

# HOWTO: How to configure IPSEC roadwarrior to gateway using The GreenBow client



# 'How-to' guides for configuring VPNs with GateDefender Integra

Panda Security wants to ensure you get the most out of GateDefender Integra. For this reason, we offer you all the information you need about the characteristics and configuration of the product. Refer to <a href="http://www.pandasecurity.com/">http://www.pandasecurity.com/</a> and <a href="http://www.pandasecurity.com/">http://www.pandasecurity.com/</a> for more information.

#### 'How-to' guides for Panda GateDefender Integra

The software described in this document is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

The anti-spam technology in this product is provided by Mailshell. The web filtering technology in this product is provided by Cobion.

#### **Copyright notice**

© Panda 2007. All rights reserved. Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda, c/ Buenos Aires, 12 48001 Bilbao (Biscay) Spain.

#### **Registered Trademarks**

Panda Security<sup>™</sup>. TruPrevent: Registered in U.S.A Patent and Trademark Office. Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other product names may be registered trademarks of their respective owners. D. L. BI-1915-07 © Panda 2007. All rights reserved.



# INDEX

IPSEC R	OADWARRIOR-TO-GATEWAY USING THE GREENBOW CLIENT	3
1.1	Scenario setup	3
1.2	GATEWAY SIDE CONFIGURATION (PANDA GATEDEFENDER INTEGRA)	5
1.2.	1 IP group configuration	5
1.2.	2 CA and local server certificates	6
1.2.	3 Users and group configuration (optional)	8
1.2.	4 IPSec configuration on the server side	
1.3	CLIENT SIDE CONFIGURATION (THEGREENBOW CLIENT)	
1.4	ESTABLISHING IPSec VPN CONNECTION	
1.5	Further considerations	
1.6	CONFIGURATION CHECKING	

#### Symbols and styles used in this documentation

#### Symbols used in this documentation:



**Note**. Clarification and additional information.



**Important**. Highlights the importance of a concept.



\$7

Tip. Ideas to help you get the most from your program.

**Reference**. Other references with more information of interest.

#### Fonts and styles used in the documentation:

Bold: Names of menus, options, buttons, windows or dialog boxes.

*Codes style*: Names of files, extensions, folders, command line information or configuration files, for example, scripts.

*Italics*: Names of options related with the operating system and programs or files with their own name.



# IPSec roadwarrior-to-gateway using The GreenBow client

(IP Secure) Security protocol that allows the secure interchange of packets in the IP layer, guaranteeing the security of the link between the device and a network. It offers integrity, authentication, access control and confidentiality for sending IP packets via Internet

Panda GateDefender Integra includes a VPN system to create your own virtual private networks, widening the reach of your network and ensuring confidential connections.

The purpose of this guide is to describe the steps to create a IPsec virtual private network (VPN) with Panda GateDefender Integra, using real data.

**Note:** It is taken for granted that the Panda GateDefender Integra appliance is already configured, at least basically, and working. For further information about how to install and configure Panda GateDefender Integra, refer to the Installation Guide.

**Important:** Panda GateDefender Integra must be working in Router mode. Otherwise, you will not be able to use the VPN system.

# 1.1 Scenario setup

The illustration below is a typical roadwarrior-to-gateway IPSec VPN scenario:

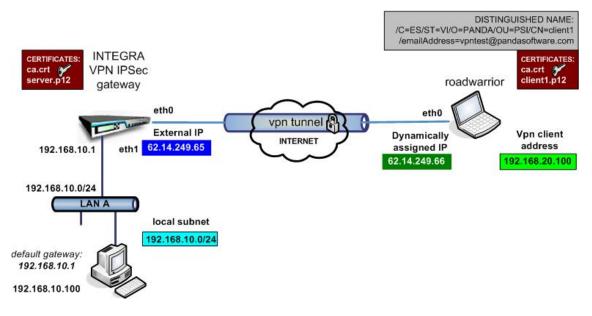


Figure 5.1: IPSec VPN



The roadwarrior has been dynamically assigned an address by the ISP and will access Integra's LAN by means of a secure tunnel using the IPSec protocol.

In this how-to, INTEGRA's WAN or Internet interface are assigned the IP address 62.14.249.66.

Clients on Integra's LAN side must have configured Integra's LAN IP **192.168.10.1** as a default gateway or as an implicit route to the roadwarrior VPN client address. See the section below on how-to configure routes on the hosts on the INTEGRA LAN side.

# 1.2 Gateway side configuration (Panda GateDefender Integra)

# 1.2.1 IP group configuration

The first step when configuring an IPSec VPN consists of defining the IP range as a local subnet which you want your roadwarrior to be able to connect to.

To define the local subnet, follow the steps described below:

- 1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
- 2. Select IP addresses.
- In the Groups section, click on Add.
   A descriptive name of the group must be provided *(ipsec local subnet* will be used for this how-to) in the Name field and the IP range (*192.168.10.0/24* will be used in this how-to) in the IP/Mask radio button section.
- 4. Click on Add IP.

The settings will be configured as shown in figure 5.2

Note that you cannot use a previously defined IP Group that has been already assigned to another VPN.

Name	Addresses
Export	Import Add Modify Delete
Groups	
Groups Name	Addresses
	Addresses 192.168.10.0/ 24

Figure 5.2



# 1.2.2 CA and local server certificates

Certificates are required for authentication purposes. You need to import the public CA certificates which signed the roadwarrior certificates. It is also necessary to import the Integra VPN gateway local certificate that will be used to authenticate the Integra VPN server itself.

In order to import the CA, follow the procedure below:

- 1. Go to the **VPN** section of the main Panda GateDefender Integra console menu.
- 2. Select Digital certificate management.
- 3. In the CA certificates section, click on Import.
  - Enter Certificate name (ca will be used in this how-to).
  - Click on Browse... to select the certificate you want to import.
  - Click on Import once you have chosen a CA certificate that you wish to import.

VPN: Import certificate	1	_		0	Help
Import certificate					
Certificate name	ca				
Certificate to import (X.509)	C:\certificates\ca.crt	Examinar			
			Import	_ c	ancel

Figure 5.3

In order to import local server certificates, follow the procedure below:

- 1. Go to the **VPN** section of the main Panda GateDefender Integra console menu.
- 2. Select **Digital certificate management** and, in the **Local certificates** section, click on **Import**.
  - Select if you want to **Import a certificate pending signing** or **Import a certificate with private key** issued by a CA.
  - If you select **Import certificate with private key**, enter the PKCS12 Certificate Name (*server* will be used in this how-to) and optionally **Password**.
- 3. Click on **Browse...** to select the certificate you want to import.
- 4. Click on **Import** once you have chosen a certificate.



VPN: Import certific	cate	_				Help
Import certificate						
O Import certificate pe	nding signing					
Cer	tificate name		19			
Import certificate wi	th private key					
PKC	512 certificate name	server				
Pas	sword (optional)					
Certificate to import	C:\certificates'	ιserver.p1ζ(jΕx	aminar])			
				Import	G	

Figure 5.4

Once the CA and server certificates have been imported successfully, the corresponding configuration screen displayed is similar to that shown in figure 5.5

server	Identif server			<b>Validit</b> 21/07/1
Import	Request signature	Generate	View Del	ete
CA certificate Name	es Identifier	Organization	Validity	y CR
ca	rootCA	PANDA	21/07/1	6 X

Figure 5.5

Note that if you select **Import certificate with private key**, you can only import local PKCS12 format certificates (files have p12 or pfx extensions).



## 1.2.3 Users and group configuration (optional)

- 1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
- 2. Select User management.
- 3. In the Users section, click on Add.
- 4. This will take you to a screen where you should provide data for at least the first three textboxes:
  - Name (*test* will be used for this how-to).
  - Password *(testing* will be used for this how-to).
  - Repeat password.
- 5. Once you have configured it, click on **Add** to save the changes.

As defined groups of VPN users were needed, you need to add previously defined users to your group.

In order to do this, follow the steps below:

- 1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
- 2. Select User management.
- 3. In the User Groups section, click on Add.
- 4. Define a group name and add users from the box below.

Once this has been done, configuration should be similar to that shown in figure 5.6

	Comm	ient		
test				
Export	Import	Add	Modify	Delete
Jser groups Name		Component	ts	
testing		test		

Figure 5.6



### **1.2.4 IPSec configuration on the server side**

This section is related to the IPSec configuration.

In order to configure IPSec using previously defined elements, follow the instructions below:

- 1. Go to the Panda GateDefender Integra administration console.
- 2. Click on **VPN** in the panel on the left.
- 3. Then select VPN management, and then IPSEC VPN management.

The available options are:

- Name: Enter the descriptive name of the VPN. ( *IPSec RW GreenBow* will be used in this how-to).
- Local IP: Enter the local public IP address or choose IP assigned by DHCP (Local public IP 62.12.249.65 will be used in this how-to).
- **Phase 1 policy**: Use the drop-down menu to select the IKE I policy you want to apply. (*1 IKE I* will be used in this how-to).

Here is the screenshot of the 1 IKE I  $\,$  policy (with a default options) used in this how-to.

VPNs IPSEC			0	Help
VPNs IPSec 0	Global configuration Phase	I IKE Phase II IKE		
III Phase 1 policie	≥s (IKE I)			
Name	Encryption algorithm	Authentication algorithm	DH group	
1 IKE I	All	All	Without DH	

Figure 5.7

- 1. Select a protocol to use: **IPSec**
- 2. When you choose IPSec, the following options will be available:
  - Local subnet: Select a subnet from those defined in the drop-down menu.
  - Phase II policy: IKE II policy identifier of this tunnel.

Here is the screenshot of the 1 IKE II policy (with a default options) used in this how-to.



VP	Ns IPSEC			🕜 Help
VPI	Ns IPSec 📔 Globa	al configuration Phase I	IKE Phase II IKE	
	Phase II policies (I	KE II)		
	Name	Encryption algorithm	Authentication algorithm	PFS
	1 IKE II	All	All	Sin PFS
			Add Modify	Delete



- Local ID: X-509 certificate: Use the drop-down menu to select the local server certificate (*server.p12* will be used in this how-to).
- **CA certificate**: Remote users authenticating using an X-509 certificate must also present the signature of a CA. Use the drop-down menu to select the CA certificate that signed the roadwarriors certificate (*ca.crt* will be used in this how-to).

Once the IPsec part has been configured, the corresponding configuration screen which will be displayed will be similar to figure 5.9



Name:       IPSec RW GreenBow         Phase I parameters       Interface settings         IP assigned by DHCP       Interface settings         Phase I policy       I IKE I         Phase I policy       I INDE         Image: I policy       I IKE I         Phase II policy       I IKE II         Phase II policy       Server         © CA certificate       Server         © CA certificate       Ca	
Interface settings     IP assigned by DHCP     Phase I policy     IKE I     Phase I policy     Protocol     L2TP/IPSec     Image: Certificate setting     Phase II policy     It is policy     Address setting     Phase II policy     It is policy     Phase II policy     It is policy     Phase II policy     It is policy     Phase II policy    <	
<ul> <li>○ IP assigned by DHCP</li> <li>Phase I policy</li> <li>1 IKE I</li> <li>Phase I policy sett</li> <li>Phase II parameters</li> <li>Protocol</li> <li>L2TP/IPSec</li> <li>③ IPSec</li> <li>Tunnel</li> <li>Local subnet</li> <li>ipsec local subnet</li> <li>Address settin</li> <li>Phase II policy 1 IKE II</li> <li>Phase II policy sett</li> </ul>	
Phase I policy 1 IKE I Phase I policy sett Phase II parameters Protocol L2TP/IPSec ③ IPSec Tunnel Local subnet ipsec local subnet Address settin Phase II policy 1 IKE II Phase II policy s Remote user identification Local ID: X.509 certificate	
Phase II parameters Protocol L2TP/IPSec  IPSec Tunnel Local subnet ipsec local subnet  Phase II policy 1 IKE II  Phase II policy 5 Remote user identification Local ID: X.509 certificate  Server Certificate sett	
Protocol L2TP/IPSec	œ
● IPSec Tunnel Local subnet ipsec local subnet ▲ Address settin Phase II policy 1 IKE II ♥ Phase II policy s Remote user identification Local ID: X.509 certificate	1 <u>05</u>
Tunnel Local subnet ipsec local subnet Address settin Phase II policy 1 IKE II Phase II policy s Remote user identification Local ID: X.509 certificate <u>server Certificate sett</u>	<u>lQ5</u>
Local subnet ipsec local subnet Address settin Phase II policy 1 IKE II Phase II policy s Remote user identification Local ID: X.509 certificate <u>server Certificate sett</u>	<u>us</u>
Phase II policy 1 IKE II Phase II policy s Remote user identification Local ID: X.509 certificate <u>server</u> <u>Certificate sett</u>	i <u>gs</u>
Remote user identification Local ID: X.509 certificate	
Local ID: X.509 certificate Server Certificate sett	ettings
CA certificate Ca Certificate sett	ings
	ings
○ X.509 users Itesting W User settings	
Additional local ID:	
<ul> <li>IP</li> <li>Address settin</li> </ul>	igs
O FQDN domain	
C Email address	

Figure 5.9

Optionally, a previously defined group of users can be provided, if option **X.509 users** is selected.

Note that if there is any NAT device between a roadwarrior and Integra VPN gateway, then you should enable the NAT transversal verification checkbox as shown below.

VPNs IPSEC	🕜 Help
VPNs IPSec Global configuration Phase I IKE Phase II IKE	
III NAT traversal 🔽	

Figure 5.10



# **1.3 Client side configuration (TheGreenBow client)**

Once it has been confirmed that the connection to the Internet is correctly configured on the client computers running Microsoft Windows 2000/XP, and you install TheGreenBow IPSec client, follow the steps described below to configure the client side.

a

**Note:** For the correct functioning of The GreenBow client it is essential to disable the IPSEC services (Control Panel--> Administrative Tools--> Services)

TheGreenBow VPN Clie	ent 🗖 🗖 🔀
File VPN Configuration Tools	?
THEGREENBOW	IPSec VPN Client
🚕 Console	Phase 1 (Authentication)
🔯 Parameters	Name CnxVpn1
S Connections	Interface 62.14.249.66
Configuration	Remote Gateway       62.14.249.65         C       Preshared Key         Confirm
	Save & Apply
VPN Tunnel opened	Tunnel: 🧿

Figure 5.11

Certificates are required for authentication purposes. You need to import the trusted public CA certificates which signed the Integra VPN gateway certificate. It is also necessary to import the roadwarrior certificate and its corresponding private key that would be used to authenticate the roadwarrior itself.

In order to import CA and local certificates for a roadwarrior, click on Certificate Import...



Once the certificates have been imported you must provide at least **local ID** by clicking on **P1 Advanced...** Then, choose the **DER ASN1 DN** ID type and enter the corresponding ID for a local certificate as shown in figure 5.14.

DER ASN1 DN ID or **Distinguished Name** can be read from the local client certificate using openssl command:

#### # openssl x509 - in client1.crt - noout - subject

It is possible to access the whole subnet or just one specific host on Panda GD Integra LAN as shown in figures 5.12 and 5.13.

VPN Configuration To	
EGREENBO	IPSec VPN Ci
Console	Phase 2 (IPSec Configuration)
Parameters	Name CnxVpn1
Connections	VPN Client address 192 . 168 . 20 . 100
Configuration	Address type     Subnet address       Remote LAN address     192 . 168 . 10 . 0       Subnet Mask     255 . 255 . 0
	ESP Encryption 3DES Authentication SHA Mode Tunnel
	PFS Group DH1024      Open Tunnel
	Save & Apply

Figure 5.12



TheGreenBow VPN Cli	ent 📃 🗖 🔀
File VPN Configuration Tools	?
THEGREENBOW	IPSec VPN Client
🔑 Console	Phase 2 (IPSec Configuration)
Parameters	Name CnxVpn1
S Connections	VPN Client address 192 . 168 . 20 . 100
Griguration Griguration Griguration Griggright Grigor Grig Grigor Grigor Grigor Grigor Gr	Address type       Single address         Remote host address       192       168       10       100         Subnet Mask       255       255       0
	ESP Encryption 3DES Authentication SHA Mode Tunnel
	FPFS Group DH1024  Open Tunnel
2	Save & Apply
VPN ready	Tunnel: 9

Figure 5.13

If Xauth is used as an authentication option on Panda GateDefender Integra then you should configure it also on the client side, as shown in figure 5.14.

Note that Aggressive Mode is not supported by Panda GateDefender Integra for security reasons.



Phase1 Advance	d	
		A
Advanced featur	es	
🔲 Config Mod	le IKE Port	
🗌 Aggressive	Mode Redund.GW	
	NAT-T	Automatic
X-Auth	up Login Password	
Local and Remo	ote ID	
Local ID	Choose the type of ID: DER ASN1 DN	Set the value for the ID: /C=ES/ST=VI/O=PAND
Remote ID	-	
	[	Ok Cancel

Figure 5.14

More details about configuration issues can be found on TheGreenBow website: <u>www.thegreenbow.com</u>



# 1.4 Establishing IPSec VPN connection

Use the following procedure in order to establish IPSec VPN connection which has been previously defined:

- 1. Click on "Save & Apply" to take into account all modifications made on your VPN Client configuration.
- 2. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser).
- 3. Select "Connections" to see open VPN Tunnels.

TheGreenBow VPN Clie	ent			
File VPN Configuration Tools	?			
THEGREENBOW			IPSe	c VPN Client
la Console	Tunnels v	view		
🚱 Parameters	Host	IP	Mode	Crypto
Connections	SCnxVpn1	192.168.10.0/255.255.255.0	Tunnel	ESP 3DES SHA
	<			ose Tunnel
			Sa	ve & Apply
VPN Tunnel opened				Tunnel: 🧿

4. Select "**Console**" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and Panda GateDefender Integra.



VPN Console ACTIVE	
Save Stop Clear Options	
125916 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [SA] [VID] [VID] 125916 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE 125916 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE 125916 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode [ID] [CERT] [SIG] 125916 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [ID] [CERT] [SIG] 125916 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode [ID] [CERT] [SIG] 125916 Default (SA CnxVpn1-P1) RECV phase 2 Main Mode [ID] [CERT] [SIG] 125916 Default (SA CnxVpn1-P1) RECV phase 2 Quick Mode [HASH] [SA 125916 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA 125916 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA 125916 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA 125916 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA	E] [CERT_REQ] E] [CERT_REQ] lient1/emailAddress=vpntest@pandasoftware.c A] [KEY_EXCH] [NONCE] [ID] (ID]
	Current line : 10 max. lines : 10000

Figure 5.15

Once the VPN tunnel has been established, specific network resources should be available to you as they are when you connect directly to the network.

In order to disconnect, right-click on the TheGreenBow icon that appears in the bottom right corner, and then select **Quit** or just press **Close Tunnel** in TheGreenBow client window.



# **1.5 Further considerations**

If Integra's firewall is used, all the corresponding configuration rules will automatically be entered in the firewall.

But if you use a personal firewall or broadband router with firewall features or if there are routers or firewalls between TheGreenBow client and the Integra VPN gateway server, the following ports and protocols must be enabled for IPSec on all firewalls and routers between them:

- UDP port 500 (IKE)
- IP protocol 50 (ESP), 51 (AH) or

UDP port 4500 (NAT-T): needed when there is at least a SNAT device between two gateways (the usual situation)

Note that IP 50 is a *protocol*, not a *port*.

If the SNAT option is enabled for the local network that intervenes in the VPN in any of the GateDefender Integra configurations -the Static key or certificates-, you need to add a NAT rule with a higher priority than the previous rule. This rule should ensure that the change of source IP header belonging to SNAT is not applied to the VPN traffic before the packets are routed to the tunnel. To do this, the *Keep original address* check box must be selected:

Filter rule			
Name:	SNAT IPSec RW		
Source: 🔘 In	terface/Zone Any	Address	ipsec loc subnet 💌 💸
Target: 🚫 Int	erface/Zone Any	🛛 💽 💽 Address	192.168.20.100
	Interface settings	Addre	ess settings
Service: Action:	Any 💌		Service settings
۲	Keep original address		
O NAT source	address Any	<ul> <li>S</li> <li>S</li></ul>	Address settings
🔘 Address gr	oup	V	
Priority:	1		
Schedule:		$\checkmark$	Schedule settings
🔲 Create log			



The example in the screenshot shows the rule to add to ensure that traffic from the local IPSEC subnet can be correctly routed through the VPN tunnel to the roadwarriors' network **192.168.20.100**.



# **1.6 Configuration checking**

In order to check the IPSec VPN configuration please proceed as described below::

- 1. Access the Panda GateDefender Integra administration console.
- 2. Click on **VPN** in the panel on the left.
- 3. Then select **VPN Monitor** which will allow you to see the status of all established VPN connections (as shown in figure 5.16).

Remote use	r tunnels (roadv	varriors)			
Name	User	Protocol	Public IP	Private IP	Traffic
VPN RW	OU=PSI, CN	/I, O=PANDA, =client1, pandasoftware.coi	IPSEC m	62.14.249.66	192.168.20.100

Figure 5.16

Any of the roadwarriors can verify the configuration settings of its Windows 2000/XP independently.

In order to carry out that task, the command prompt should be used:

The **ping** –**n** 10 192.168.10.100 command pings from the roadwarrior to one of the hosts that reside on the internal network behind Integra VPN gateway and should see a response from the remote host.

At the same time, a network traffic monitoring tool such as Ethereal can be used to check if all the traffic between a roadwarrior and the gateway is encrypted.

The encrypted ESP (Encapsulating Security Payload) packets will be seen when observing traffic in the external network interface

More details about troubleshooting issues of TheGreenBow client can be found on its website: <u>www.thegreenbow.com</u>

#### Index

© Panda 2006 0707-PGDIHT09-03-EN