



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).

Juniper-ScreenOS Administration Tools (ns25) - Microsoft Internet Explorer						
Elle Edit View Favorites Iools Help						
↓ Back + → → · ③ ② Δ 🖞 @ Search 🝙 Favorites ③ Media 🧭 🔄 + 🎒 🖾 📄						
Address 🕘 https://connect.hhait.net/nswebui.html,DanaInfo=192.168.	57.198+		▼ ∂°G0			
Configuation > Auth > A	uth Servers > Edit		ns25 💡			
) 🖬 🔍 📕 🗎			
NetScreen-25 Name	SecurEnvoy	_				
- Home IP/Domain Name	192.168.57.209					
Configuration Backup1						
+ Undate						
Admin Backup2						
- Auth Timeout	10 (0 to disable)					
WebAuth Account Type		min 🔽 XAuth				
- Firewall						
Report Settings						
Network RADIUS	Radius port	1812 Retry Timeout	5 Sec			
+ Screening	Shared Secret	*****				
Policies						
- VPNs O SecurID	Client Retries	3 Client Timeout	5 coconde			
AutoKey IKE	Cliente Redites		seconds			
AutoKey Advanced	Authentication Port	5500				
- Gateway						
- P1 Proposal	Encryption Type	💿 DES 🔘 SDI				
XAuth Settings						
VPN Groups	Use Duress	O Yes 🖸 No				
Manual Key						
E Remove			j j 📋 j 🥶 Internet 🥼			



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.

Juniper-Screen05 Administra	ation Tools (ns25) - Microsoft Internet Explorer	
File Edit View Favorites To	ools Help	
Allert - A - O B A	Sauch DEmonitor Martin 24 R A = P -	
	Constant Marana California California California	
Agdress en https://connect.hhait.n	het/nswebui.html,DanaInfo=192.168.57.198+	
	Objects > User Groups > Local > Edit	ns25
Juniper [®] I.		
		1 🖬 🕯
MatScroon-25		-
- VPNo		
AutoKey IKE	Group Name (Securenvoy Group	
- AutoKey Advanced	<- Group Members -> <- Available Members ->	
Gateway	anthony fletcher	
- P1 Proposal	external admin	
- P2 Proposal		
- XAuth Settings		
VPN Groups		
– Manual Key	>>	
 L2TP 		
- Monitor Status		
 Objects 		
 Addresses 		
 Services 		
 Users 	OK Cancel	
- Local		
- Local Groups		
External Groups		
IP Pools Cabadulas		
Group Expressions		
Certificates		
Attacks		
Antivirus		
		1.0.1-
🕅 🙈 💹 💽 🗌 🕅 c. 178 c.		E 🐹 🌠 +/+ 🔼 20:05

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.

Juniper-ScreenOS Administratio	on Tools (ns25) - Microsoft Internet Explorer	
Ele Edit View Favorites Tools	: Help	
↔Back • → - 🔕 🗿 🖄 🚳	Search 🖻 Favorites 🛞 Media 🧭 🗟 - 🎯 🛒 📄 📖	
Address 🕘 https://connect.hhait.net/	nswebui.html,DanaInfo=192.168.57.198+	• @G
	Objects > Users > Local > Edit	ns25 ?
Juniper 📃		
		🔹 🕻 🗟 🔹 🥥 📕 -
NetScreen-25	Auth/IKE/L2TP/XAuth User	
VPNs		
- AutoKey IKE	User Name external.admin Groups: SecurEnvoy Group	
- Autokey Advanced	Status 📀 Enable 🔿 Disable	
- P1 Proposal		
- P2 Proposal	IKE User Number of Multiple Logins with Same ID 1	
- XAuth Settings	Simple Identity	
- VPN Groups	IKE ID Type AUTO KE Identity external.admin@acmel.com	
T-12TP	C Use Distinguished Name For ID	
Monitor Status		-
Objects	Authentication User User Password	
 Addresses 		
Services	XAuth User Confirm Password	
Local	L2TP User	
- Local Groups	1 OTD (VAuth Description Cothings (Description 10: 0.0.0.0.)	-
External Groups	(Remote Protocolo)	
- IP Pools	IP POOL INONE Static IP U.U.U.U	
- Schedules	Primary DNS IP 0.0.0.0 Primary WINS IP 0.0.0.0	
Certificates	Secondary DNS IP 0.0.0.0 Secondary WINS IP 0.0.0.0	
🏦 Start 🛛 🚮 🏉 🔣 🙆 🖉 🚺 🚺 С.	, 🕼 C., 😋 D., 🧆 S., 🏧 D., 🖉 S., 🧿 I., 🖂 R., 🦉 J., 😋 L., 🔛 A., 🗐 N., 😓 🏷 🌾 🔛	🖸 💐 🌠 🕬 🚫 20:08

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.

Juniper-ScreenOS Administ	stration Tools (ns25) - Microsoft Internet Explorer	ol ×l
Elle Edit View Favorites	Tools Help	11
4= Back • ⇒ · (2) (2) (3)	Consearch GalFavorites @Media 🕼 🖧 🌧 🛒 🗐 🖄	
Address (a) https://connect.hhal	alt.net/nswebu.html.DanaInfo=192.168.57.198+	Go
- 12	VPNs > AutoKev Advanced > Gateway > Edit ns25	
		-
(
Juniper		
A ANETWORKS	1	
NotScroon 25	Gateway Name SecurEnvoy-nateway	-
- VPNs	Annual and a Constant of Annual to Constant of Annual	
- AutoKey IKE	Security Level & Standard & Compatible & Basic & Custom	
AutoKey Advanced		
Gateway	kemote Gateway Type	
PT Proposal P2 Proposal	C Static IP Address IP Address/Hostname	
- XAuth Settings	C Dynamic IP Address Peer ID	
VPN Groups	C Dialun User User None	
– Manual Key		
L2TP Manifest Status	Group Secure way a compared a compa	
- Monitor Status		
 Addresses 	Preshared Key	
 Services 	Local ID (optional)	
 Users 	Outgoing Interface ethernet3	
- Local		
External Groups	OK Cancel Advanced	
- IP Pools		
- Schedules		
Group Expressions		
Certificates		
Allacks Antivinus		
Annoing		
e Done	🗎 😰 Internet	11.

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.

ew Favorites Tools Help	310
v A B A A Gravethe Alfavorites @Media A B. A ⊂ B ⊂ B ↔	
The interview of the contract of the second se	∂ Go
VPNs > AutoKev Advanced > Gateway > Edit ns25	2
	·
niper*	
Predefined O Standard O Compatible O Basic	-
vreer-25 User Dennes U	
y inter prege dees and in Prone	
away	
Proposal Mode (Initiator) C Main (ID Protection) C Aggressive	
Proposal	
Groups	
Key Kepaliye Fraguency D	
Heartbeat Heartbeat	
ses Hello O Seconds (0~3600 Sec)	
s Reconnect 0 Seconds (60~9999 Sec)	
Threshold 5	
a Groups C None	
email Groups C XAuth Server	
S C Use Default	
The second Authentication	
ates CUser None	
C User Group None	
Allowed Authentication Type 🔽 CHAP Only	
🖲 🕑 External Authentication SecurEnvoy 🔽 🗖 Query Remote Setting	
C Allow Any	•

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.

i luniner-Screen(15 Administration Tools (ns25) - Microsoft Internet Explorer
The Edit View Favorites Tools Heb
b Back + → → @ D Al @Search Bull-Reventes @Media (A D)+ As III = 11
VEX.S and A state of the state
N Juniper*
NorSersen-25 VPN Name DialUp-P2
VPNs Security Level C Standard C Compatible C Basic C Custom
AutoKey IKE
AutoKey Advanced Remote Gateway Predefined SecurEnvoy-gateway
Gateway C Create a Simple Gateway
P1 Proposal Gateway Name
P2 Proposal
Value State P Value State P
Manual Kay
C Dialup User User None
Monitor Status C Dialup Group Group Rone
Objects
Addresses
Services Preshared Key Use As Seed
Users Security Level © Standard © Compatible © Basic
Local Outgoing Interface ethemet3
Eucar Groups
IP Pools OK Cancel Advanced
Schedules
Group Expressions

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

Jumper-Screenus Administrat	tion Loois (ns25) - Microsoit Internet Explorer	르비스
e Edit View Favorites Too	ols Help	10
Back 🔹 🔿 👻 🙆 🚮 🔇	🔕 Search 🔊 Favorites 🛞 Media 🧭 🛃 - 🍙 🗹 📄 📖	
dress 🕘 https://connect.hhait.ne	t/nswebui.html,DanaInfo=192.168.57.198+	▼ (~)G0
	VPNs > AutoKey IKE > Edit	ns25 ?
Juniper		
NETWORKS	Security Level	
NetScreen-25	Predefined C Standard C Compatible C Basic	
VPNs	User Defined (* Custom	
- AutoKey IKE	Phase 2 Proposal	
AutoKey Advanced	nopfs-esp-3des-sha 🔽 nopfs-esp-3des-md5 💌	
- Gateway	nopfs-esp-des-sha. 💌 nopfs-esp-des-md5 💌	
PT Proposal R2 Proposal		
- XAuth Settings	Replay Protection 🗖	
- VPN Groups	Transport Mode 🗌 (For L2TP-over-IPSec only)	
– Manual Key	Bind to C None	
L2TP	C Tunnel Interface	
- Monitor Status	C Tunnel Zone Untrust-Ti	in T
Addresses		
Services	Proxy-ID 🗖	
- Users	Local IP / Netmask 0.0.0.0 /	
- Local	Remote IP / Netmask 0.0.0.0 /	
- Local Groups	Service ANY	
External Groups		
Schedules	VPN Group None 🗾 Weight 🛛	
- Group Expressions	VPN Monitor	
- Certificates	Source Interface default	
Attacks	Destination IP 0.0.0	
- Antivirus -	Ontimized	
Wizards	Rekey	
		i i i i i i i i i i i i i i i i i i i



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.

er-ScreenOS Administrat	ion Tools (ns25) - Microsoft Inte	met Explorer
lit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	ols <u>H</u> elp	(f)
• ⇒ • 🕲 🙆 🖽 🤅	🗟 Search 🛛 🗟 Favorites 🏼 🤭 Media	🗳 🗗 🖅 🗐 🛄
https://connect.hhait.ne	t/nswebui.html,DanaInfo=192.168.57	.198+ 💌 🔗 Go
	Policies (From Untrust To) Trust) ns25 ?
Juniper		
	Name (optional)	
NetScreen-25		C New Address
нср 🔟	Source Address	Caddrees Beek Entry Diald In VPN
PPoE		
SRP	Destination Address	C New Address
ening		Address Book Entry HHAIT Multiple
cies	Service	ANY Multiple
st Policies		
S	Application	None
utoKey Advanced		
Gateway		URL Filtering
P1 Proposal	Action	Tunnel Deep Inspection
P2 Proposal		
- XAuth Settings		Attached AV Object Names
anual Key	Antivirus Objects	
2TP		>>
Ionitor Status	Tunnel	VPN DialUp-P2 -
ects		
ddresses		mouny matching durectional vew policy
sers		L2TP None
- Local	Logging	
- Local Groups		
External Groups		OK Cancel Advanced
Pools -		

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

	Radius Recipients Scal Users 🖓 Log Viewer 🗙 Logout			
Network Access Server	NAS IP Address 192.168.99.202 Format(xxx, xxx, xxx)			
	Manage Shared Secret "Radius Shared secret"			
Attributes - See radius.dct or (vendorname).dct				
	Delete Number VenderID Type Value			
	Number V			
Delete selected >	Send >			
Copyright , SecurEnvo	y. Patent pending EP1387239 powered by SecurEnvoy \mathcal{L}			

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.

Internet Authentication Service			
Eile Action View Help			
 Internet Authentication Service (Local) RADIUS Clients Remote Access Logging Remote Access Policies Connection Request Processing Connection Request Policies Remote RADIUS Server Groups 	Internet Authenticati General Ports Enter the RADIUS au Authentication: Accounting:	ion Service (Local) Properties uthentication and accounting port numb 9999 1813	pers.

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.

Internet Authentication Service				_ 🗆 🗙	
Eile Action View Help					
P Internet Authentication Service (Local)	Friendly M	lame	Address	Protocol	
	<u>∎</u> SE		10.0.10.1	RADIUS	
E Pro	perties			? 🗙	
Connection Request Processing Sett	ings				
Remote RADIUS Server Groups	endly name:				
		k.			
	<u>V</u> erify				
lfy	If you are using remote access policies based on the client vendor's				
atti	ribute, specify the	e vendor of th	ie RADIUS client.		
Clig	ent-Vendor:	RADIUS	Standard	.	
	Bequest must c	ontain the Me	essage Authenticator	attribute	
	<u>H</u> oquest must c	on can't the bit			
<u>S</u> h	ared secret:		******		
	nfirm shared secr	et:	*****		
		00.	1		



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.