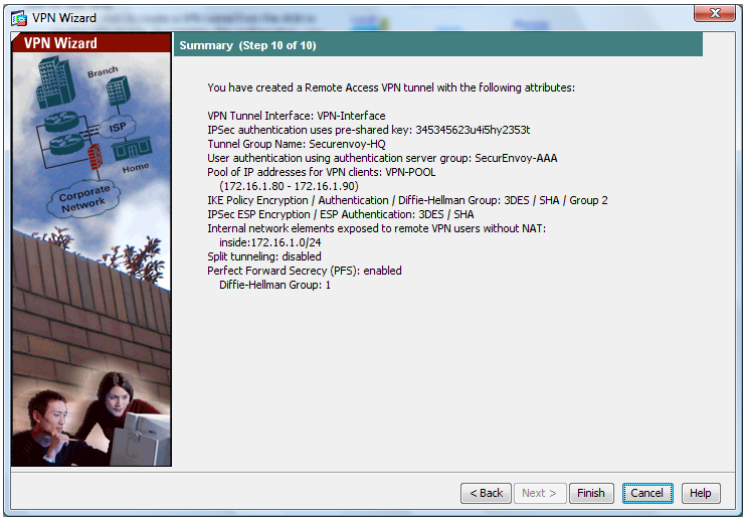
Enter details for NAT.

Click next.



Finalise settings.

Click next.



© 2005 SecurEnvoy Ltd. All rights reserved

2.0 Configuration of SecurEnvoy - PIN configuration

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing LDAP password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone via SMS.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click **"Config"**

Select **Windows** – Microsoft Password is the PIN under PIN Management

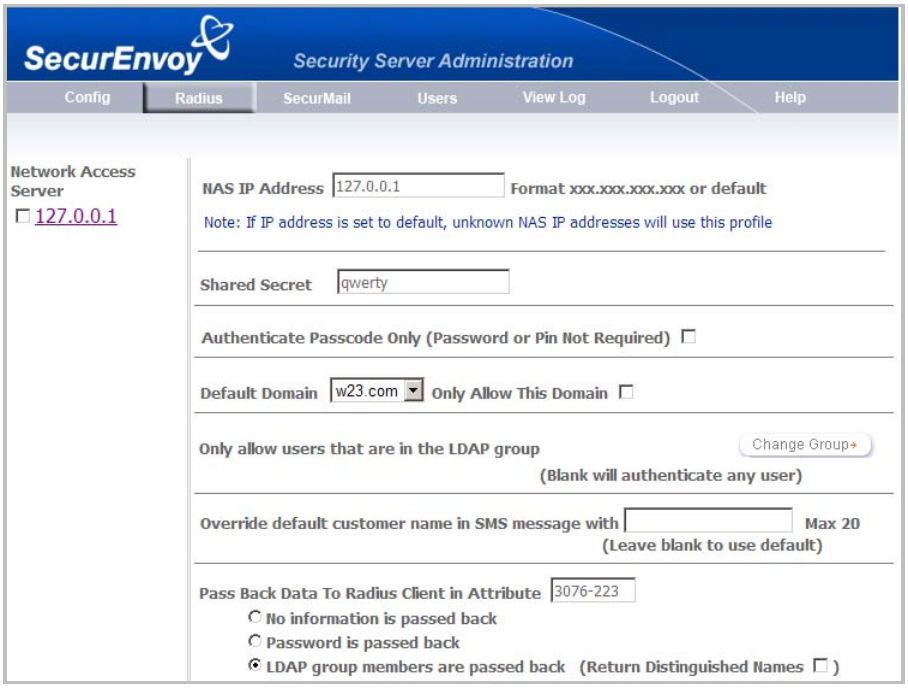
This will now use the users existing password as the PIN.

Click **"Update"** to confirm the changes

2.1 Configuration of SecurEnvoy - RADIUS configuration

Click the **"Radius"** Button

Enter IP address and Shared secret for each Cisco ASA that wishes to use **SecurEnvoy** Two-Factor authentication.



Optional: SecurEnvoy RADIUS can also respond with LDAP group membership via Radius return attribute 3076-223.

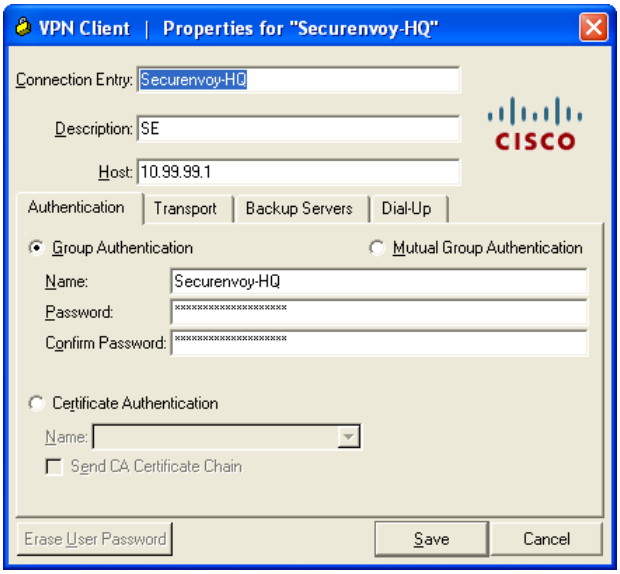
Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

© 2005 SecurEnvoy Ltd. All rights reserved

3.0 Cisco VPN Client Configuration

The VPN client requires minimal configuration, enter details for the entry and a description. Designate what the Cisco ASA VPN public IP address is. Finally set the VPN group name and password (Pre-shared secret set in VPN wizard). Click “Save”



4.0 Test logon

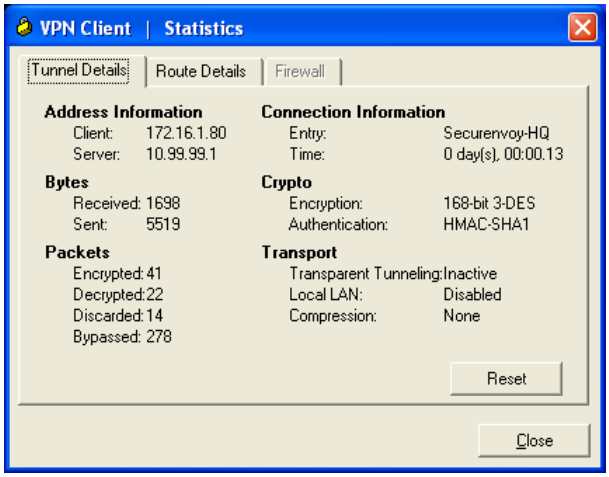
Once the configuration has been saved, the connection can be initiated by selecting the VPN profile for SecurEnvoy and click “connect”



Enter your Windows Username in the username field and password (PIN) and Passcode in the password field. Click “OK” to complete the logon process.

E.g. *P4ssw0rd*678123

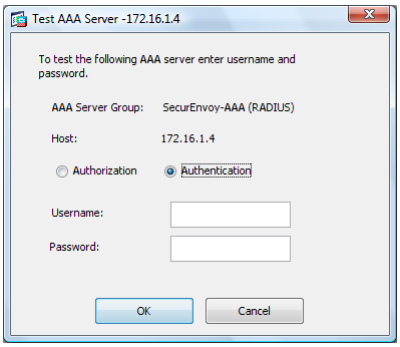
Right mouse click VPN icon in sys tray and select statistics to show additional information about the VPN



© 2005 SecurEnvoy Ltd. All rights reserved

5.0 Troubleshooting RADIUS connection

Navigate to AAA setup, go to AAA server, select the SecurEnvoy AAA server and “Test authentication”

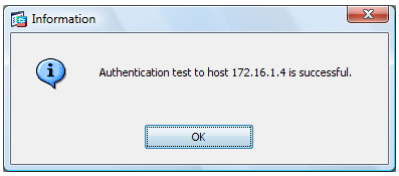


Enter Domain UserID in username field and domain password plus SMS passcode.

E.g. *P4ssw0rd*678123

Click OK

Information window will show response.



© 2005 SecurEnvoy Ltd. All rights reserved

5.0 Appendix – CLI additional lines added to Cisco ASA

AAA server setup

```
aaa-server SecurEnvoy-AAA protocol radius
  max-failed-attempts 1

aaa-server SecurEnvoy-AAA (inside) host 172.16.1.4
  key qwerty1234
  authentication-port 1812
```

VPN setup

```
crypto isakmp enable VPN-Interface
access-list inside_nat0_outbound line 1 extended permit ip 172.16.1.0 255.255.255.0
172.16.1.80 255.255.255.240
ip local pool VPN-POOL 172.16.1.80-172.16.1.90 mask 255.255.255.0
tunnel-group Securenvoy-HQ type ipsec-ra
tunnel-group Securenvoy-HQ general-attributes
  authentication-server-group  SecurEnvoy-AAA
  address-pool  VPN-POOL
tunnel-group Securenvoy-HQ ipsec-attributes
  pre-shared-key 345345623u4i5hy2353t
crypto isakmp policy 10 authen pre-share
crypto isakmp policy 10 encrypt 3des
crypto isakmp policy 10 hash sha
crypto isakmp policy 10 group 2
crypto isakmp policy 10 lifetime 86400
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map VPN-Interface_dyn_map 20 set  pfs group1
crypto dynamic-map VPN-Interface_dyn_map 20 set  transform-set  ESP-3DES-SHA
crypto map VPN-Interface_map 65535 ipsec-isakmp dynamic VPN-Interface_dyn_map
crypto map VPN-Interface_map interface  VPN-Interface
nat (inside) 0 access-list inside_nat0_outbound  tcp 0 0 udp 0
```

© 2005 SecurEnvoy Ltd. All rights reserved