HOWTO: How to configure the firewall for VPNs

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

Copyright notice

Registered Trademarks

CONTENTS

1. INTRODUCTION 3
2. CONFIGURING THE FIREWALL 4
2.1 IPSEC VPN 4
2.1.1 *Gateway-to-gateway* *4*
2.1.2 *Gateway-to-Roadwarrior* *8*
2.2 L2TP VPN 10
2.3 PPTP VPN 12
2.4 SSL VPN 14
2.4.1 *Gateway-to-gateway* 14
2.4.2 *Gateway-to-Roadwarrior* 17

Conventions used in this document:

Icons used in this document:

Note. Provides additional information and useful data.

Important. Highlights the importance of a concept.

Tip. Useful ideas to help you get the most out of the program.

Reference. Other points that offer more information that you might find useful.

Fonts and styles used in this document:

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

Code: Names of files, extensions, folders, commandline information or configuration files such as scripts.

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

1. Introduction

Panda GateDefender Integra includes a VPN module, which you can use to setup VPNs in Gateway-to-Gateway and Gateway-to-Roadwarrior architectures.

You can use any of the following protocols to establish the tunnel: PPTP, L2TP, SSL, and IPsec.

After you have configured the VPN, Panda GateDefender will automatically adjust the firewall to ensure that the ports required to establish the tunnel with the other side are open and available. The necessary rules are included in the system totally transparently to the user, and they will not even be displayed in the console.

Even though the tunnel is established without needing to configure the firewall, after the encrypted traffic that reaches Integra has passed through the VPN module and has been decrypted, it will be sent back to the firewall. The firewall then applies the filtering rules configured by the user in the web console.

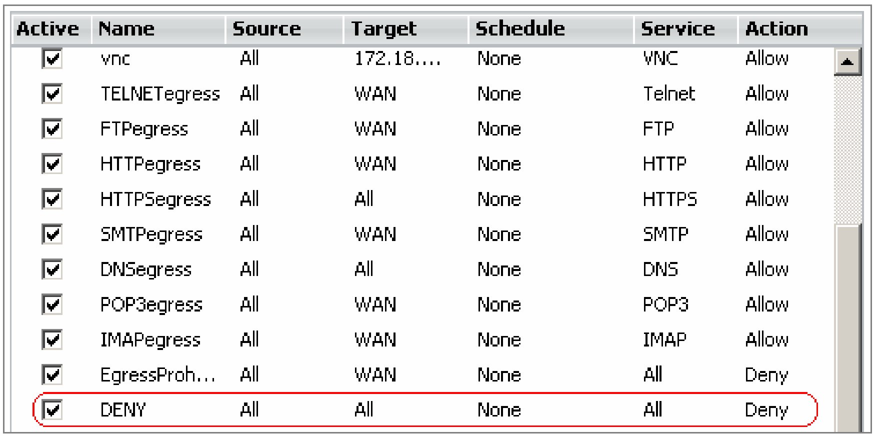
⚠ **IMPORTANT:** Therefore, you must define a specific configuration for user traffic to circulate through the tunnel.

This document explains how the GateDefender Integra firewall must be configured when VPNs (Virtual Private Networks) are used and Panda GateDefender Integra is involved in setting up the tunnels, as a VPN server or as a client, so that the traffic sent to the tunnel is not filtered.

Contents

2. Configuring the firewall

The definition of how the firewall must be configured is based on the fact that the default firewall policy is **Deny**. This policy is included in the factory settings of Panda GateDefender Integra:



Active	Name	Source	Target	Schedule	Service	Action
☑	vnc	All	172.18....	None	VNC	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	All	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	All	None	DNS	Allow
☑	POP3egress	All	WAN	None	POP3	Allow
☑	IMAPegress	All	WAN	None	IMAP	Allow
☑	EgressProh...	All	WAN	None	All	Deny
☑	DENY	All	All	None	All	Deny

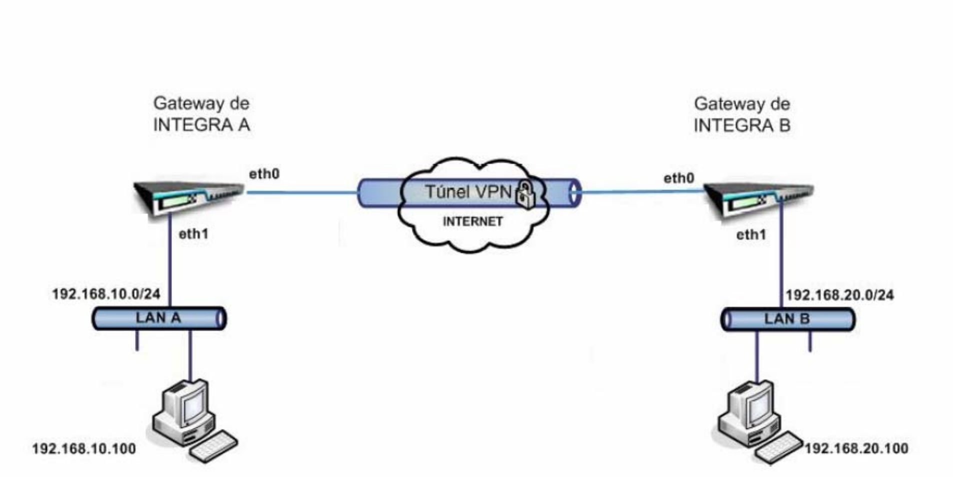
Therefore, this rule is left as a low priority rule (situated at the bottom of the filtering rules list). When configuring a VPN, you must enter the higher priority filtering rules that allow and do not deny the "real" traffic transmitted in the VPN's encrypted packets.

2.1 IPsec VPN

Panda GateDefender Integra allows you to implement two different architectures for this protocol:

Gateway (office)-to-gateway (office), and Gateway (office)-Roadwarrior:

2.1.1 Gateway-to-gateway



In the scenario in the diagram, an IPsec tunnel is established between two Panda GateDefender Integra appliances.

In both appliances, various address ranges that include the local and remote address ranges have been previously defined from the **Definitions** menu:

Integra A: Local_A= 192.168.10.0/24
Remote_B= 192.168.20.0/24

Integra B: Local_B= 192.168.20.0/24
Remote_A= 192.168.10.0/24

For LAN A to be able to reach LAN B, you must not only establish the tunnel that securely connects them via the Internet, but also configure the firewall with the appropriate rules.

- **Case 1: LAN A wants to access LAN B**

The following filtering policies must be configured:

Integra A: **Allow** the traffic from the **source** *LanA* to the **target** *LanB* for the required services.

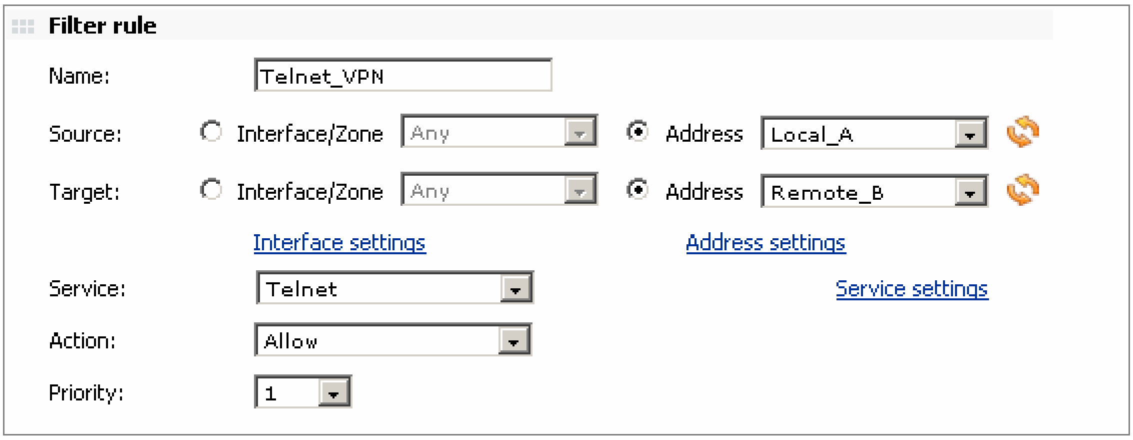
Integra B: **Allow** the traffic from the **source** *LanA* to the **target** *LanB* for the required services.

Note: You do not need to enable an explicit rule in the firewall to allow the responses to the sessions already established with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

Example: Which rules must be added to the firewalls in both Integra appliances for the host of network A (192.168.10.100) to reach the host of network B via Telnet (TCP 23)?

Solution:

Integra A firewall:



Filter rule

Name: Telnet_VPN

Source: ○ Interface/Zone Any ● Address Local_A

Target: ○ Interface/Zone Any ● Address Remote_B

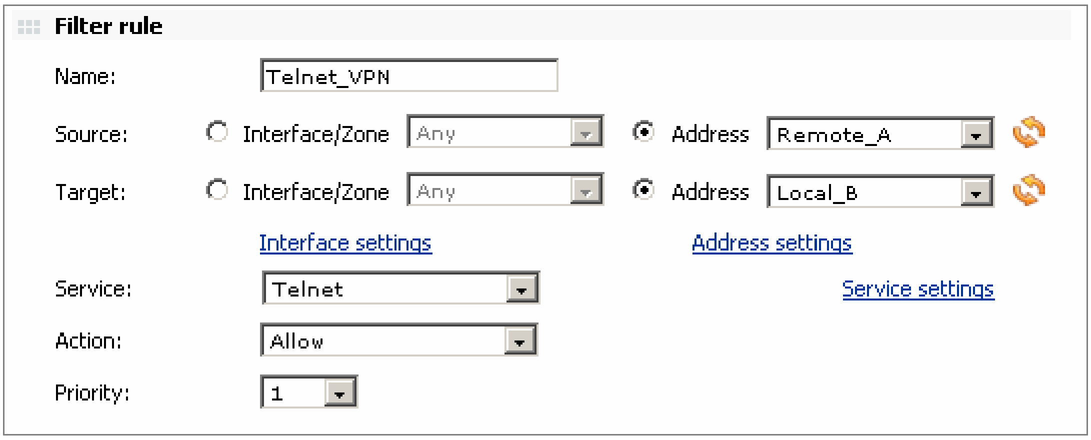
Interface settings Address settings

Service: Telnet Service settings

Action: Allow

Priority: 1

Integra B firewall:



Filter rule

Name: Telnet_VPN

Source: ○ Interface/Zone Any ● Address Remote_A

Target: ○ Interface/Zone Any ● Address Local_B

Interface settings Address settings

Service: Telnet Service settings

Action: Allow

Priority: 1

These rules will allow the host of local network A to access the host of network B via Telnet.

- **Case 2: LAN B wants to access LAN A**

The following filtering policies must be configured:

Integra B: **Allow** the traffic from the **source** *LANB* to the **target** *LANA* for the required services.

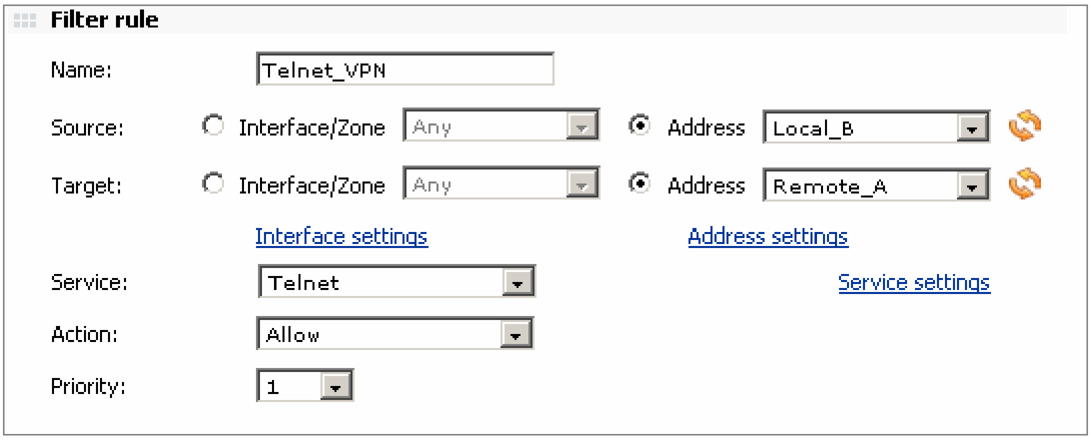
Integra A: **Allow** the traffic from the **source** *LANB* to the **target** *LANA* for the required services.

Example:

To access the host of network A from the host of network B via Telnet, you must change the source and target of the packets compared to the previous example:

Solution:

Integra B firewall:



Filter rule

Name: Telnet_VPN

Source: ○ Interface/Zone Any ● Address Local_B

Target: ○ Interface/Zone Any ● Address Remote_A

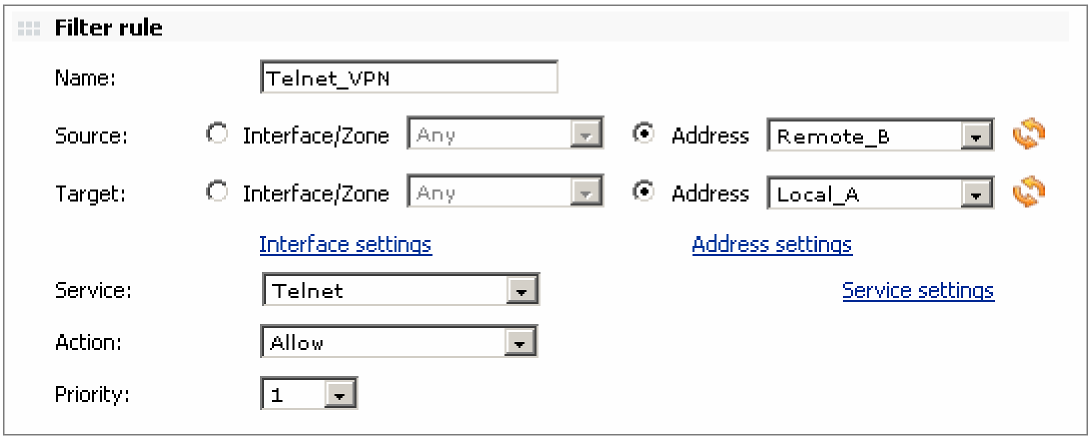
Interface settings Address settings

Service: Telnet Service settings

Action: Allow

Priority: 1

Integra A firewall:

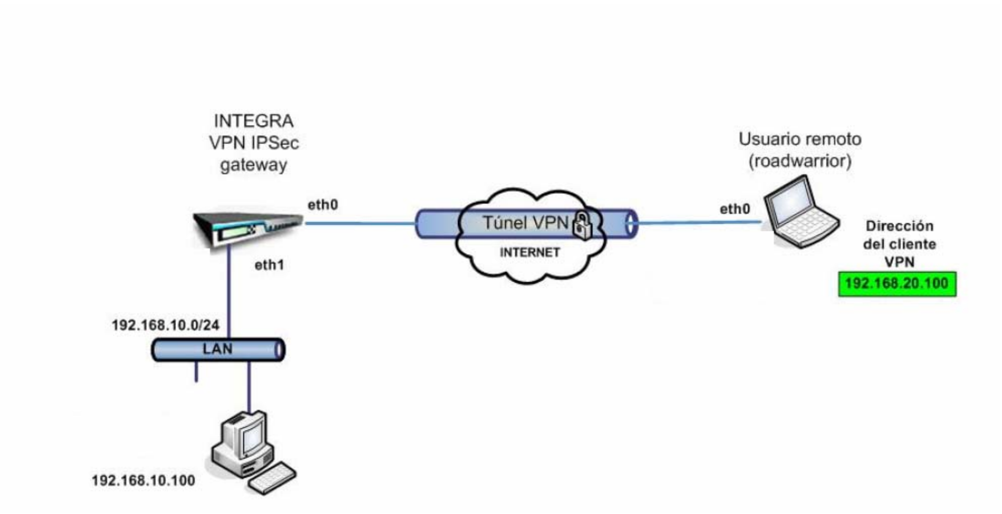


Filter rule

Name:	Telnet_VPN	
Source:	○ Interface/Zone Any	● Address Remote_B
Target:	○ Interface/Zone Any	● Address Local_A
	Interface settings	Address settings
Service:	Telnet	Service settings
Action:	Allow	
Priority:	1	

Contents

2.1.2 Gateway-to-Roadwarrior



In the scenario in the diagram, a Panda GateDefender Integra appliance acts as a VPN server for remote clients (roadwarriors) between which an IPsec tunnel has just been established.

In the case of IPsec, the roadwarrior accesses the local VPN with the real IP address assigned to it in its own network, usually a private IP address. As these IP addresses will be used in the local LAN of the VPN server, these addresses must be used to establish the security policies.

Note: To check the IP address of each roadwarrior, access the **VPN monitor submenu** from the **VPN menu** in the web console.

To simplify management of the firewall rules, the following address ranges are defined from the **Definitions menu** in Integra:

- Virtual_IPSEC = 192.168.20.10 (for the example in the diagram)
- Local=192.168.10.0/24

If you want to allow the roadwarrior to access the local network with certain services, once the VPN tunnel has been established with the IPsec VPN server, you need to configure the Panda GateDefender Integra security policies in the following way:

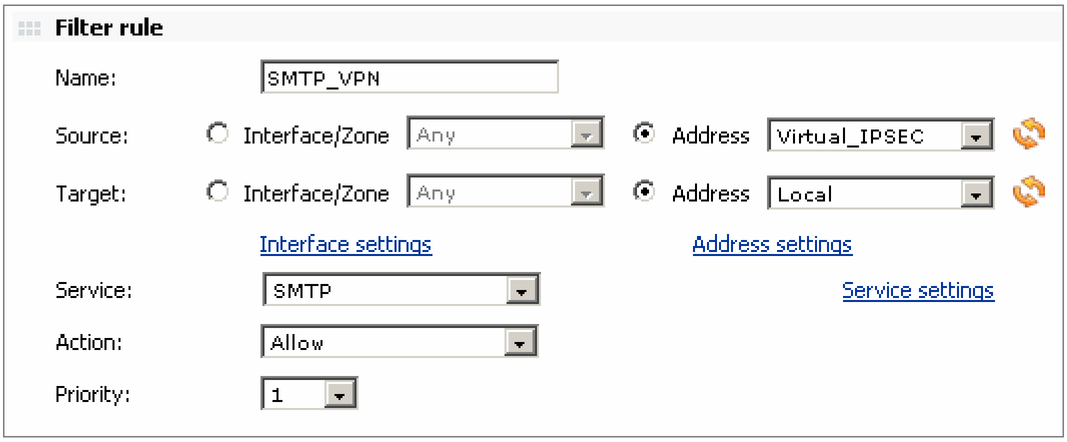
> Integra: **Allow** the traffic from the **source** *roadwarrior* to the **target** *Lan* for the required services.

Note: You do not need to enable an explicit rule in the firewall to allow the responses to the sessions already established with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

Example: Which rules need to be added to the Integra firewall for the roadwarrior to be able to access the local network of Integra via SMTP (TCP 25)?

Solution:

Integra firewall:



Filter rule

Name: SMTP_VPN

Source: ○ Interface/Zone Any ● Address Virtual_IPSEC

Target: ○ Interface/Zone Any ● Address Local

Interface settings Address settings

Service: SMTP Service settings

Action: Allow

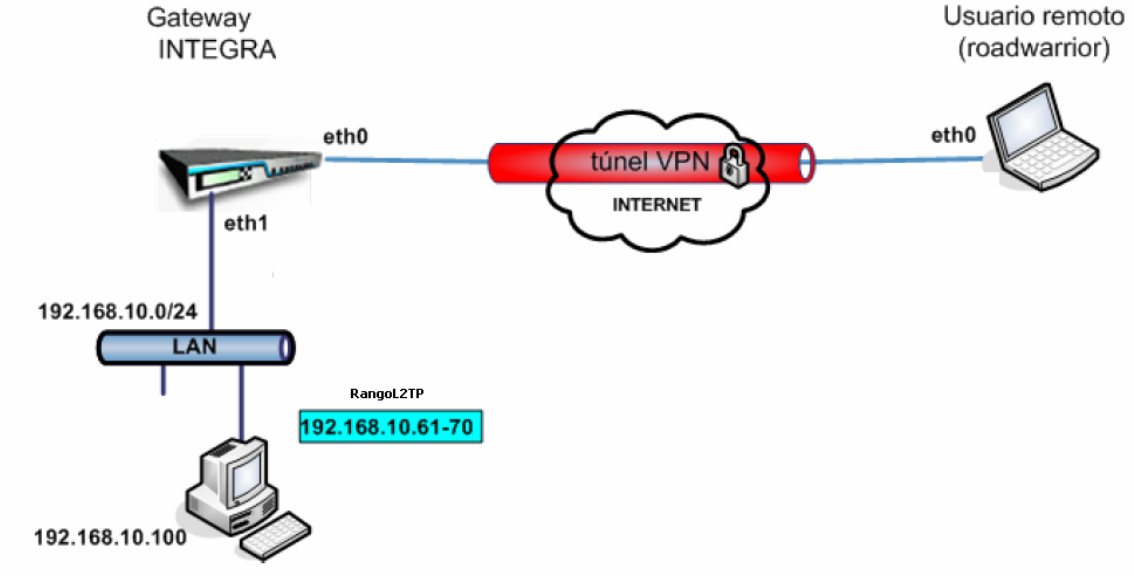
Priority: 1

Contents

2.2 L2TP VPN

Panda GateDefender Integra allows you to implement one architecture for this protocol:

Gateway (office)-to-Roadwarrior:



In the scenario in the diagram, a Panda GateDefender Integra appliance acts as a VPN server for remote clients (roadwarriors) between which an L2TP tunnel has just been established.

The L2TP address range (see diagram) will be used to assign IP addresses to the roadwarriors that connect to the server. These IP addresses will be used in the local network of the VPN server.

Note: To check the IP address assigned to each roadwarrior, access the **VPN monitor submenu** from the **VPN menu** in the web console.

To simplify management of the firewall rules, the following address ranges are defined from the **Definitions menu** in Integra:

- Range_L2TP = 192.168.10.61-70
- Local=192.168.10.0/24

If you want to allow the roadwarrior to access the local network with certain services, once the VPN tunnel has been established with the L2TP VPN server, you need to configure the Panda GateDefender Integra security policies in the following way:

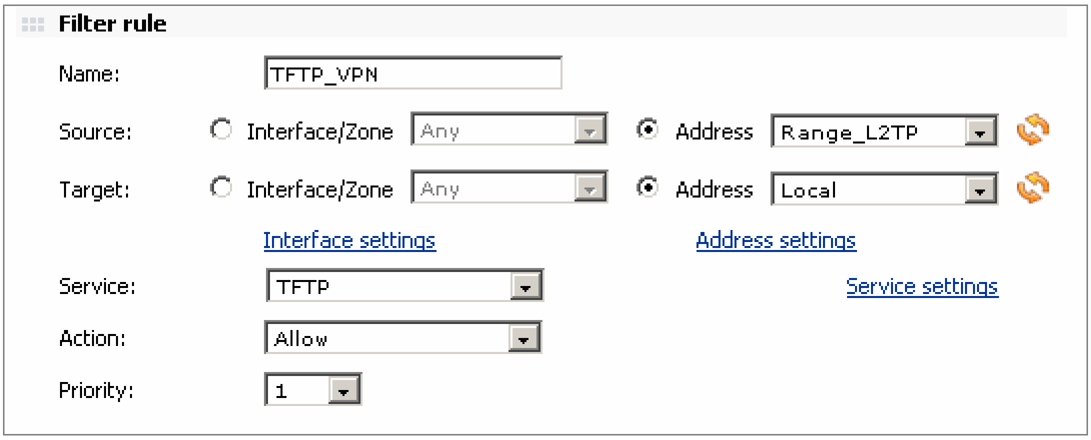
> Integra: **Allow** the traffic from the **source** *roadwarrior* to the **target** *Lan* for the required services.

Note: You do not need to explicitly enable the return to the same session with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

Example: Which rules need to be added to the Integra firewall for the roadwarrior to be able to access the local network of Integra via TFTP (UDP 69)?

Solution:

Integra firewall:



Filter rule

Name: TFTP_VPN

Source: ○ Interface/Zone Any ● Address Range_L2TP

Target: ○ Interface/Zone Any ● Address Local

Service: TFTP

Action: Allow

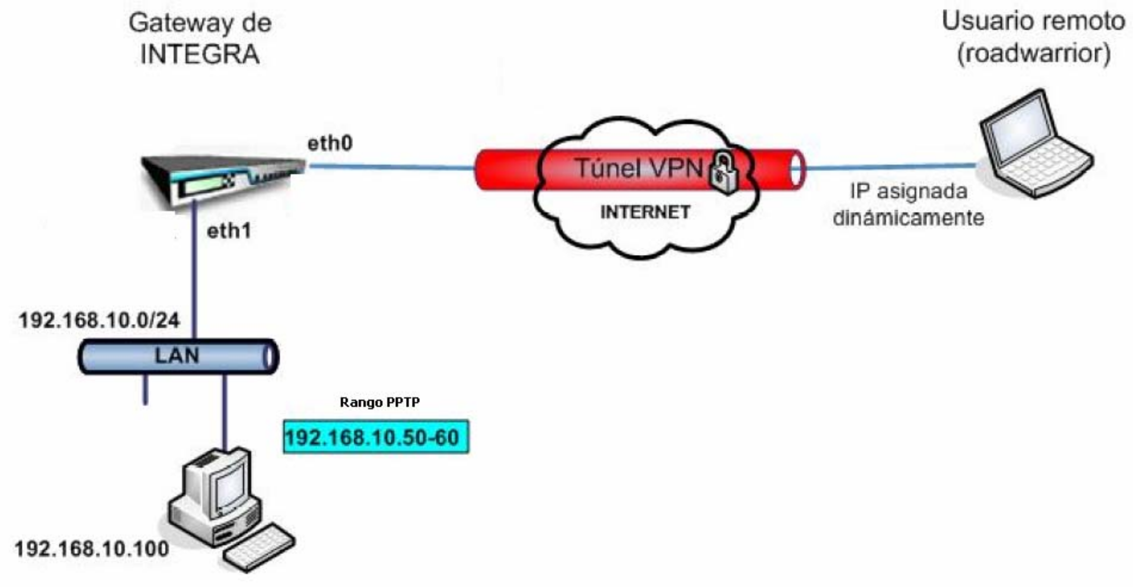
Priority: 1

[Contents](#)

2.3 PPTP VPN

Panda GateDefender Integra allows you to implement one architecture for this protocol:

Gateway (office)-to-Roadwarrior:



We will use the scenario in the diagram as an example, where a Panda GateDefender Integra appliance acts as a VPN server for remote clients (roadwarriors) between which a PPTP tunnel has just been established.

The PPTP address range (see diagram) will be used to assign IP addresses to the roadwarriors that connect to the server. These IP addresses will be used in the local network of the VPN server.

Note: To check the IP address assigned to each roadwarrior, access the **VPN monitor submenu** from the **VPN menu** in the web console.

To simplify management of the firewall rules, the following address ranges are defined from the **Definitions menu** in Integra:

- Range_PPTP= 192.168.10.50-60
- Local=192.168.10.0/24

If you want to allow the roadwarrior to access the local network with certain services, once the VPN tunnel has been established with the PPTP VPN server, you need to configure the Panda GateDefender Integra security policies in the following way:

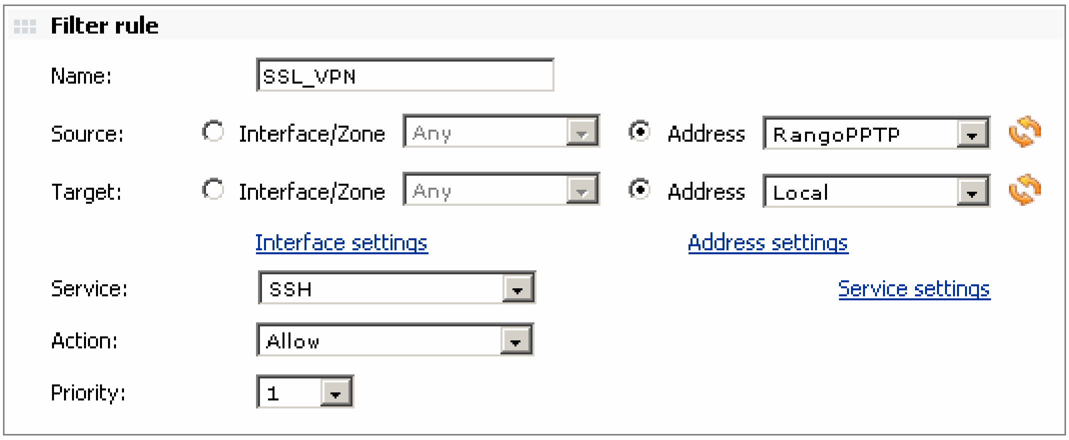
> Integra: **Allow** the traffic from the **source** *roadwarrior* to the **target** *Lan* for the required services.

Note: You do not need to enable an explicit rule in the firewall to allow the responses to the sessions already established with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

<u>Example</u>: Which rules need to be added to the Integra firewall for the roadwarrior to be able to access the local network of Integra via SSH (TCP 22)?

<u>Solution:</u>

Integra firewall:



Filter rule

Name: SSL_VPN

Source: ○ Interface/Zone Any ● Address RangoPPTP

Target: ○ Interface/Zone Any ● Address Local

Interface settings Address settings

Service: SSH Service settings

Action: Allow

Priority: 1

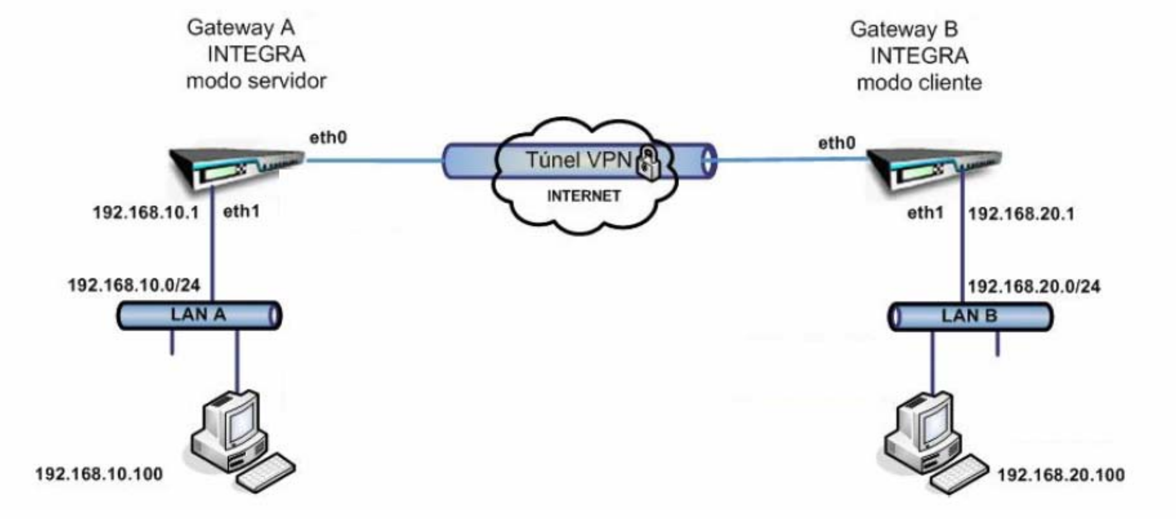
Contents

2.4 SSL VPN

Panda GateDefender Integra allows you to implement two different architectures for this protocol:

Gateway (office)-to-gateway (office), and Gateway (office)-Roadwarrior:

2.4.1 Gateway-to-gateway



This will be the scenario in the diagram, where there are two Panda GateDefender Integra appliances between which an SSL tunnel has just been established.

In both appliances, various address ranges that include the local and remote address ranges have been previously defined from the **Definitions** menu:

Integra A:

Local_A= 192.168.10.0/24
Remote_B= 192.168.20.0/24

Integra B:

Local_B= 192.168.20.0/24
Remote_A= 192.168.10.0/24

For LAN A to be able to reach LAN B, you must not only establish the tunnel that securely connects them via the Internet, but you must also configure the firewall with the appropriate rules.

- Case 1: LAN A wants to access LAN B

The following filtering policies must be configured:

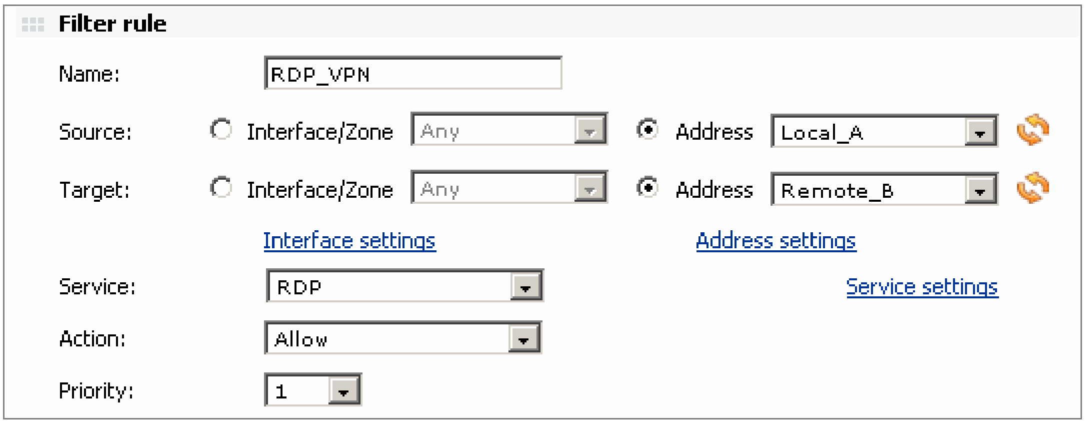
Integra A: **Allow** the traffic from the **source** *LANA* to the **target** *LANB* for the required services.
Integra B: **Allow** the traffic from the **source** *LANA* to the **target** *LANB* for the required services.

Note: You do not need to enable an explicit rule in the firewall to allow the responses to the sessions already established with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

Example: Which rules must be added to the firewalls in both Integra appliances for the host of network A (192.168.10.100) to reach the host of network B via RDP (TCP 3389)?

Solution:

Integra A firewall:



Filter rule

Name: RDP_VPN

Source: ○ Interface/Zone Any ● Address Local_A

Target: ○ Interface/Zone Any ● Address Remote_B

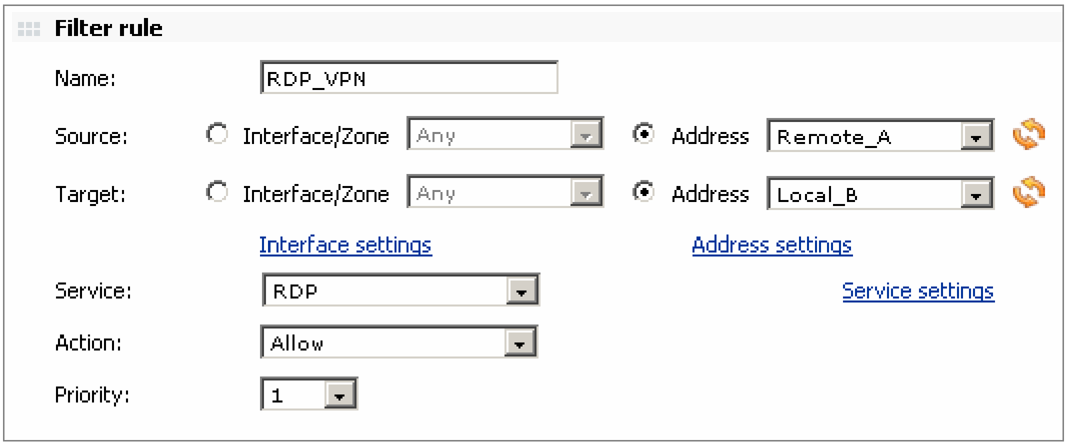
Interface settings Address settings

Service: RDP Service settings

Action: Allow

Priority: 1

Integra B firewall:



Filter rule

Name: RDP_VPN

Source: ○ Interface/Zone Any ● Address Remote_A

Target: ○ Interface/Zone Any ● Address Local_B

Interface settings Address settings

Service: RDP Service settings

Action: Allow

Priority: 1

These rules will allow the host of local network A to access the host of network B via RDP.

- **Case 2: LAN B wants to access LAN A**

The following filtering policies must be configured:

Integra B: **Allow** the traffic from the **source** *lanB* to the **target** *LanA* for the required services.

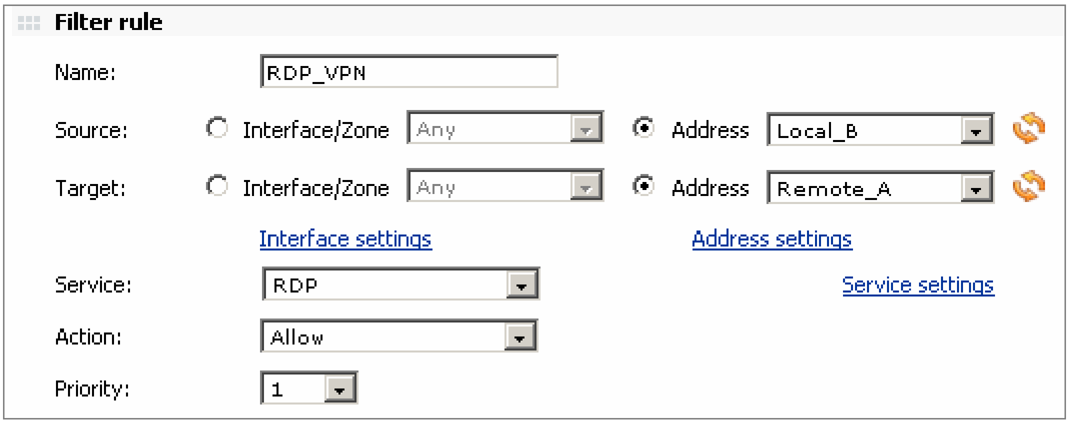
Integra A: **Allow** the traffic from the **source** *LanB* to the **target** *LanA* for the required services.

Example:

To access the host of network A from the host of network B via RDP, you must change the source and target of the packets compared to the previous example:

Solution:

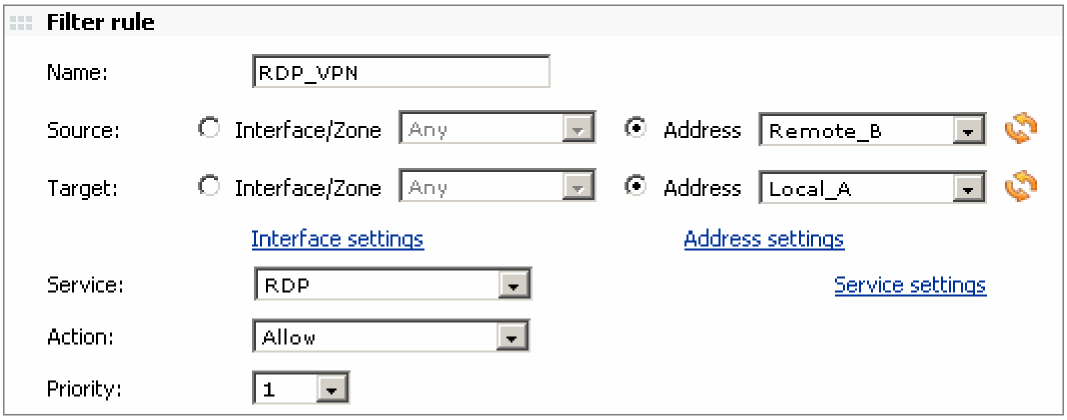
Integra B firewall:



Filter rule

Name:	RDP_VPN			
Source:	○ Interface/Zone	Any	● Address	Local_B
Target:	○ Interface/Zone	Any	● Address	Remote_A
	Interface settings		Address settings	
Service:	RDP			Service settings
Action:	Allow			
Priority:	1			

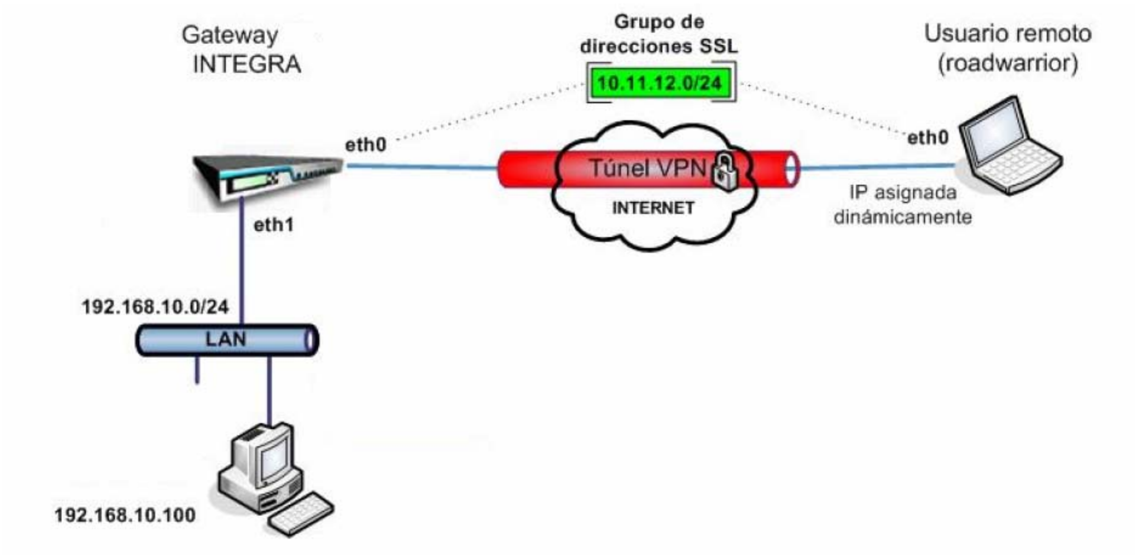
Integra A firewall:



Filter rule

Name:	RDP_VPN			
Source:	○ Interface/Zone	Any	● Address	Remote_B
Target:	○ Interface/Zone	Any	● Address	Local_A
	Interface settings		Address settings	
Service:	RDP			Service settings
Action:	Allow			
Priority:	1			

2.4.2 Gateway-to-Roadwarrior



In the scenario in the diagram, a Panda GateDefender Integra appliance acts as a VPN server for remote clients (roadwarriors) between which an SSL tunnel has just been established.

The SSL address range (see diagram) will be used to assign virtual IP addresses to the roadwarriors that connect to the server. These IP addresses will be used in the local network of the VPN server.

Note: To check the IP address assigned to each roadwarrior, access the **VPN monitor submenu** from the **VPN menu** in the web console.

To simplify management of the firewall rules, the following address ranges are defined from the **Definitions menu** in Integra:

- Virtual_SSL= 10.11.12.0/24
- Local=192.168.10.0/24

If you want to allow the roadwarrior to access the local network with certain services, once the VPN tunnel has been established with the SSL VPN server, you need to configure the Integra security policies in the following way:

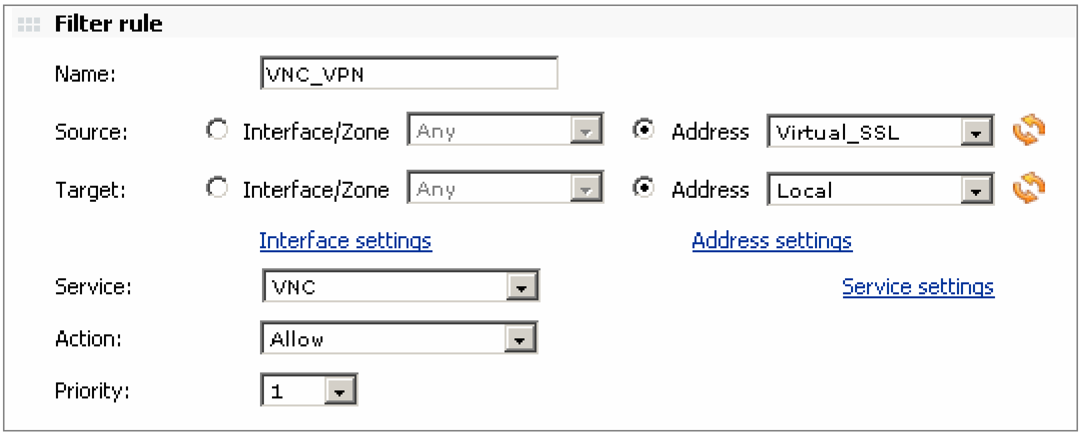
> Integra: **Allow** the traffic from the **source** *roadwarrior* to the **target** *Lan* for the required services.

Note: You do not need to enable an explicit rule in the firewall to allow the responses to the sessions already established with the inverse filtering rules, as Integra includes the Connection tracking option that will take care of this.

Example: Which rules need to be added to the Integra firewall for the roadwarrior to be able to access the local network of Integra via VNC (TCP 5900)?

Solution:

Integra firewall:



Filter rule

Name: VNC_VPN

Source: ○ Interface/Zone Any ● Address Virtual_SSL

Target: ○ Interface/Zone Any ● Address Local

Interface settings Address settings

Service: VNC Service settings

Action: Allow

Priority: 1

Contents