



**External Authentication with Cisco Pix Firewall and
Cisco EZVpn client**

**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 Cisco Pix with Cisco EZVpn Client and SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Cisco PIX VPN Client provides - Secure Remote Access to the internal corporate network for all Client/Server applications.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cisco 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.

Cisco Pix 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 Cisco EZVpn client was configured. All authentication requests were forwarded to SecurEnvoy Authentication server. SecurEnvoy utilizes a web GUI for configuration, whereas the PIX configuration is shown with command line through Cisco IOS. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below

Cisco

Pix 515e Firewall

Software Revision Version 6.1(4)

Cisco EZVpn client Version 4.0.3 (D)

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

The Pix configuration is shown below, all relevant commands are highlighted in blue, additional text has been added to help explain the configuration, yet this is not to be entered into the actual configuration.

Connect by console cable, telnet or SSH to the PIX, logon and carry out a display of the running config by entering "wr t"

```
PIX Version 6.1(4)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password S6B.OP8DuEq4aS8B encrypted
passwd hryCz0BGY1IgKIi/ encrypted
hostname SecurEnvoyFW
domain-name Securenvoy.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 101 permit ip 10.0.0.0 255.255.0.0 30.0.0.0 255.255.255.0
    #this command sets what is defined as interesting VPN traffic
access-list smtp_www permit tcp any host x.x.x.x eq smtp
access-list smtp_www permit tcp any host x.x.x.x eq www
access-list smtp_www permit tcp any host x.x.x.x eq 443
pager lines 24
logging on
logging console debugging
logging buffered debugging
logging trap debugging
logging queue 8096
interface ethernet0 100basetx
interface ethernet1 auto
interface ethernet2 100basetx
icmp deny any outside
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside x.x.x.x 255.255.255.240
ip address inside 10.0.0.1 255.255.0.0
```

```
ip audit info action alarm

ip audit attack action alarm
ip local pool securevoy 30.0.0.1-30.0.0.20
    #this set the IP address pool for VPN clients
pdm history enable
arp timeout 14400
global (outside) 1 x.x.x.x netmask 255.255.255.240
nat (inside) 0 access-list 101
    #this command sets that the VPN traffic is not to be sent through the
    NAT process, i.e. NoNat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) x.x.x.x 10.0.0.2 netmask 255.255.255.255 50 20
static (inside,outside) x.x.x.x 10.0.0.3 netmask 255.255.255.255 100 50
access-group smtp_www in interface outside
route outside 0.0.0.0 0.0.0.0 x.x.x.x 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server Securevoy protocol radius
    #this command sets aaa server Securevoy is using the Radius
    protocol
aaa-server Securevoy (inside) host 10.0.11 SharedSecret timeout 10
    #this command sets the IP address, shared secret and timeout in
    seconds
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt security fragguard
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client authentication Securevoy
    #this command tells the VPN client config to use Securevoy for the
    authentication
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
```

```

isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 3600
vpngroup SECURENVOYvpn address-pool Securevoy
vpngroup SECURENVOYvpn dns-server 10.0.1.1
vpngroup SECURENVOYvpn wins-server 10.0.1.1
vpngroup SECURENVOYvpn default-domain securevoy.com
vpngroup SECURENVOYvpn idle-time 1800
vpngroup SECURENVOYvpn password *****
telnet 10.0.0.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:731dfb67cc82df4717b6ceb357130bd0
: end

```

To set up Radius on SecurEnvoy SecurAccess,

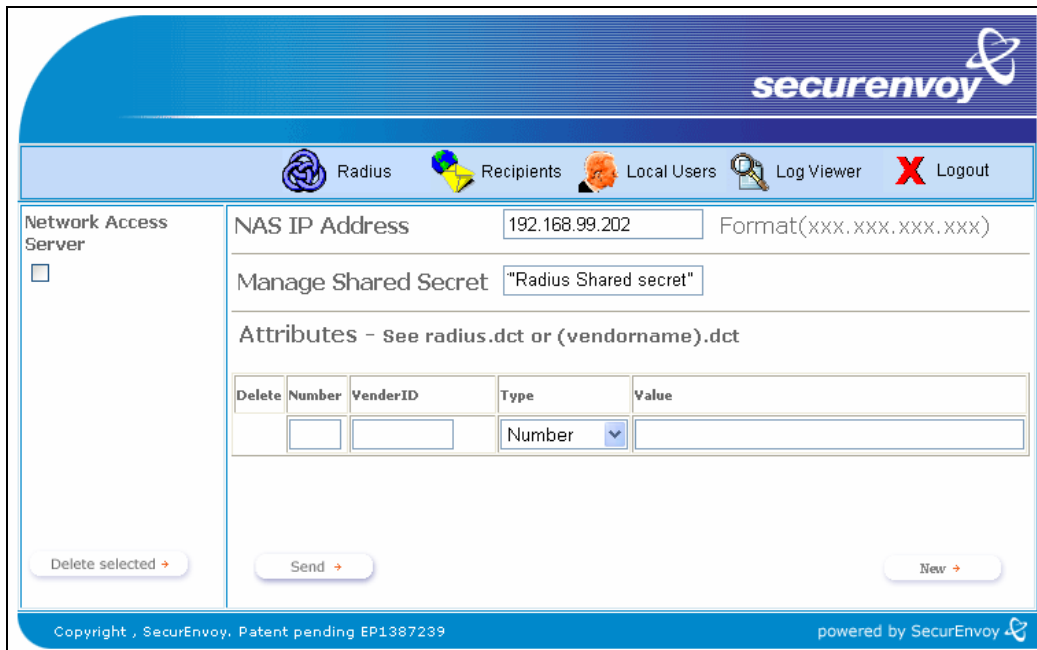
Launch local Security Server Administration

Select Radius

Enter NAS IP address, this will be the internal address of the Pix firewall

Enter "Radius Shared Secret", this must match what was entered within the Pix config.

Click Send



securevoy

Radius Recipients Local Users Log Viewer Logout

Network Access Server

NAS IP Address 192.168.99.202 Format(xxx.xxx.xxx.xxx)

Manage Shared Secret "Radius Shared secret"

Attributes - see radius.dct or (vendorname).dct

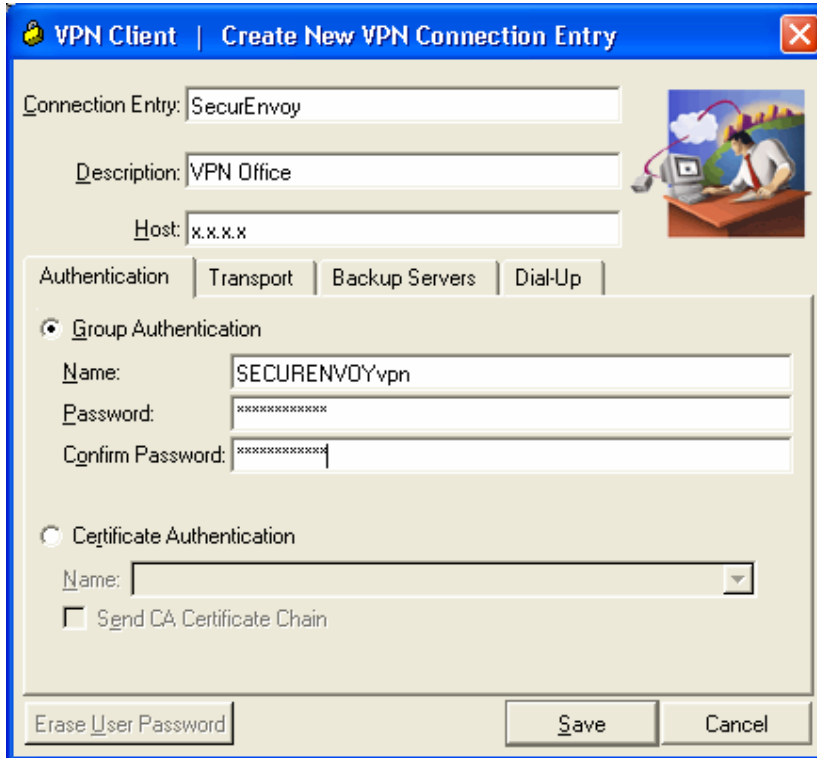
Delete	Number	VendorID	Type	Value
	<input type="text"/>	<input type="text"/>	Number	<input type="text"/>

Delete selected → Send → New →

Copyright , SecurEnvoy. Patent pending EP1387239 powered by SecurEnvoy

Click "logout"

The VPN client requires minimal configuration, enter details for the entry and a description. Designate what the PIX public IP address is. Finally set the VPN group name and password. Click "Save"



The screenshot shows the 'VPN Client | Create New VPN Connection Entry' dialog box. It has a blue title bar with a close button. The main area is light beige and contains several input fields and tabs. The 'Connection Entry' field is filled with 'SecurEnvoy'. The 'Description' field is filled with 'VPN Office'. The 'Host' field is filled with 'x.x.x.x'. There are four tabs: 'Authentication' (selected), 'Transport', 'Backup Servers', and 'Dial-Up'. Under the 'Authentication' tab, there are two radio buttons: 'Group Authentication' (selected) and 'Certificate Authentication'. Under 'Group Authentication', there are three input fields: 'Name' (filled with 'SECURENVOYvpn'), 'Password' (filled with '*****'), and 'Confirm Password' (filled with '*****'). Under 'Certificate Authentication', there is a 'Name' dropdown menu and a checkbox for 'Send CA Certificate Chain'. At the bottom, there are three buttons: 'Erase User Password', 'Save', and 'Cancel'.

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



The screenshot shows the 'VPN Client | User Authentication for "SecurEnvoy"' dialog box. It has a blue title bar with a close button. The main area is light beige and contains the Cisco Systems logo on the left. To the right of the logo are two input fields: 'Username' and 'Password'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Enter your NT Username in the username field and PIN Passcode in the password field. Click "OK" to complete the logon process.