

HOWTO: Practical guide to configuring high availability in Panda GateDefender Integra



'How-to' guides for configuring high availability in GateDefender Integra

Panda Software 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 www.pandasoftware.com/product and www.pandasoftware.com/support for more information.

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 Software 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 Software, c/ Buenos Aires, 12 48001 Bilbao (Biscay) Spain.

Registered trademarks

Panda Software is a trademark or registered trademark belonging to Panda Software. Windows is a trademark or registered trademark of the Microsoft Corporation. Other product names that are mentioned in this guide may be registered trademarks of their respective owners.

INDEX

1	INTRODUCTION	3
2	HIGH AVAILABILITY	3
2.1	PREPARE THE SCENARIO	3
2.2	CLUSTER OF TWO INTEGRA APPLIANCES	5
2.3	STEP 1: CONFIGURE THE MASTER APPLIANCE	6
2.4	STEP 2: CONFIGURE THE SLAVE APPLIANCE	8
2.5	STEP 3: SET UP THE CLUSTER	10

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 is a practical guide to configuring high availability in Panda GateDefender Integra. It describes, step by step, how to prepare the scenario, how to configure the master appliance, how to configure the slave appliance, and how to set up the cluster between the two.

2 High availability

2.1 Prepare the scenario

In this scenario, Panda GateDefender Integra is placed between the network perimeter, offering its security services to both the LAN and the DMZ:

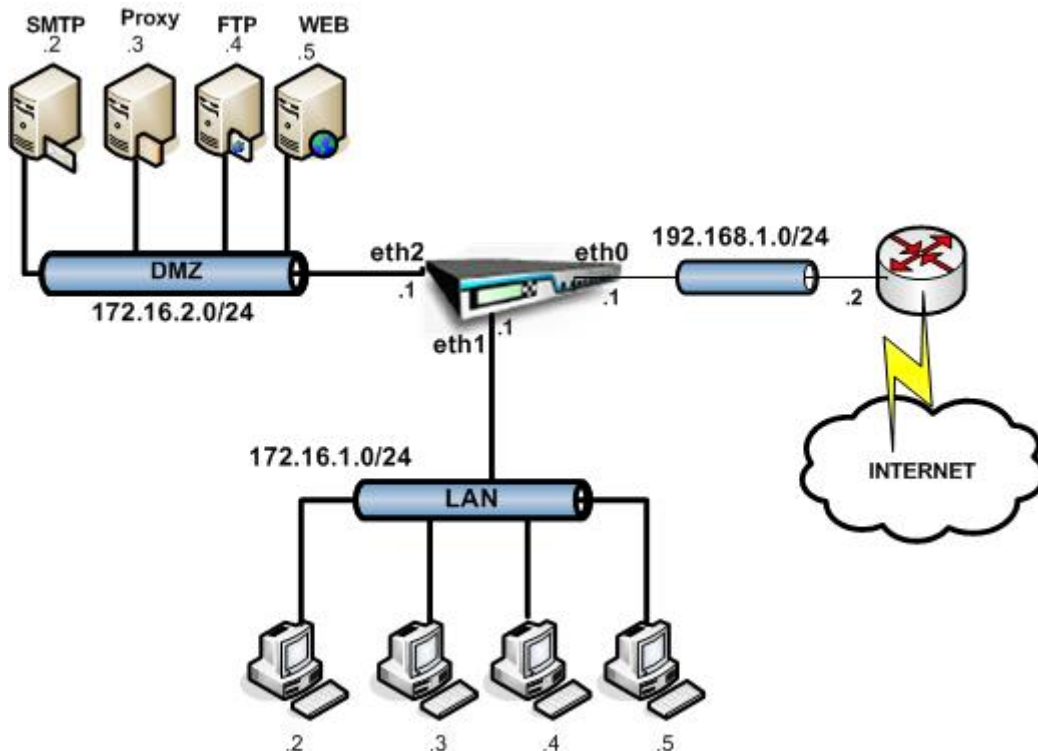


Figure 1: Panda GateDefender Integra placed in the network perimeter

In this context, only three network interface cards are configured in Integra: Eth0 (Wan), Eth1 (LAN) and Eth2 (DMZ). The rest of the network interface cards are not used and therefore, you do not need to configure them. For this reason, **you should disable them from the web console**. This will prevent problems when configuring high availability.

GateDefender Integra has been configured to access the Internet through the router that appears in the diagram, which will be used as the outbound gateway. This router will perform NAT for the private address range 192.168.1.0/24 for connecting to the Internet.

Furthermore, the rest of the necessary network parameters have also been configured:

- Eth0 (WAN): 192.168.1.1/24
- Eth1 (LAN): 172.16.1.1/24
- Eth2 (DMZ): 172.16.2.1/24
- Gateway: 192.168.1.2/24

The following IP address has been assigned to access the administration console, which is only accessible from the Eth1 network interface card:

- Configuration IP: 10.0.0.1/24

With this configuration, Panda GateDefender Integra has been correctly registered and its protection units will update periodically.

Then, you must configure the **security policies through the firewall module**. To do this, add the filter rules that allow authorized inbound and outbound traffic, and SNAT and DNAT rules, if necessary.

You must also configure the IPS module and the VPN module, if you want to establish virtual tunnels.

Finally, configure the filter modules available in the appliance:

- Anti-malware
- Anti-spam
- Content-filter
- Web Filtering

If you want to configure any additional features, such as the warnings or definitions, you can do so now or when the cluster is in operation. However, these options must be configured in the GateDefender Integra appliance with the master role.

After defining the basic configuration of GateDefender Integra, the rest of the corporate network can start operating as normal.

From now on, GateDefender will become the outbound gateway for both the LAN and the DMZ.

For example:

- Typical network configuration of a device in the LAN:

Network IP: 172.16.1.2/24
Gateway: 172.16.1.1

The devices in the DMZ will use the Integra eth2 network interface card as the outbound gateway.

- Typical network configuration of a device in the DMZ, for example, a mail server:

Network IP: 172.16.2.2/24
Gateway: 172.16.2.1

[Content](#)

2.2 Cluster of two Integra appliances

At this point, GateDefender Integra is configured and integrated, functioning correctly within the corporate network and a second GateDefender Integra appliance needs to be incorporated to add high availability characteristics to the perimeter protection.

The final structure is shown in the following diagram:

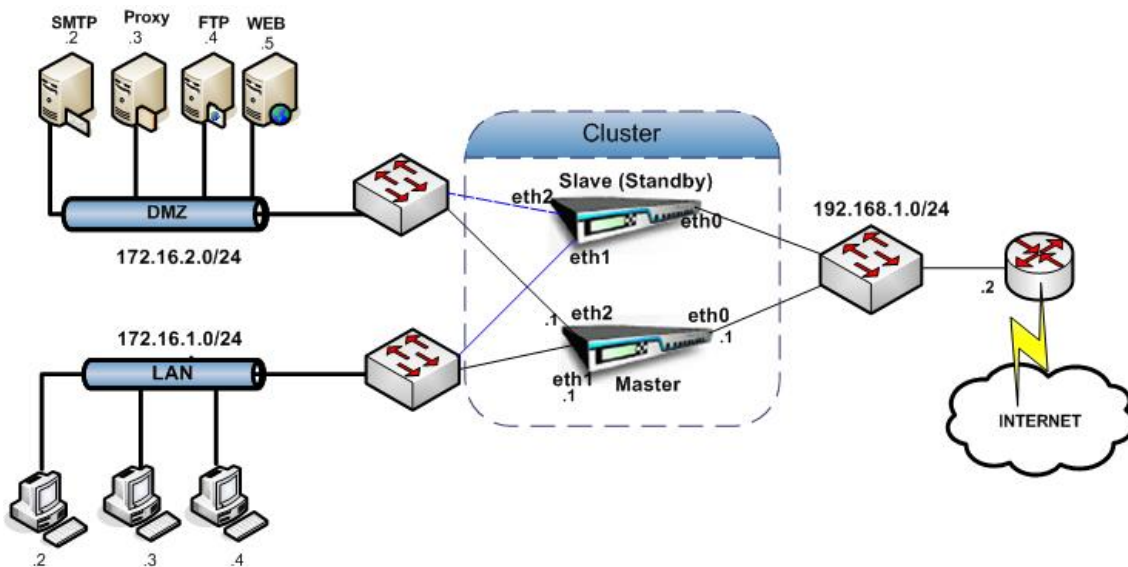


Figure 2: Cluster of two Integra appliances

As you can see, in the cluster made up of the two Integra appliances, the original appliance is the master and the second is on standby, so that if the master appliance fails, services will be kept intact.

Several important aspects must be considered:

- Make sure that the appliance that has already been configured is going to be the master appliance, as the configuration applied in point 2.1 must be kept in the network.
- Minimum settings need to be applied to the slave, as the rest of the settings will automatically synchronize with the master. In this way, the slave appliance will remain on standby, ready to take over the master role if the first appliance fails, without affecting the rest of the network.
- The physical set up shown in the diagram must be adhered to for the cluster to function correctly.

[Content](#)

2.3 Step 1: Configure the master appliance

In order to prepare the GateDefender Integra appliance in the network for high availability, first, you must open the administration console and **enable High availability mode** from System settings -> High availability:

Figure 3: System settings-Slave

Enter the Group and Password parameters:

- **Group:** Enter the number of the group the appliance belongs to. The other appliances in the cluster must belong to the same group. This value must be between 1 and 255.
- **Password:** This data is used to logon the cluster.
- **Repeat password:** Confirmation of the password entered

When selecting the operation mode of this GateDefender Integra appliance in the cluster, you can use either of the modes specified.

- **Automatic:** If you select this mode, the appliances choose which of them is going to be the slave. To do this, the appliance with the highest configuration IP will be assigned the master role.
- **Manual:** If you select this mode, the appliance will take on the mode selected, regardless of its configuration IP.

In this case, we want the first GateDefender Integra appliance to be the master appliance, as all of the parameters have been configured in this appliance. Therefore, manually select master mode:

System settings: High availability Help

High availability

Lets you administer the operation of the unit in parallel with another GateDefender Integra, thereby increasing fault tolerance. Choose between individual mode or high availability, as well as the system used to select if GateDefender Integra will operate as a master and which will replace it in case of failure.

Individual mode

High availability mode

Group it belongs to: 1

Password: ●●●●●

Repeat password: ●●●●●

Select the way in which the master GateDefender Integra will be selected within the cluster

Automatic

Manual: Master

OK Cancel

Figure 4: System settings-Master

With this simple configuration, the appliance that was integrated in the network will be ready to operate in a cluster, of which it will be master.



Warning: Bear in mind that regardless of the method you use to configure this appliance as the master, if the appliance has operational problems or if a network interface card is enabled but not in use, for example, it cannot work as the master (even if it is manually forced in this mode).

On inserting the second appliance in the cluster (with the minimum configuration), if it enters as the master instead of entering as the slave and synchronizing its configuration with the master, it will send its basic configuration to the original appliance, removing the configuration previously defined and making the entire network unstable.

[Content](#)

2.4 Step 2: Configure the slave appliance

Once the original GateDefender Integra appliance has been set up as the master, the necessary settings can be defined in the slave.

This appliance must have the same software version and the same patches (hotfixes or hotfix packs) as the first appliance.

What's more, you do not need to apply the same configuration to the protection units and modules, as it will automatically import the settings from the master.

The only configuration parameter you need to specify is the *configuration IP address* that will be used for communications in the cluster.

This IP address must fulfill two requirements:

- It must be in the same logical range as the configuration IP address of the master.
- It must be assigned to the same network interface card as the configuration IP address of the master.

The master appliance had the following configuration:

Configuration IP: 10.0.0.1/24
NIC: Eth1

You can assign the following settings to the slave, for example:

10.0.0.2/24
NIC: Eth1

To do this, go to System settings-> Access the console and define the configuration IP:

Configure access to the console Help

User
(Specify a user name for accessing the web console).
User name:

Password
(Specify a password for accessing the web console. Passwords must be 6 to 12 characters long.)
Password:
Repeat password:

Note: Bear in mind that you must remember this user name and password in order to access Panda GateDefender Integra.

Configuration IP
Interface:
Configuration IP:
Subnet mask:

Figure 5: Console access settings

After entering the configuration IP address, simply enable high availability and configure the parameters:

System settings: High availability Help

High availability

Lets you administer the operation of the unit in parallel with another GateDefender Integra, thereby increasing fault tolerance. Choose between individual mode or high availability, as well as the system used to select if GateDefender Integra will operate as a master and which will replace it in case of failure.

Individual mode

High availability mode

Group it belongs to: 1

Password: ●●●●●●

Repeat password: ●●●●●●

Select the way in which the master GateDefender Integra will be selected within the cluster

Automatic

Manual: Slave

OK Cancel

Figure 6: Enable high availability mode

The group and the password must be the same as the credentials configured in the master device.

The rest of the settings do not need to be customized, as once it is operating in the cluster, the slave appliance will automatically receive the configuration from the master.

If the master fails, the slave will take over the role of the master and apply the configuration it has received from the master. This process is automatic, transparent, and will not affect the corporate network in any way.

NOTE: Just as in the case of the master device, should the slave appliance not work correctly, or for instance, have any active interface that is not being used, it will never be able to work as slave (even if it is configured so).

[Content](#)

2.5 Step 3: Set up the cluster

After configuring the minimum parameters in the slave, you can insert the second appliance in the corporate network along with the master in order to set up the GateDefender Integra appliances cluster.

To do this, you must strictly adhere to the diagram shown in point 2.2, using switches instead of hubs.

In just a few seconds both appliances will establish communication and the following operations will be carried out:

1. The slave will synchronize the time with the master.
2. The slave will receive the configuration from the master and go on standby.

From then on, communications will only be managed by the master.

The IP addresses used by the LAN and the DMZ as the gateway will continue to be those configured in the master, which will correspond in some way with the virtual IPs of the cluster. If an error occurred in the network and the second appliance had to take over the master role, the rest of the network would not be affected and this failure would be transparent.

[Content](#)
