

## Howto: How to configure static port mapping in the corporate router/firewall for Panda GateDefender Integra VPN networks



### '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 <http://www.pandasecurity.com/> and <http://www.pandasecurity.com/enterprise/support/> 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™. 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.

## CONTENTS

1	Introduction .....	3
2	VPN protocols .....	4
2.1	IPSEC VPN .....	4
2.2	L2TP VPN .....	6
2.3	SSL VPN .....	7
2.4	PPTP VPN .....	8
3	Conclusions .....	9

### Symbols and styles used in this documentation

#### Symbols used in this documentation:



**Note.** Clarification and additional information.



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



**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.

# 1 Introduction

The following document explains how to configure the corporate firewall/router located in front of GateDefender Integra so that VPN traffic reaches GateDefender Integra in the corporate network in the event that Integra is acting as a gateway in a VPN tunnel with the other device on the other side of the firewall/router.

The scenario that will be used throughout the document and which is illustrated in the diagram below, is one of the most common situations when installing Panda GateDefender Integra in router mode in a corporate network.

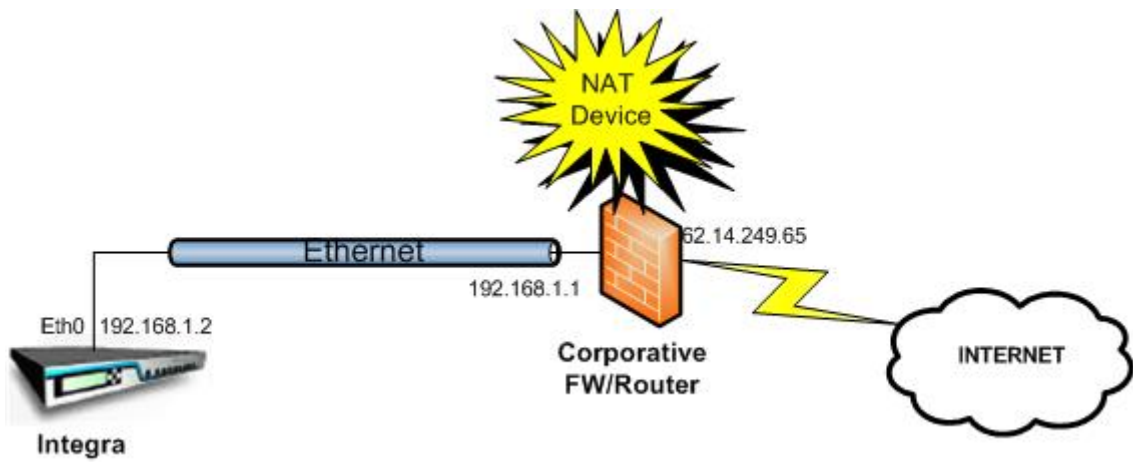


Figure 1

The Panda GateDefender Integra is located at the network entry point, just behind the corporate firewall/router.

The device that is located in front of the GateDefender Integra unit, either firewall or router, can be applying security policies that control inbound/outbound traffic.

Normally, GateDefender Integra will have a private IP address assigned and the corporate firewall/router will use the NAT protocol to direct all internal traffic on to the Internet. In this situation, the corporate network has a single public IP address (external interface of the firewall). In the case of the diagram, the IP address is: 62.14.249.65

In this case, if Integra is acting as a VPN gateway, VPN network packets that reach the public IP address of the external router/firewall interface (62.14.249.65) have to be redirected to the Integra VPN Gateway protected by the NAT router/firewall.

Therefore, for the VPN tunnels to be established correctly from Panda GateDefender Integra, ports will have to be statically mapped, also known as **Destination Nat** or **Port Forwarding** in the NAT device (corporate router/firewall).

Below you'll find the ports and protocols that need to be mapped in the corporate firewall/router to the Integra private IP address (in the diagram, 192.168.1.2).

## 2 VPN protocols

### 2.1 IPSEC VPN

In this scenario, Panda GateDefender Integra will be the VPN Gateway for an IPSEC tunnel. As they are protected by a NAT device, (corporate router/firewall) which translates or changes the private IP address when going out to the Internet, packets sent from the opposite end of the tunnel, (Gateway or Roadwarrior) are received in the public IP address, and have to be redirected to the private IP address of Panda GateDefender Integra, in this case 192.168.1.2.

Therefore, in the corporate router/firewall, it will be necessary to statically map traffic reaching IP 62.14.249.65 through port UDP 500 and through port UDP 4500 (if NAT-T is activated and NAT is detected) to IP 192.168.1.2 in port UDP 500 and UDP 4500 as shown in the diagram:

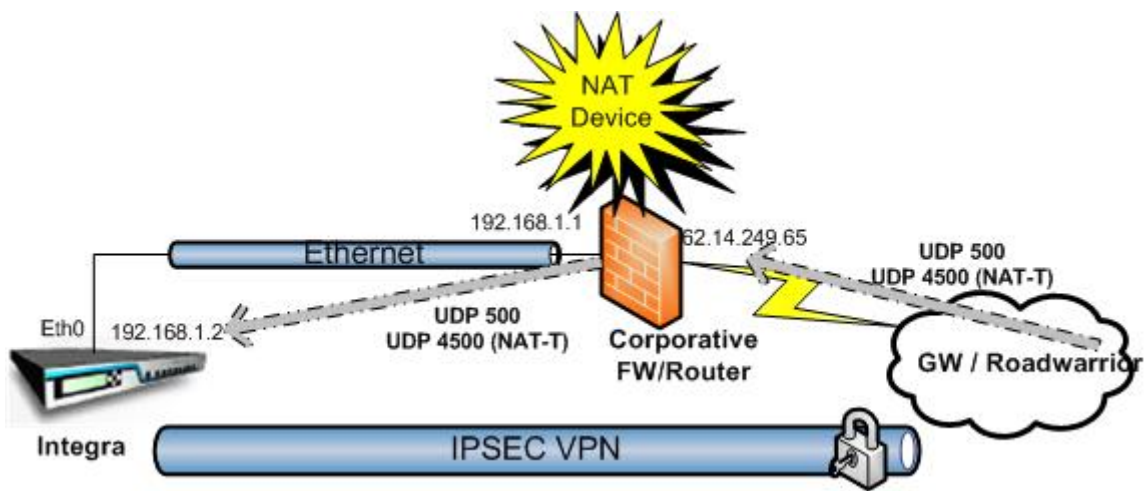


Figure 2



## 2.2 L2TP VPN

This case is very similar to the previous case. L2TP works over IPSEC, so the mapping in this case is the same as in the previous one:

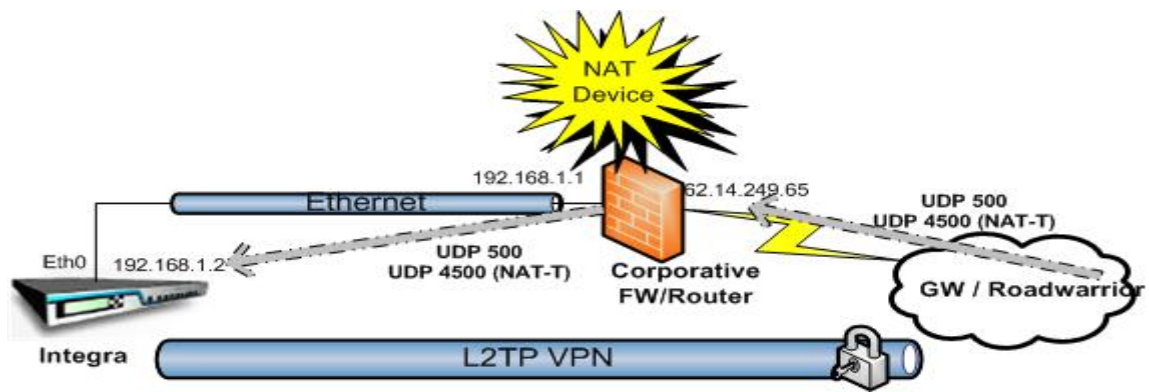


Figure 4

## 2.3 SSL VPN

Let's suppose that GateDefender Integra establishes a VPN using SSL.

Traffic in this case will only use UDP port 1194. This means all traffic received in the external interface of the router/firewall, at IP 62.14.249.65 (UDP port 1194), must be redirected to the internal IP address of Integra 192.168.1.2 in UDP port 1194.

Both in the case of Gateway-Roadwarrior architecture and Gateway-Gateway architecture, this redirecting of traffic is only carried out in the corporate router/firewall where the server is, as on the client side, it is only necessary to ensure that outbound traffic is allowed through UDP 1194.

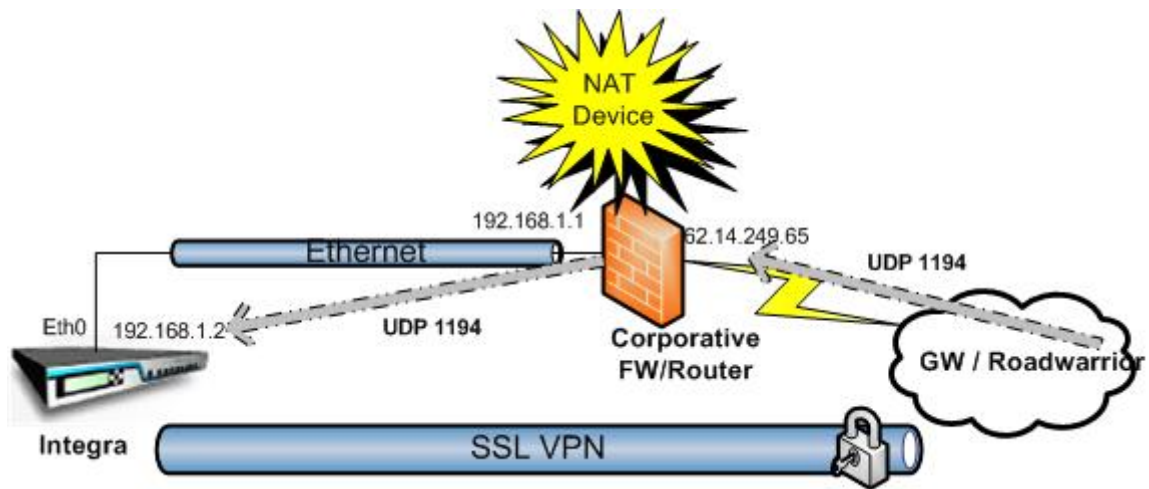



Figure 5


## 2.4 PPTP VPN

The final scenario that could occur with GateDefender Integra is that of a PPTP VPN, in which Integra acts as a VPN gateway for a Roadwarrior.

In this case, there are two different types of traffic:

- Traffic for establishing the tunnel consisting of TCP packets whose target is port 1723.
- Encrypted traffic consisted of IP 47 packets also known as **GRE** (Generic Routing Encapsulation)).

 **Note:** 47 refers to the number of the protocol and not the number of port.

 **Warning:** Bear in mind that the corporate router/firewall must have PPTP connection tracking to allow simultaneous multiple connections with the roadwarriors behind it.

In the corporate router/firewall in which the VPN Integra server is located, it will be necessary to redirect TCP 1723 traffic received in the public IP address to Integra's private address in TCP port 1173. Once you have done this, IP 47 traffic will be sent automatically to the VPN Integra server using the connection tracking of the corporate router/firewall.

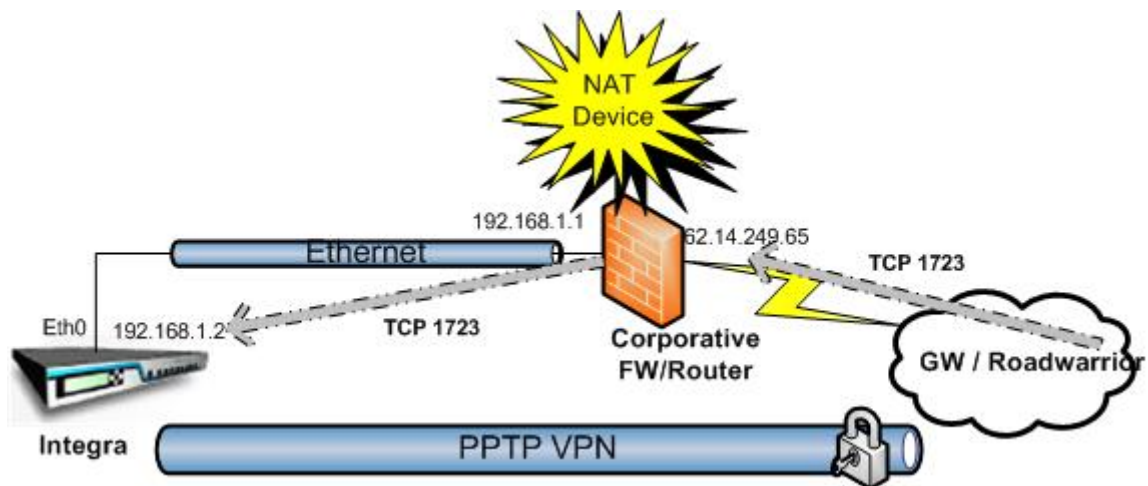


Figure 6

### 3 Conclusions

This document describes factors that have to be taken into account for the correct processing of VPN traffic from the remote Gateway/Roadwarrior when Panda GateDefender Integra is located behind a NAT device.

In order for the VPN to operate, the VPN traffic received in the public interface of the router/firewall must be redirected to the private IP address of Integra, either when it has the role of the VPN server for protocols such as PPTP or SSL, or when it operates as a gateway for protocols such as IPSEC or L2TP.

In order for the VPN network to operate correctly in this type scenario, it is not enough just to process and VPN traffic coming in from the outside, but outbound traffic must also be allowed.