

## HowTo: What ports have to be opened in the corporate firewall/router when Panda GateDefender Integra acts as a VPN Gateway



### **'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 .....	5
2.3	SSL VPN .....	5
2.4	PPTP VPN .....	6
3	Conclusions .....	7

### 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.

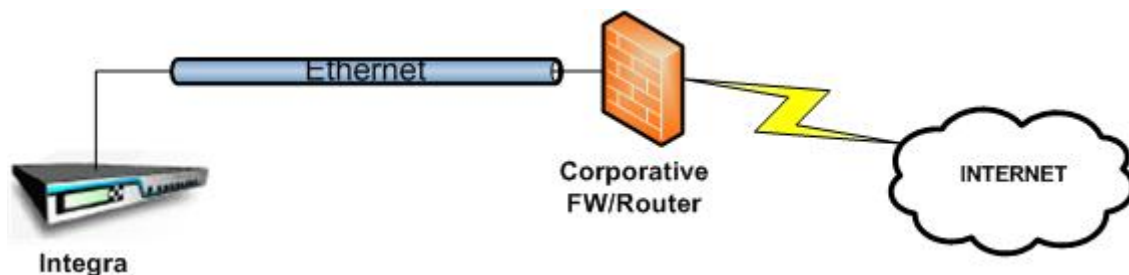
*Codes style:* Names of files, extensions, folders, command line information or configuration files, for example, scripts.

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

## 1 Introduction

This document explains how to configure the corporate firewall/router located in front of GateDefender Integra in order to allow outbound VPN traffic when Integra acts as a gateway.

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



The Panda GateDefender Integra unit 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 apply security policies that control inbound/outbound traffic. In this case, if Integra acts as a VPN Gateway, you must ensure that certain outbound traffic is allowed in order to be able to establish and use the VPN network, depending on the protocol configured for the tunnels.

Below we describe the ports and protocols that will need to be opened in the corporate firewall/router.

### [Contents](#)

---

## 2 VPN protocols

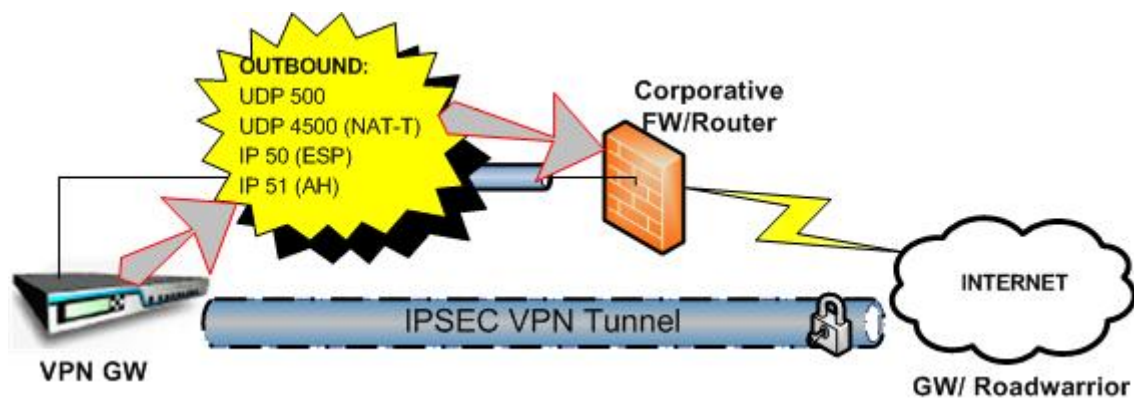
### 2.1 IPSEC VPN

In this first case, GateDefender Integra will establish an IPSEC VPN tunnel with a remote device, either GW-GW (gateway-gateway) or GW-RW (gateway-roadwarrior).

In order to establish and use the tunnel correctly, the following ports have to be opened in the corporate firewall/router to allow outbound traffic from GateDefender Integra:

- UDP 500 to establish the tunnel.
- Protocol IP 50 if using ESP (Encapsulating Security Payload), or protocol IP 51 if using AH (Authentication Header).
- If using NAT-T (Nat transversal) in those cases where it is necessary, UDP 4500 packets should be used in addition to UDP 500 packets.

The following diagram illustrates this scenario:



### [Contents](#)

---

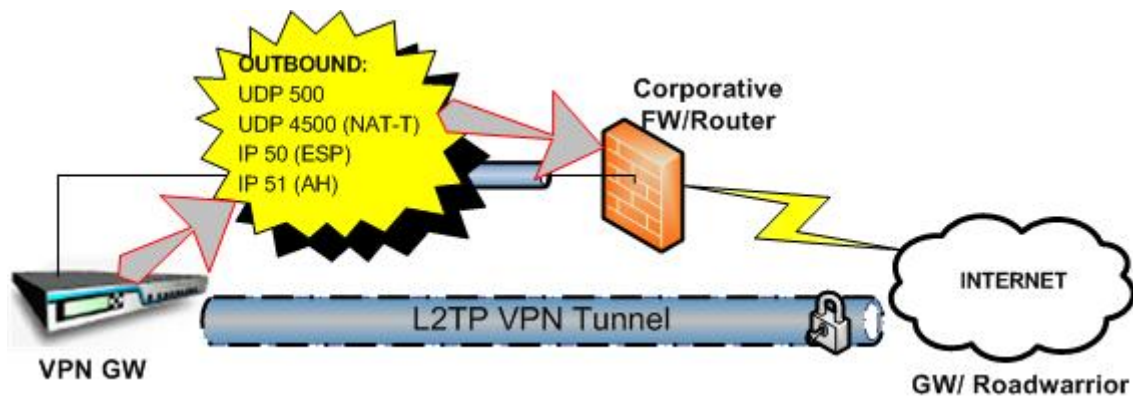
## 2.2 L2TP VPN

The setup for L2TP is similar to the previous case, as L2TP operates over IPSEC.

Therefore, the ports that will have to be opened in the corporate firewall/router for the L2TP VPN to operate correctly are as follows:

- UDP 500 to establish the tunnel.
- Protocol IP 50 if using ESP (Encapsulating Security Payload), or protocol IP 51 if using AH (Authentication Header).
- If using NAT-T (Nat transversal) in those cases where it is necessary, UDP 4500 packets should be used in addition to UDP 500 packets.

The following diagram illustrates this scenario:



### [Contents](#)

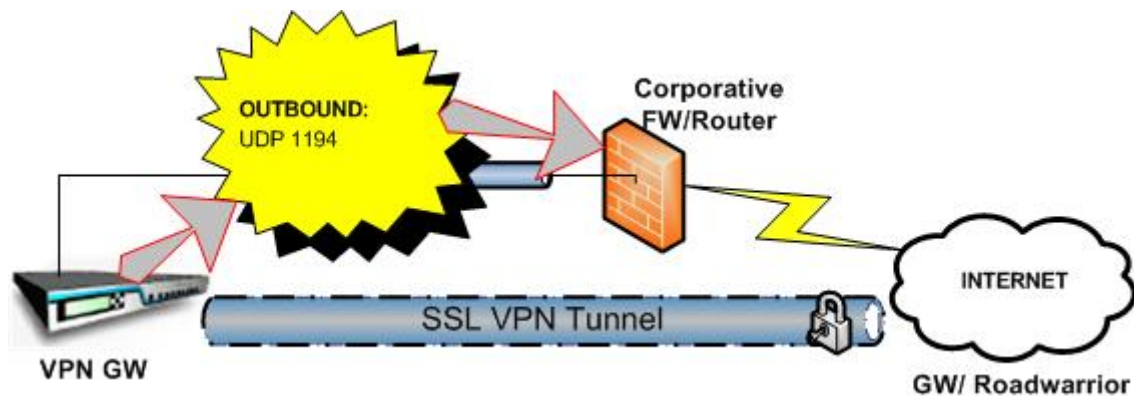
---

## 2.3 SSL VPN

The case of the SSL protocol is simpler than that of IPSEC.

For the SSL VPN to operate correctly, it is only necessary to allow one type of outbound packet: UDP 1194.

Therefore, the corporate firewall/router security policy must allow these outbound packets:



[Contents](#)

---

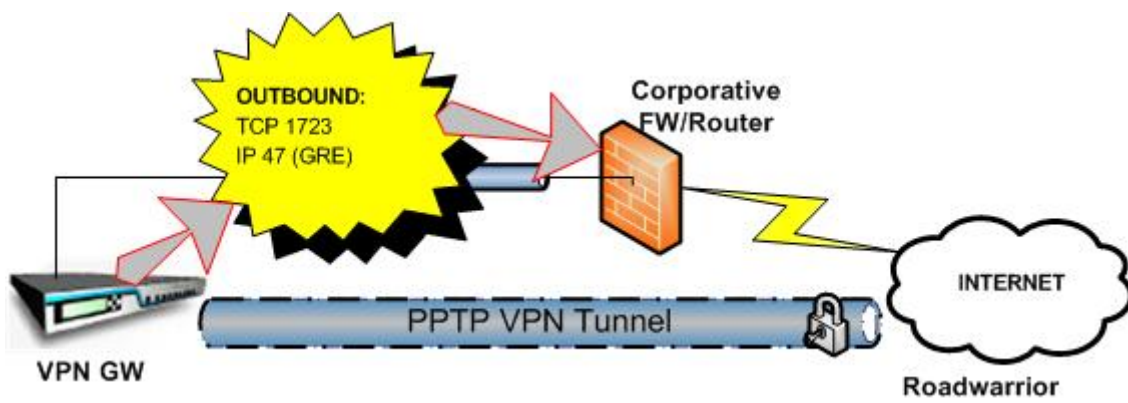
## 2.4 PPTP VPN

The PPTP protocol uses two different packets in order to implement the tunnels:

- TCP 1723 for the control channel
- IP 47 (GRE) for the data channel

For the tunnel to operate correctly these packets must pass through the corporate router/firewall.

The following diagram illustrates this scenario:



[Contents](#)

---

### 3 Conclusions

This document demonstrates how to configure the corporate router/firewall in order not to block VPN packets in the event that security policies are applying restrictions on outbound traffic.

If the security policies are implemented by Integra and no other device is restricting traffic, it is not necessary to apply these configurations in the Integra firewall, as the VPN enters the necessary rules in its own system to allow these outbound packets.

 **NOTE: With the VPN configuration, Integra prepares its firewall so the VPN can be established. However, it is necessary afterwards to define adequate rules if you want to apply security policies to the VPN traffic once it has been decrypted.**

For the VPN network to operate correctly, in addition to allowing certain outbound traffic for each scenario, additional configuration may be necessary to apply to inbound packets.

[Contents](#)

---