

External Authentication with Checkpoint R75.40 Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information			
SecurEnvoy	www.securenvoy.com	0845 2600010	
	Merlin House		
	Brunel Road		
	Theale		
	Reading		
	RG7 4AB		
Phil Underwood	Punderwood@securenvoy.com		
Special thanks to	Assurix Ltd		
Adrian Bishop of	Mill Reef House		
Assurix Ltd for	9-14CheapStreet		
Checkpoint Integration	Newbury Berkshire RG14 5DD		



1 Contents

1	Cor	ntents	.2					
2	Che	Checkpoint R75.40 Integration Guide						
3	Pre	Pre Requisites						
4	Tok	enless Authentication (All Types)	.4					
	4.1	Configuration of Checkpoint® R75.40	.4					
	4.2	Configuration of SecurEnvoy	.9					
	4.3	Test Logon (SSL VPN)	10					
	4.4	Test Logon	10					
		•						



2 Checkpoint R75.40 Integration Guide

This document describes how to integrate a Checkpoint® R75.40 with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Checkpoint® R75.40 provides - Secure Application Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Checkpoint® R75.40) 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 directory server such as Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed to the SecurEnvoy Security Server via the RADIUS protocol, where it carries out a Two-Factor authentication. It provides a seemless login into the corporate network environment by the remote User entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the Checkpoint® R75.40 Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Checkpoint®

Checkpoint R75.40

Microsoft (for installation of SecurEnvoy Security Server) Windows 2008 server IIS installed with SSL certificate (required for management and remote administration) Access to Active Directory with an Administrator Account

SecurEnvoy

SecurAccess software release v6.2.500



3 Pre Requisites

It is assumed that the Checkpoint® R75.40 is setup and operational. It is also assumed that the SecurEnvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and Checkpoint® R75.40, additional open ports will be required.

NOTE: SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the Checkpoint® R75.40.

Only a single configuration is required, this will then support users with SMS sent via Pre-Load and Real Time as well as Soft Tokens, as Checkpoint® R75.40 supports RADIUS (Challenge Response). Configuration in this guide refers to this type of approach.

4 Tokenless Authentication (All Types)

4.1 Configuration of Checkpoint® R75.40

Launch the Checkpoint® R75.40 admin interface through the management GUI.

Verify that the Check Point firewall is currently VPN "Enabled"

Go to "Network Objects" "CheckPoint" and selecting the Checkpoint firewall you wish to configure. "Properties"





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.

Click OK to Save.

General Properties	Host Node - Ge	neral Properties			
- NAT	Machine -				
Other	Name:	rotterdam		Color:	Sky Blue
	IP Address:	10.14.2.47	Resolve from Name		
	Comment:	SecurEnvoy Server			
	Products:				
		Servers			

The SecurEnvoy RADIUS Server is configured by default to communicate on Port 1812, using Protocol UDP.

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.

+	IDP Service Properties - NEW-RADIUS							
+								
+	General							
+	Name: NEW PADIUS							
÷	Nalle. Iternational							
÷	Comment: NEW - Remote Authentication Dial-In Liser S							
÷	Commerce.							
+	Color: Firebrick -							
÷								
÷	Port: 1812 Get							
Ŧ	To proof a part range and a humber between the							
÷	lowest and the highest port numbers, for example 44-55.							
+								
+	Keep connections open after Policy has been installed							
+	Advanced							
+								
+								
+	OK Cancel							
	Services 8 23							
	Senting							
•	G UDB services							
•	Show: UDP services							
•	UOP name							
(F)	UIP abagea							
+	UCP NetFlow							
	UDP NEW-RADIUS							
	UP NEW-RADIUS-ACCOUNTING							
	UOP nfsd 👻							
	NEW - Remote Authentication Dial-In User Service							
	New Remove Edit							

👯 Firewall 🔠 NAT 🚼 Application & URL Filtering 🏝 Data Loss Pr

Advanced UDP Service Properties								
Source port: 1812								
To specify a port range, add a hyphen between the lowest and the highest port numbers, for example 44-55.								
Protocol Type:								
Accept Replies								
V Match for 'Any'								
Virtual Session Timeout:								
Other 40 seconds								
Enable Aggressive Aging Angressive Aning Timequit: @ Default: 15 seconds								
Other 15 A seconds								
Synchronize connections on Cluster								
Start synchronizing								
(Only for Clusters using an acceleration device supporting this feature. See the Performance Pack manual for details.)								
Perform static NAT good port selection on Cluster.								
(Only for Clusters with version R70 and above.)								
OK Cancel Help								

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 diagram.

Click OK to Save.



Specify 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".



There are many ways of setting up VPN users in CheckPoint. Configuration can be set to authenticate users by various methods, Users can be setup and authenticated directly upon Checkpoint, they can be setup as LDAP users and authenticate against Microsoft Active Directory, or can be authenticated against RADIUS.

In this example, we are going to configure CheckPoint to authenticate all external users to the SecurEnvoy RADIUS Server.

An External User Profile will be created that mandates RADIUS Authentication for all users that do not have a Check Point user account.

The Match all users profile with the profile name generic* is limited to only one property set. CheckPoint applies the restrictions specified for an ordinary user in the User Properties tabs (for example **Groups**).

For authentication purposes Check Point uses the name typed in by the user instead of generic*.

The following steps describe the process to configure an External Profile of "Match All Users".



Go to Manage > Users and Administrators > New > External User Profile > Match All Users.

The user generic* is created and a new window opens. Select Authentication from the left tool bar. Select RADIUS from the drop down box, as the user's Authentication Scheme.

General Properties	Authentication
Groups Authentication Location Time Certificates Encryption	Authentication Scheme: RADIUS Settings:
	Select a RADIUS Server or Group of Servers:
	SecurEnvoy -

Click **OK** to save changes.

From the "Users and Administrators" tab, "Right-Click" "User Groups" _ New User Group...

Create a "Remote_Access_VPN_Group" for external users.

	i 🖪 👻) % 🖬 🛅	: 🏭 🛍	略 発		•	"
This group is used as a Global Authentication Group for "Check Point Secure/Remote Client"	₽ < 	Users and Administrators Access Roles Administrator Groups		No. H	all 📰 NAT 😜	Application & URI Sourc	- Filtering 🦓 Data Loss Pre ce Destination
Remote Access VPN users.		External User Profiles LDAP Groups Templates	oteAccessUsers	+	Users and Administrat Show: All	ors: sers	
Click Ok to Save	<u>ا</u> الم	Name: Comment: Color: Mailing List Address:	RemoteAccessU	Jsers	•		H.
		Available Members:		Add >	Selected Members: AdminStaff SalesStaff TechnicalStaff		8 33-101)
		Show: External User P	rofiles 🔹	< Remove	View expanded	1 group	(Rules 114-117) 8-119) 22-129)
					UK	Cancel	

Select the "VPN Communities" tab, then "Right-Click" Remote Access,

_ New Remote Access Community, and configure.



On the "Participating Gateways" tab, select your CheckPoint.

Remote Access Community	y Properties - RemoteAccess	? 🗙
General	Participating Gateways	
Participating Gateways	All the connections between the Gateways below and the	
	Participants Users Groups will be encrypted. Participant Gateways:	
	FOX	
	New	
	Add Edit Remove	

Then, on the "Participating User Groups", select the "Remote_Access_VPN_Group" you created earlier.

Add this group into the Check Point "VPN Communities" properties.

	Remote Access Community	Properties - RemoteAccess	? 💌
	General Participating Gateways Participant User Group	Participant User Groups Remote Access User Groups:	New
Click Ok to Save.		Add Edit Remove	

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

P	i Fi	rewall 📰	NAT 🚼 Applicatio	n & URL Filtering 🖉	🖣 Data Loss Preventi	on 🚺 IPS 🐯 Ai	nti-Bot & Anti-Virus	🎒 Anti-Spam & Mai	Mobile Access	i 🔞 IPSec VPN 🛔	🛛 QoS 🗖 Desktop	😽 😽 Web Access
	No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
		0		Fox	🛄 rotterdam	😿 Any Traffic	UDP NEW-RADIUS	accept	- None	😿 Policy Targets	🖹 Any	Allow RADIUS Authentication connections between firewall and RADIUS servers

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



4.2 Configuration of SecurEnvoy

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

To Support Pre-Load and Real-Time SMS as well as Soft Tokens the following configuration is required.

Go to Config-Real Time	Allow Real Time Passcodes	
	Enable Real Time Prompt Enter Your 6 Digit Passcode	
Enable the checkbox	 Default (new users have real time set by default) 	
Click Update to complete		
Go to Config-Soft Tokens	Allow Soft Tokens	
Enable Soft Tokens	Enable Soft Tokens	
Enable PC Soft Tokens (If Required)	Support Google Authenticate Warning, if this mode is selected enrolment copy protection is redu	ced
Click Update to complete	Allow Laptops (PC or Mac)	

Click the "Radius" Button

Enter IP address and Shared secret for each Checkpoint®R75.40 that wishes to use **SecurEnvoy** Two-Factor authentication.

NAS IP Address 10.0.10.11	Format xxx.xxx.xxx or default for undefined IP's
Shared Secret qwerty	
Authenticate Passcode Only (passw	vord or pin not required) 🔲
Handle all passcode types in the same w	vay as Real Time Codes 🗹 Access Challange All
Default Domain w2008.com	Allow these domains V2008.com
	isa
	Select All Unselect All

Click checkbox "Handle all passcodes in the same way as Real Time"

Click "Update" to confirm settings.

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



4.3 Test Logon (SSL VPN)

Navigate to the relevant URL for the SSL VPN e.g. Https://remote.office.com	💿 Standar
	User name
User enters their Domain UserID and	Password:
password, click "Sign In"	🔘 Certifica

User is then prompted for their 6 digit Passcode.

Click "Submit" to complete the logon.

User nam	e; secur	envoy			
Password	••••	•••••			
🔘 Certifica	te Sign In				
📃 Use Cheo	k Point Secur	e Workspace			
Change Langu	age To: Englis	h	~	Sign In	
© Copyright 200	4-2012 Check Po git Passcode	oint Software Tech	inologies Lt	d. All rights rese	nve:
© Copyright 200 Enter Your 6 D	4-2012 Check Pr	oint Software Teof	inologies Lt	d. All rights rese	nve:

4.4 Test Logon

User launches the Endpoint VPN Client.

User enters their Domain UserID and password then clicks "Connect"



User is then prompted for their 6 digit Passcode.

Click "Connect" to complete the logon

