intelbras

Configuration Interface Manual

IH 3000

Version of this manual: 1.0.1

IH 3000
Wi-Fi 6 Router

Congratulations, you have just purchased a product with Intelbras quality and safety.

The IH 3000 features high-performance 802.11ax technology, designed for applications in corporate environments, such as companies, hotels, and events.

INDEX

REQUIREMENTS

Before you start using the *web* manager, pay attention to the requirements so that you can use it without difficulty.

Operating system

The *web* manager is not a *desktop* application, but a *web* application, so there is no restriction on the operating system and version to be used.

Web browser

The *web* manager works under the *web* platform, meaning that you will need a *web* browser to run it. The compatible browsers are shown below:

Desktop/Notebook/Smartphones/Tablet

Chrome®

Firefox®

Edge®

Safari® (Mac OS X® - 8 a 10.1)

Opera®

Attention: For a better view of the configuration interface, we recommend that the screen width be at least 320 pixels.

Web browsers are updated constantly. Versions higher than those listed above have a good chance of still being compatible, but there is a period of time after their release for our development team to validate their compatibility. As soon as this validation is done and compatibility is verified, the above information will be updated

EXPORT TO PDF

To export this manual to PDF file format, use the print feature that browsers such as Google Chrome® and Mozilla Firefox® have. To access it, press the *CTRL + P* keys or click here. If you prefer, use the browser menu, accessing the *Print* tab, which is usually located in the upper right corner of the screen. On the screen that will open, follow the steps below, according to the browser:

Google Chrome®: in the print screen, in the *Destination* field, click *Change*, select the *Save as PDF* option in the *Local Destinations* section, and click *Save*. The operating system screen will open asking you to name the file and choose where to save it.

Mozilla Firefox®: in the print screen, click *Print*, in the *General* tab, select the *Print to file* option, in the *File* field, name the file and choose where to save it, select *PDF* as the output format, and click *Print*.

LOGIN

To access the configuration interface, you need to be connected to the router.

You can connect to the router through the network cable on the IH 3000's LAN connection, or through the Wi-Fi connection.

The Wi-Fi password information and the password to access the configuration interface are on the label at the bottom of the product.

When connected, make sure your device is configured to receive an IP from the IH 3000.

Once connected to the router, open your web browser, go to http://192.168.1.1 (http://192.168.1.1), and you will see this screen:

The user is **admin**, and the password is on the label underneath the product.

When accessing the product for the first time, you will be prompted to change the password.

After entering the new password, the router will return to the initial login screen.

Basic Mode

Here we will show you the basic settings of the IH 3000 router.

Wi-Fi Network Configuration

Basic

On this screen, you will configure your wireless network.

Dual-band *: Here you will set whether the Wi-Fi settings will apply to both the 2.4GHz and the 5GHz networks. To keep the settings the same for both networks, select the *Enable* option, and if you want different settings, select the *Disable* option.

Enable Wi-Fi network: In this field select whether you want to leave Wi-Fi enabled or disabled.

SSID: In this field enter the name for your Wi-Fi.

Security Mode: In this field, set the security of your wireless network.

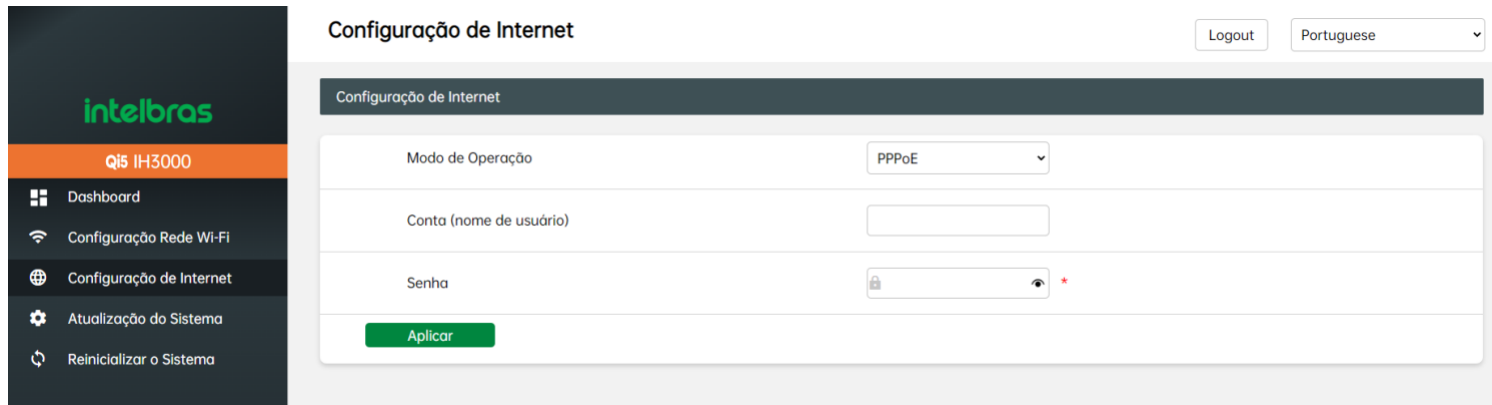**WPA Encryption:** In this field, select the type of security mode encryption.

Password: In this field, set a password for your wireless network. Note that the password must be at least 8 characters long.

Click **Apply** to save and apply the settings.

Guest Network

On this screen, you will set up the wireless network for the guests. This network is isolated from the main network. You cannot activate the guest network with the Mesh function active.

Dual-band *: Here you will set whether the Wi-Fi settings will apply to both the 2.4GHz and the 5GHz network. To keep the settings the same for both networks, select the *Enable* option, and if you want different settings, select the *Disable* option.

Enable Wi-Fi network: In this field select whether you want to leave Wi-Fi enabled or disabled.

Enable Scheduling: Allows you to create rules to control the Guest Network's Internet access, setting times and days of the week.

SSID: In this field enter the name for your Wi-Fi.

Security Mode: In this field, set the security of your wireless network, it is recommended to use WPA2- PSK or WPA3-PSK mode.

WPA Encryption: In this field, select the type of security mode encryption.

Password: In this field, set a password for your wireless network. Note that the password must be at least 8 characters long.

Click **Apply** to save and apply the settings.

Internet Configuration

PPPoE

On this screen, you will set up the username and password for Internet access, if you use the IH 3000 to receive an Internet signal via network cable on the router's WAN connection.

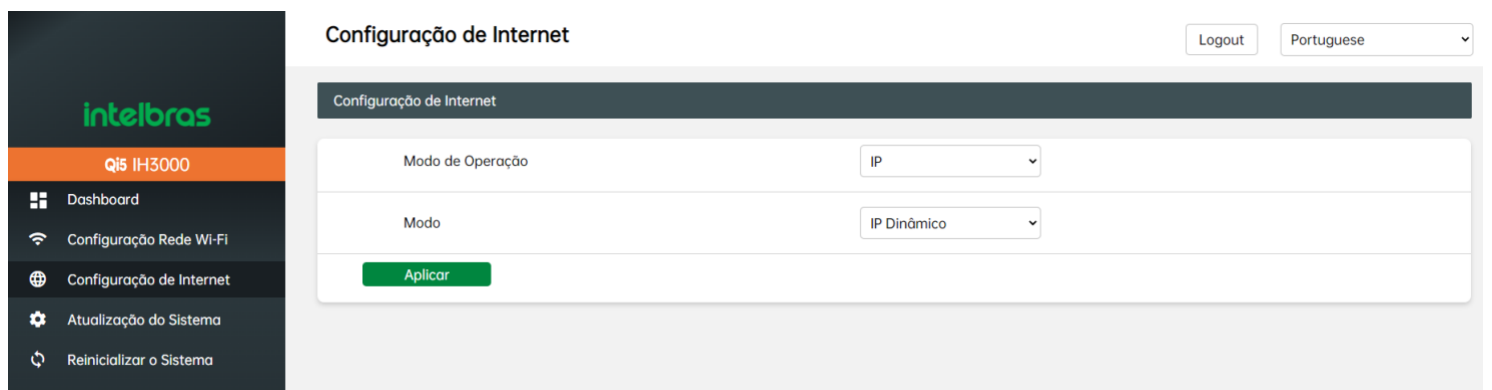Use this mode if your Internet connection (WAN) settings require PPPoE authentication.

At least one username and password (provided by your internet service provider or operator) will be required to authenticate with the internet.

Account (username): Enter the PPPoE user provided by your Internet provider.

Password: Enter the PPPoE password provided by your Internet service provider.

Click **Apply** to save and apply the settings.

IP

On this screen, you will configure the IP mode of the WAN.

Mode: you can select two types of IP connection on the IH 3000's WAN, which are:

• **Dynamic IP:** Use this mode if the settings for your Internet connection (WAN) are provided automatically via a DHCP server.

- **Static IP:** Use this mode if your Internet (WAN) connection settings are provided via a static IP address. All information required for this connection must be provided by your Internet Service Provider or operator.

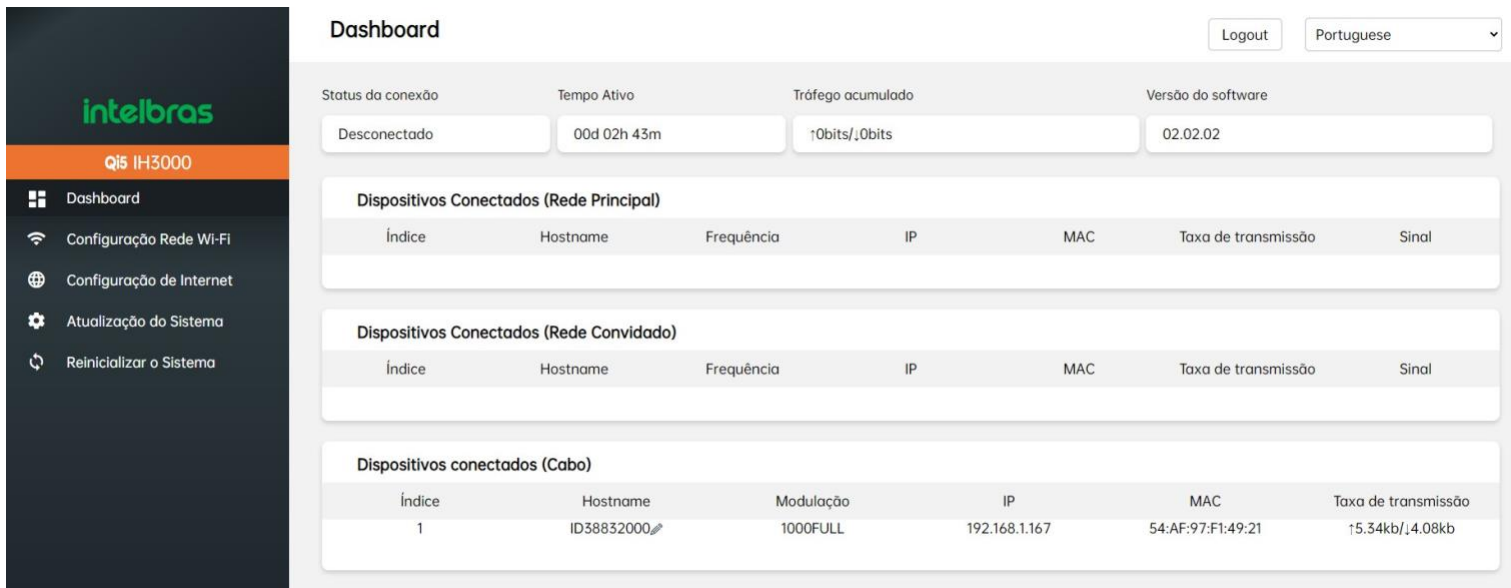Click **Apply** to save and apply the settings.

Bridge Mode
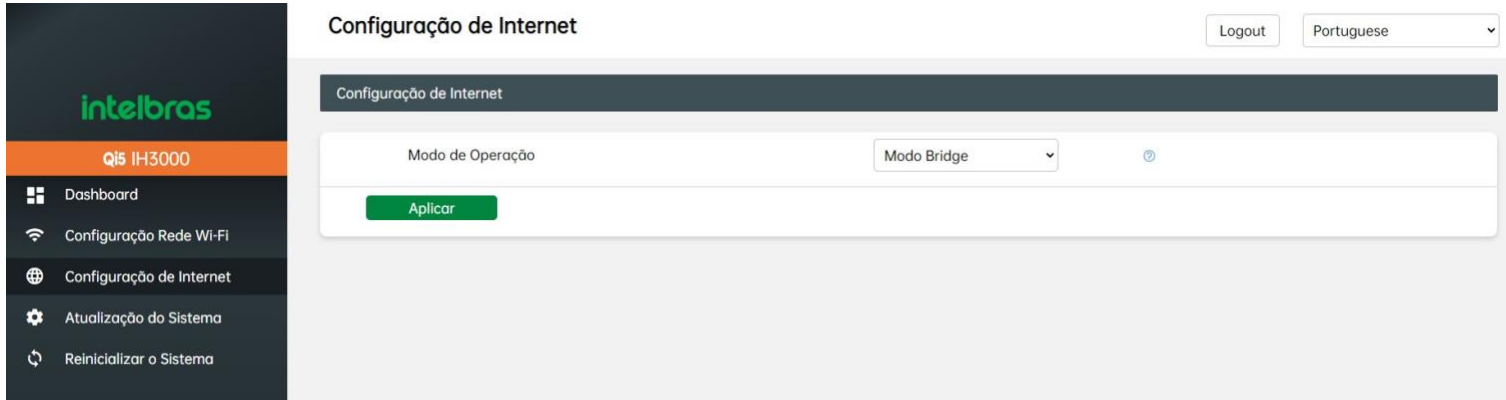
On this screen you can set the IH 3000 as a bridge, turning the router's WAN connection into a LAN, so the IH 3000 will pass on all information without routing.

To configure, enable the **Bridge Mode** option, and Click **Apply** to save and apply the settings.

Dashboard

On this screen, you can check the information about your network

Here you will see the **connection status, router uptime, accumulated traffic**, and **software version**, as well as the **devices connected** on both the main network and the guest network, with information about **frequency range, device IP, MAC address, transfer rate,** and **signal**.

System Update

Software

On this screen, you can check the IH 3000's current **software version**, and you can also check for a new software version, as well as update the product's software.

In **Update Mode**, if you select the **Auto** option, you can click **Check for a new version** to automatically check if a new version is available for update. To perform the firmware version update you need to have a cable connected to the WAN interface with Internet access.

If you select the **Manual** option, the **File Path** field will be enabled to select the software file and update the product manually.

Check the website www.intelbras.com (https://www.intelbras.com/pt-br/) or an updated software version to update manually.

Restart the System

In this screen, you can restart the IH 3000 by clicking the **Restart** button.

Note that the IH 3000 will only restart, i.e., no settings will be lost.

Advanced Mode

Dashboard

On this screen, you can check your network information.

Here you will see the **connection status**, router **uptime**, **accumulated traffic**, the **software version**, as well as the **connected devices** on both the main and guest network with information on **frequency range**, **device IP, MAC address, transfer rate,** and **signal.**

Information

Network and System

Logout | Portuguese

intelbras

Qi5 IH3000

- Dashboard
- Informação
  - Rede e Sistema
  - Wi-Fi
- Configuração
- Ferramentas

Modo Básico

Rede e Sistema

Informações do Dispositivo

Modelo	IH 3000
Nome do dispositivo	IH 3000
Versão do software	02.02.02

Endereço IP

WAN (IPv4)	--
Máscara de Sub-Rede WAN (IPv4)	--
Gateway Padrão WAN (IPv4)	--
DNS 1 WAN (IPv4)	--
DNS 2 WAN (IPv4)	--
WAN (IPv6)	--
Endereço de prefixo WAN (IPv6)	--
Gateway Padrão WAN (IPv6)	--
DNS 1 WAN (IPv6)	--
DNS 2 WAN (IPv6)	--
LAN (IPv4)	192.168.1.1
LAN (IPv6)	fe80::26fd:dff:fe22:fe38

Endereço MAC

WAN	24:FD:0D:22:FE:37
LAN	24:FD:0D:22:FE:38
WLAN (2.4GHz)	24:FD:0D:22:FE:39
WLAN (5GHz)	24:FD:0D:22:FE:3A

On this screen, you will have the IH 3000 information such as the **model, device name, software version**, WAN/LAN **IP address** information, and **MAC address** information**.**

Model: Informs the product´s model.

Device Name: Informs the name of the IH 3000. You can change the name of the product.

Software version: Informs the current software version.

WAN (IPv4): Informs the IPv4 address of the WAN interface.

WAN (IPv6): Informs the IPv6 address of the WAN interface.

LAN (IPv4): Informs the IPv4 address of the LAN interface.

LAN (IPv6): Informs the IPv6 address of the LAN interface.

MAC Address: Informs the MAC addresses of the IH 3000 interfaces, such as the WAN MAC address, the LAN MAC address, the 2.4GHz Wi-Fi MAC address, and the 5GHz Wi-Fi MAC address.

Wi-Fi

2.4GHz

On this screen, you will have information about the main 2.4GHz Wi-Fi network, such as **Network name, Total data traffic**, **and Transfer rate.**

5GHz

On this screen, you will have information about the main 5 GHz Wi-Fi network, such as **Network name, Total Data Traffic**, **and Transfer rate.**

2.4GHz (Guest)

On this screen, you will have information about the 2.4GHz guest Wi-Fi network, such as **Network name, Total Data Traffic**, **and Transfer rate.**

5GHz (Guest)

On this screen, you will have information about the 5GHz guest Wi-Fi network, such as **Network name, Total Data Traffic**, **and Transfer rate.**

Configuration

WAN Configuration

On this screen, you will configure the internet access, if you use the IH 3000 to receive an internet signal via network cable on the router's WAN connection. Three modes can be selected in **Operation Mode**, they are:

- **PPPoE:** Use this mode if your Internet connection (WAN) settings require PPPoE authentication. You will need at least one account (username) and password (provided by your Internet service provider or operator) to authenticate with the Internet.

- **IP:** When you select this option, the *Mode* option will be enabled, and can be used in either *Dynamic IP* or *Static IP*. Use this Dynamic IP mode if your Internet connection (WAN) settings are provided automatically through a DHCP server, or select Static IP mode to manually set an IP on the WAN.

- **Bridge Mode:** Use this mode if you want to turn the router's WAN connection into a LAN connection, so the IH 3000 will pass on all information without routing.

LAN Configuration

IPv4

On this screen, you can configure the IPv4 information of the LAN, which is:

IP: In this field, you must configure the IP address you want to access your router. When you make the change and save, the DHCP server settings (start and end IP address) will be automatically adjusted to the configured range.

Subnet Mask: You must set the subnet mask you want. When you make the change and save, the DHCP server settings (start and end IP address) will be configured accordingly.

DHCP Server: If enabled, devices connected to the IH 3000 will automatically receive an IP address, within the range set in the Start IP Address and End IP Address fields. If unchecked, devices connected to the IH 3000 will not receive an IP address, so all devices connected to the IH must configure an IP address manually.

Start IP address: You can configure the first available IP address that your devices can connect to. This address is limited by the subnet mask configured on the LAN.

End IP address: You can configure the last available IP address that your devices can connect to. This address is limited by the subnet mask configured on the LAN.

Allocation time: Here you configure for how long the IP address will be allocated to the device that will connect to the IH 3000.

DNS: It is the service responsible for converting the domain names of websites into IP addresses, by default the Router will use your ISP's DNS servers, or you can manually configure 2 DNS servers of your preference.

IPv6

In this menu, you can adjust settings related to your IPv6 connection on the router's LAN. Below we will explain each available option. To adjust these settings, you must have knowledge of these configuration modes:

Stateless: This autoconfiguration does not require manual configuration of hosts, or additional servers. This mode of operation is a key feature of IPv6, allowing the host itself to generate its IPv6 address, from a combination of locally available information and information announced by routers.

Stateful: The DHCPv6 server is responsible for informing clients of the IPv6 addresses that should be used on their network interfaces, maintaining the status of which address has been assigned to a particular client.

IPv6 address: Manually configure the IPv6 address.

DHCPv6 Service: Allows you to enable/disable IPv6 on the Router's LAN interface.

DHCPv6 Mode: Allows you to change between Stateless, Stateful, and Stateless + Stateful modes

System Configuration

Password

On this screen, you can set the password to access the router's settings. The default password is given on the label at the bottom of the product.

To change the password, in the **Old Password** field enter the router's current password. In the **New Password** field, enter the new router password. The password can be up to 32 characters long, and cannot be blank. Confirm the new password in the **Confirm Password** field, and click **Apply**.

Restore

On this screen, you can see options to restore the product to factory default and also to restart the product.

Reset to Factory Settings: When you click this option, the router will reboot and go back to the factory settings, and you will need to reconfigure it again.

Reset to factory settings (Keeping only TR069 and WAN settings): When you click this option, the router will reboot and go back to factory settings, but the WAN and TR069 settings will be kept.

Restart system: When you click this option, the router will just restart, but no settings will be affected.

Update
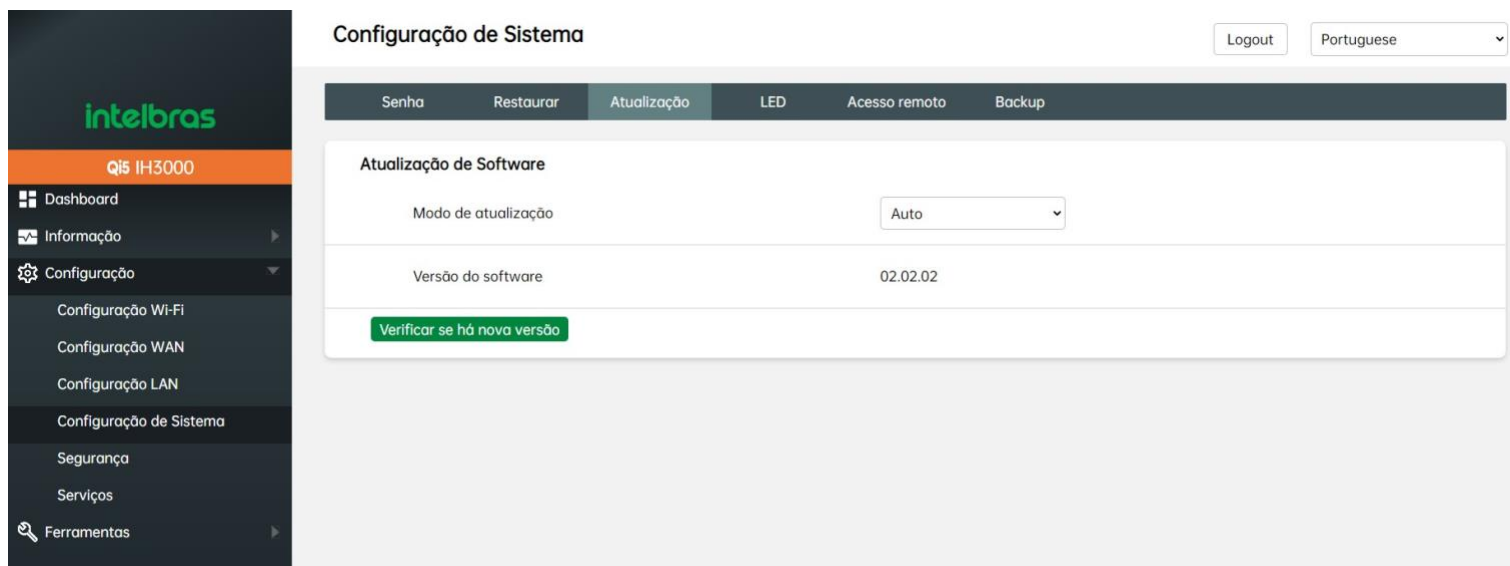
On this screen, you can see the current software version of the IH 3000 and the update mode.

Under **Software Update**, there is an option called **Update Mode**, which has two options, which are:

- **Auto:** if you select this option, you can click *Check for a new software version*, the router will check the cloud for a new software version of the router, and if there is, you will be asked whether you want to install the new software version or not.
- **Manual:** If you select this option, the **File Path** field will be enabled to select the software file and update the product manually.

Check the website www.intelbras.com.br for an updated software version to update manually.

> The firmware update does not interfere with the router settings. When you upgrade the IH 3000, all settings will remain the same.

LED

On this screen, you can configure the LED on the router base.

LED: select whether to *enable* or *disable* the *LED* at the base of the router.

If enabled, select one of the available colors, which are: magenta, cyan, purple, white, red, green, blue, or pink.
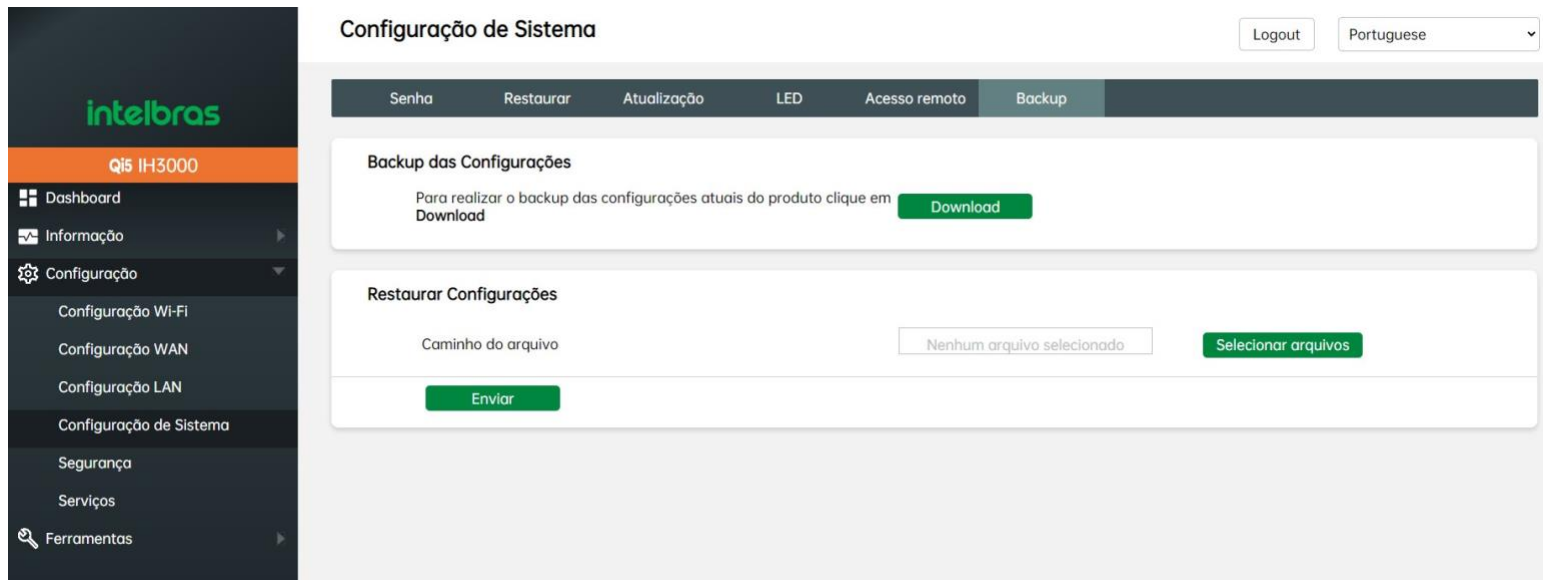
Remote Access

On this screen, you will configure the remote code.

Remote access from the Web: Here you can *enable* or *disable* access to the product's web interface outside the network.

If enabled, select the web access port.

SSH remote access: Here you can *enable* or *disable* SSH access to the product from outside the network. If enabled,

select the SSH access port.

Backup

On this screen, you will configure the backup of the router's settings. In the **Settings Backup** option, when you click the Download button, you will download the backup of the current router settings.

From the **Restore Configuration** option, you will select the saved backup and upload it to the router. When you upload the backup and press the upload button, the router will reboot to apply the backup.

Wi-Fi Configuration

Basic

On this screen, you will configure your wireless network.

Dual-band *: Here you will define whether the Wi-Fi settings will apply to both the 2.4GHz and the 5GHz network. To keep the settings the same for both networks, select the *Enable* option, if you want different settings for both networks, select the *Disable* option.

Enable Wi-Fi: Select whether you want to keep the Wi-Fi network *enabled* or *disabled*.

SSID: In this field write the name for your Wi-Fi.

Security Mode: In this field, set the security of your wireless network.

WPA encryption: In this field, select the security mode encryption type

Password: In this field set a password for your wireless network. Note that the password must be at least 8 characters long.

Hide SSID: If this option is enabled, the Wi-Fi network name will be hidden and will no longer appear in the network lists. Thus, to connect to the network, you will have to manually specify the name and password in the additional network settings of your device.

Isolate SSID: If this option is enabled, the Wi-Fi networks will be isolated from each other, so a device connected to one network will not be able to see/access a device that is on the other Wi-Fi network.

Max. connected clients: in this field, you will set how many clients can connect to the wireless network, which can be from 1 to 64.

Click **Apply** to save and apply the settings.

> * If the Dual band Disable option is used, the 2.4GHz and 5GHz network settings must be configured separately.

Advanced

On this screen, you will configure the parameters of your wireless network, both for the 2.4GHz network and for the 5GHz network.

Power: here you can specify the Wi-Fi transmission power of the device. The higher the value in *db*, the greater the Wi-Fi signal coverage.

Bandwidth: In this field select the wireless network bandwidth, which can be set to 20, 40, 80, or 160MHz (5GHz) and 20 or 40MHz (2.4GHz).

Channel: In this field select the operation channel of the wireless network.

IEEE Mode: In this field select the wireless network transmission protocol. This field can change the transmission rate of the wireless network.

Region: In this field, select the region of the Wi-Fi. Depending on the region selected, the number of broadcast channels can be changed.

Click **Apply** to save and apply the settings.

Guest Network

On this screen, you will configure the guest wireless network parameters.

Dual-band *: Here you will define whether the Wi-Fi settings will apply to both the 2.4GHz and the 5GHz network. To keep the settings the same for both networks, select the *Enable* option, if you want different settings for both networks, select the *Disable* option.

Enable Wi-Fi: Select whether you want to keep the guest Wi-Fi network *enabled* or *disabled*.

Enable Scheduling: Allows you to create rules to control the Guest Network's Internet access, setting times and days of the week.

SSID: in this field set the name of the wireless network for visitors.

Security Mode: In this field, set the security of your wireless network.

WPA encryption: In this field, select the security mode encryption type.

Password: In this field set a password for your wireless network. Note that the password must be at least 8 characters long.

Hide SSID: If *Enabled*, the Wi-Fi network will not be visible for connection, so to connect to the network, you must manually configure the network name, encryption, and password on the devices. If you leave it *Disabled*, the network will be visible for everyone to connect to.

Isolate SSID: If *Enabled*, the devices connected to the network will not see each other, so the connected device will not be able to access any other devices on the network. If *Disabled*, devices will see each other normally.

Max. connected clients: In this field, you will set how many clients can connect to the wireless network, which can be from 1 to 64.

Click **Apply** to save and apply the settings.

EasyMesh

On this screen, you configure EasyMesh, where you can create a mesh network using the GX 3000* and IH 3000.

EasyMesh: Enable or disable the EasyMesh configuration option. When enabled, you need to adjust the following parameters:
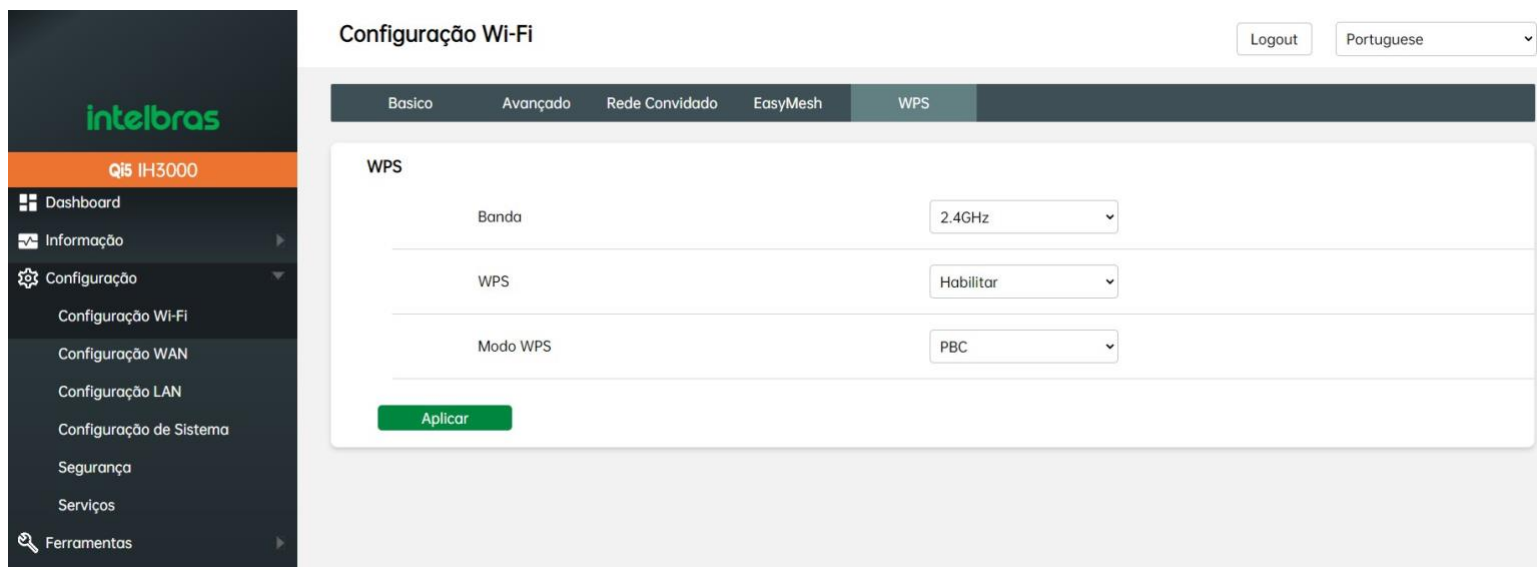
Operation Mode: You can configure the equipment as a **Gateway** or as an **Extender**, as a gateway it will receive the internet link via Ethernet cable or via cell phone and distribute it to the rest of the network, acting as a router. As an extender, the equipment will connect to the gateway and pass on its configurations.

Connection Mode: In this option you can define by which wireless frequency the extender will connect to the other Mesh devices in the network, having the options of 2.4 and 5GHz, we recommend using 5GHz to get better communication speed between the EasyMesh devices in the network and 2.4GHz if you want to prioritize the range. If you want to change the communication frequency of the Mesh network after setup, you need to pair the equipment again.

The GX 3000 is a router with 5G mobile Internet technology and Wi-Fi 6 Mesh from Intelbras' Qi5 family.

To see the EasyMesh configuration tutorial*, click here (./manualOpeRamal_pt-BR.html).*

WPS

On this screen you configure the WPS, to connect devices via Wi-Fi without the need for password authentication.

- • **Band:** Here you select the frequency at which the devices will connect through WPS.

- • **WPS:** Here you select whether to *enable* or *disable* the router's WPS function.

- • **WPS Mode:** This option is available if WPS is enabled. Here you will select the WPS connection method, which can be:
- **-** **Client PIN:** In this WPS mode, the connection is made by entering a PIN code on the device you want to connect to the router.
- **-** **PBC:** In this WPS mode, the connection is made by pressing the WPS button on the router and activating the WPS option on the device you want to connect to. To activate the WPS from the button, you need to press the button once, wait 4 seconds and press it again. After pressing it a second time, the WPS function is activated.
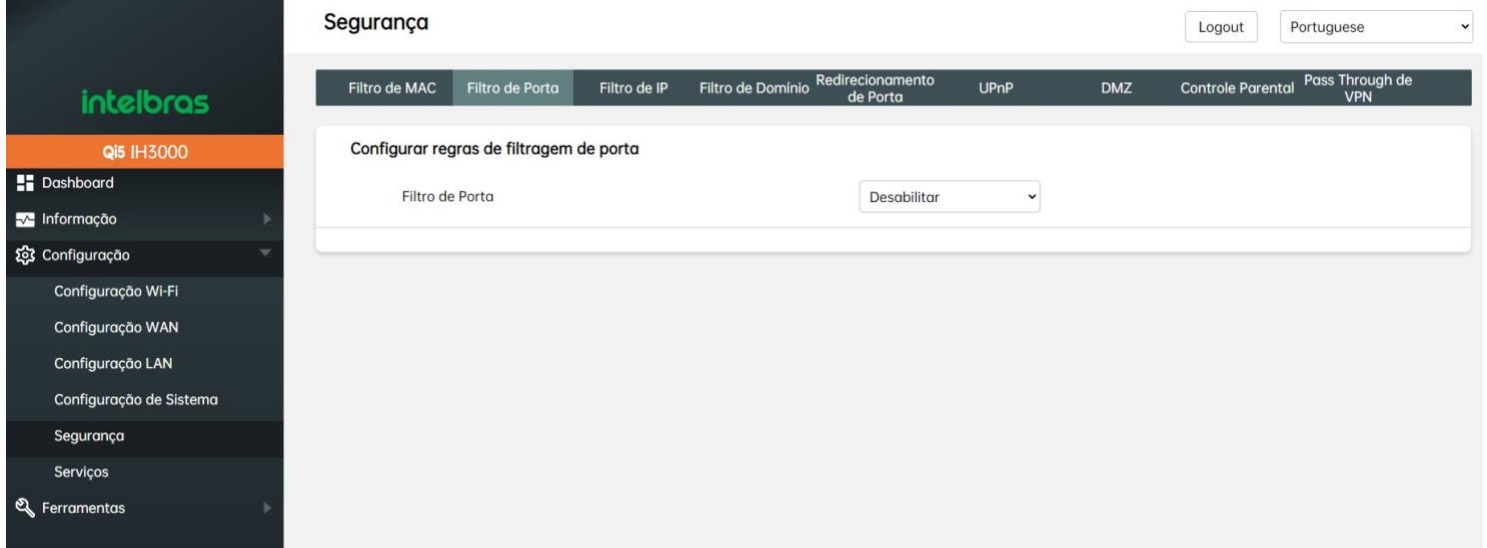
Security

MAC Filter
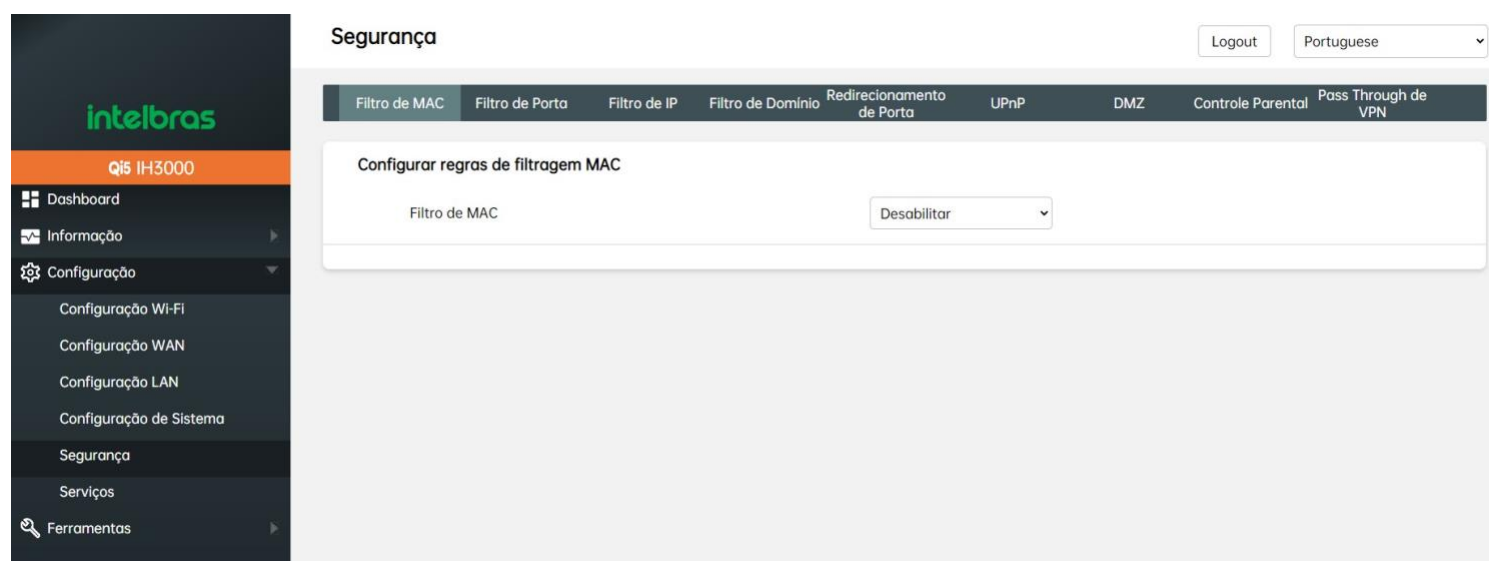
Through the MAC Filter, you can block devices from connecting to the router via Cable and Wi-Fi. On this screen, you will see the list of blocked MAC addresses, as well as options to add new MACs, edit, and delete.

You can configure up to 32 MAC filter rules.

Port Filter

The Port Filter setting allows you to restrict communication from the router by a specific port and/or port range. This function can be used for example to limit access to certain online applications.

On this screen you will see the options to add new filters, you will also be able to edit and delete existing filters.
You can configure up to 32 port filter rules.

IP Filter
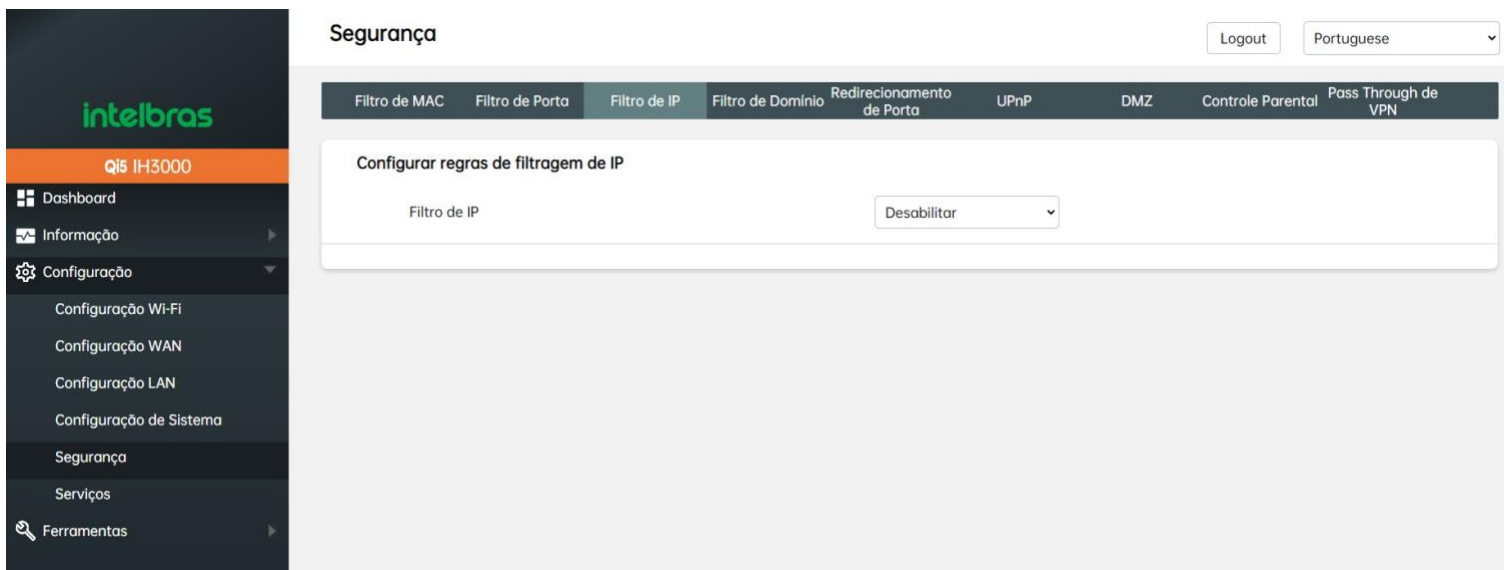
Through the IP Filter, you will be able to block communication with the router's network from a specific IP address in TCP or UDP protocol. On this screen, you will see the IP filters you have created, as well as options to add, edit or delete filters.

You can configure up to 32 IP filter rules.
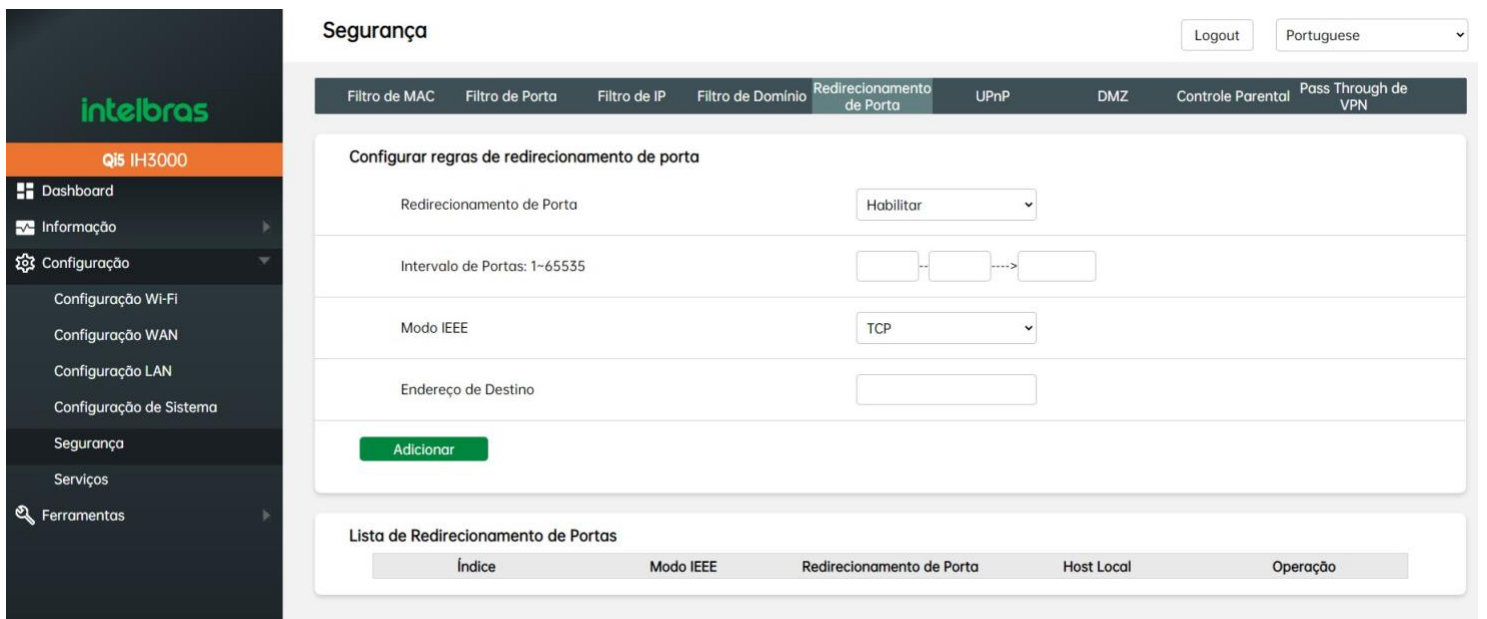
Domain Filter

Through the Domain Filter, you will be able to block or enable websites and URLs.

You can configure up to 32 domain filter rules.

> * It will only work on sites with HTTP, sites with HTTPS will not be blocked.

Port Forwarding

On this screen, you can see all existing forwarding rules and also options to create, edit or remove.

You can configure up to 32 port forwarding rules.

UPnP

On this screen, you will configure the UPnP protocol.

If enabled, the UPnP (Universal Plug and Play) protocol will be active on the router, allowing for automatic configuration of port forwarding rules for external requests. If disabled, UPnP will be turned off and unable to create rules automatically.

DMZ

On this screen, you will configure the DMZ.

If enabled, you will be able to define a DMZ Host that will be the DMZ of your local network, i.e., this IP will be exposed to any service from the external network (internet).

Note: If you enable the DMZ and save, UPnP will be disabled automatically, and port forwarding will no longer work.

Parental Control

In the Parental Control menu, you will be able to access the Block Schedule settings and view the Parental Control rules for connected devices.

You can configure up to 32 parental control rules.

VPN Pass-Through

On this screen, you can enable or disable the VPN tunneling protocols.

Services

NTP

On this screen, you can configure the NTP (Network Time Protocol), so that the router will adjust the date and time according to the configured NTP server, as long as it has Internet access.

ALG

ALG stands for Application Layer Gateway. Its purpose is to avoid some of the problems caused by router firewalls by inspecting VoIP traffic (packets) and, if necessary, modifying it. On this screen, you can *enable* or *disable* the ALG option for H323E, FTP, SIP, RTSP, and PPTP services.

QoS
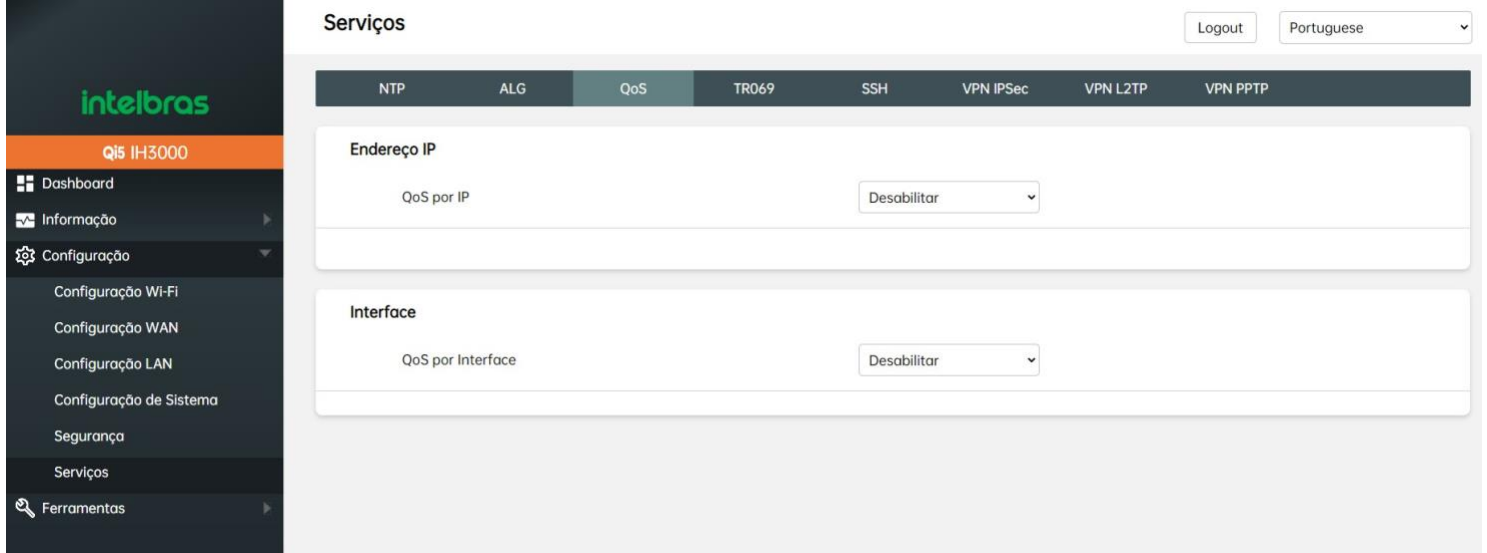
QoS works with bandwidth guarantees, for example, if you set 80% for the main wireless network and 20% for the guest wireless network, the guest wireless network will be guaranteed this percentage of bandwidth whenever needed. When the main network is not using the percentage of bandwidth reserved for it, QoS will automatically free up more bandwidth for the guest network and vice versa. As the main network starts using more bandwidth again, the QoS will decrease the guest network's bandwidth until it equalizes to the percentage configured here.

TR069
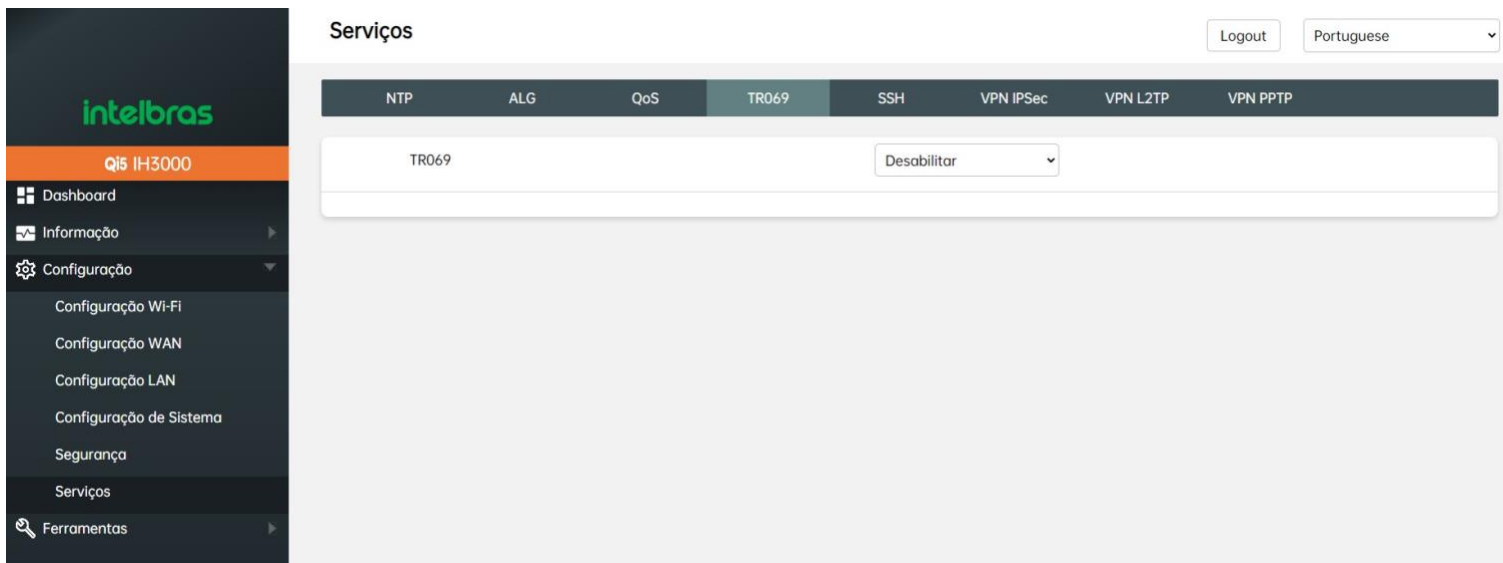
On this screen you can configure TR069, which is an application that allows service providers and equipment manufacturers to remotely manage, configure, and update devices connected to the network.

SSH
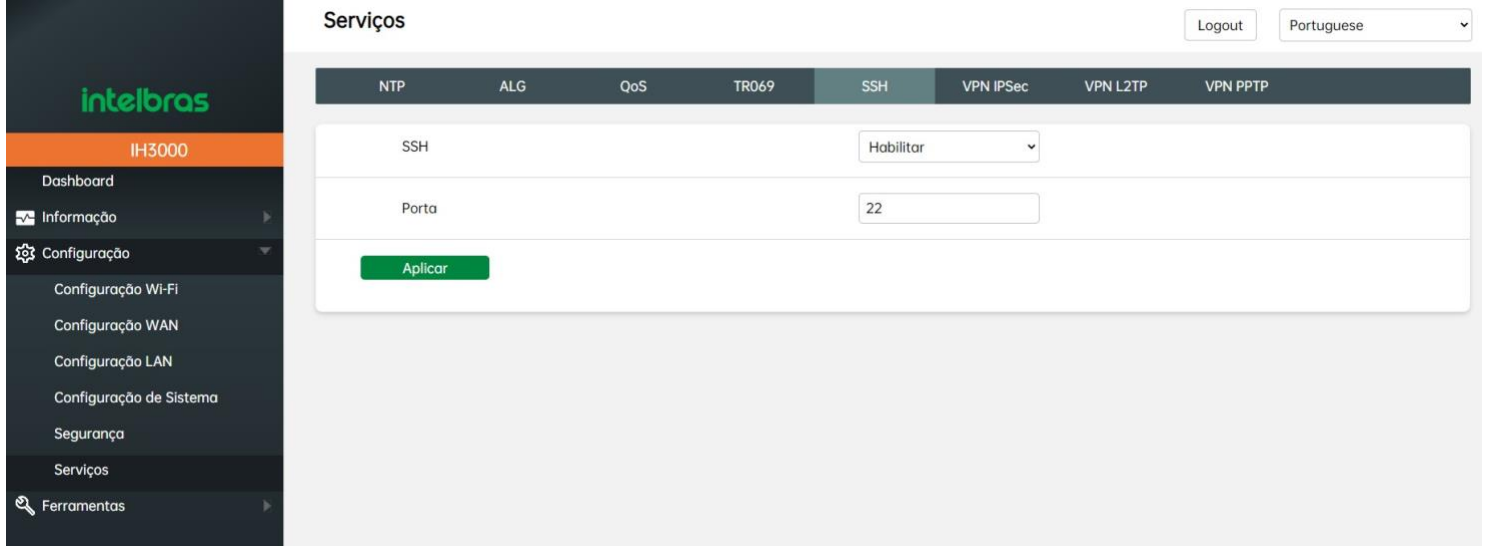
On this screen, you will be able to *enable* or *disable* SSH access to the router, and if enabled, choose the SSH access port.

VPN IPSec
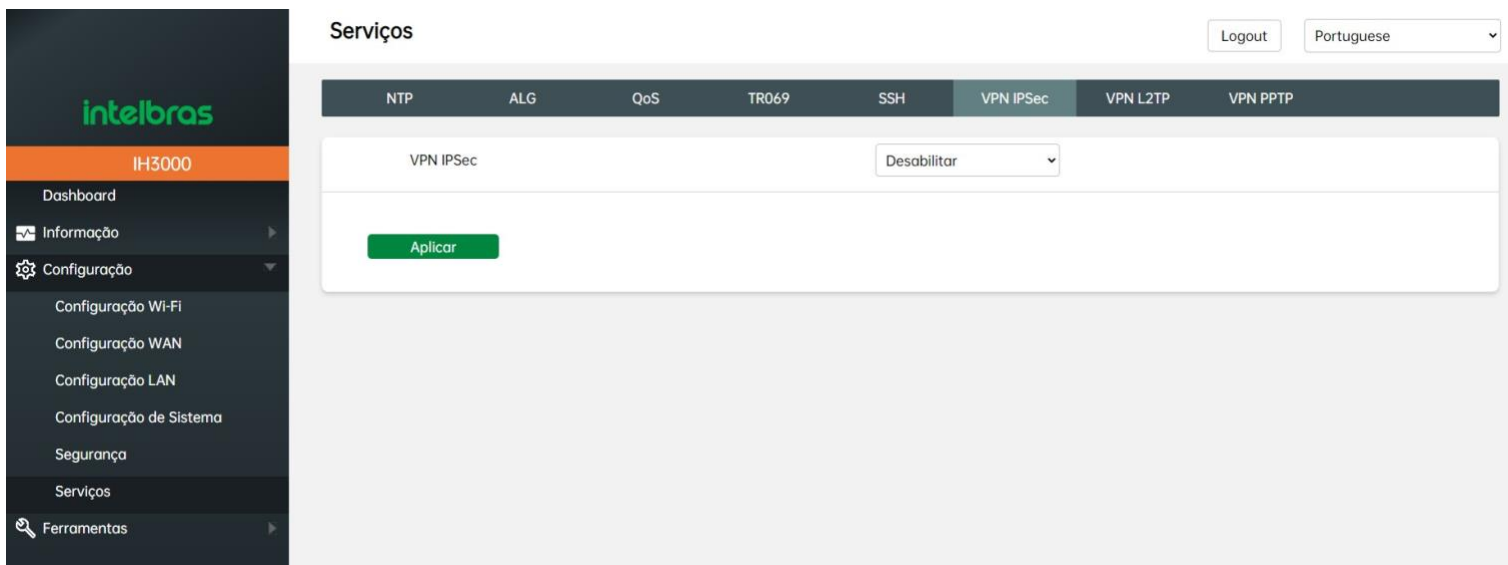
On this screen, you can configure IPSec, used for the VPN connection.

VPN L2TP
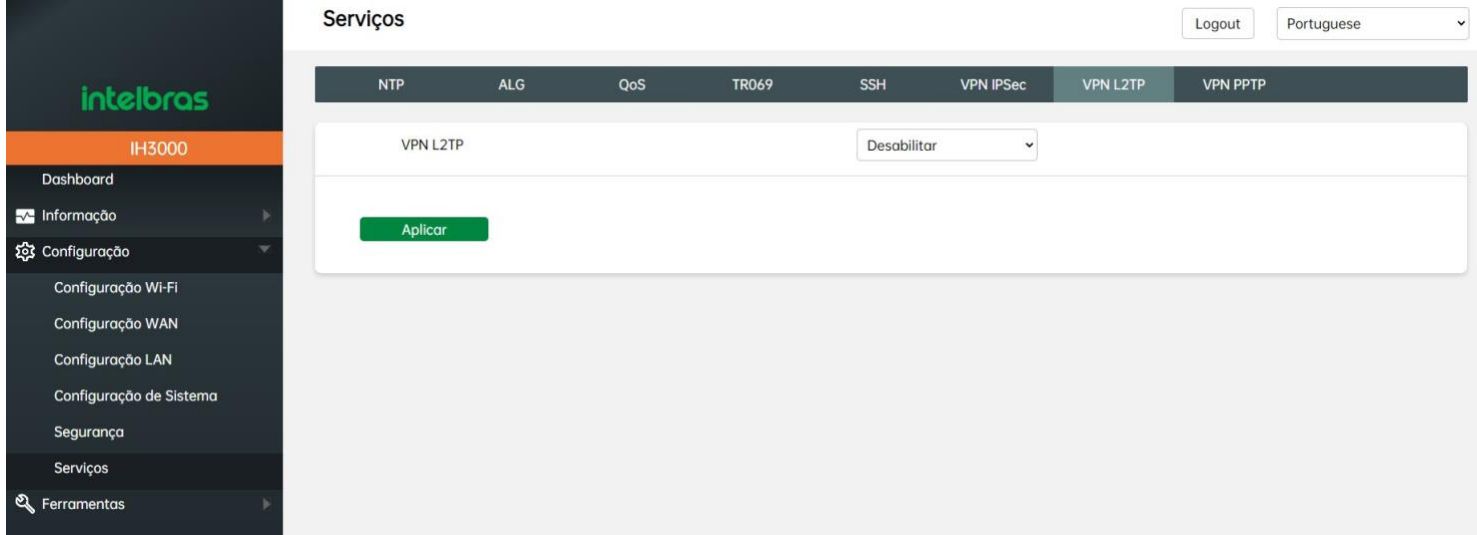
On this screen, you can configure the L2TP, used for the VPN connection.

VPN PPTP
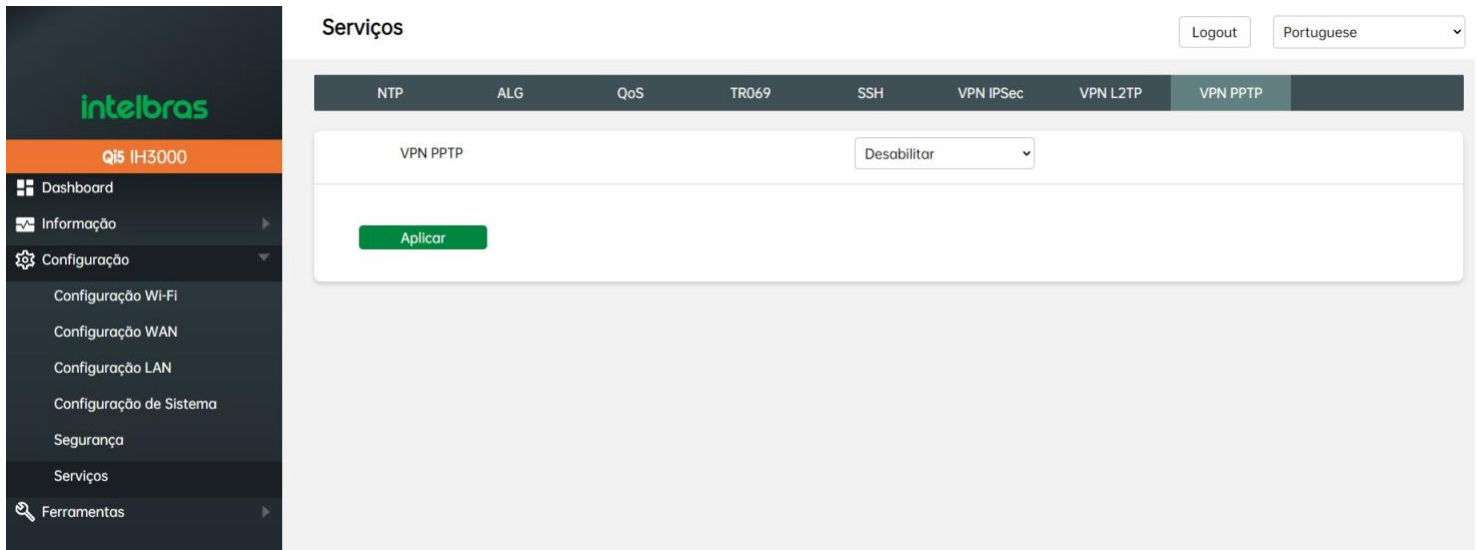
On this screen, you can configure the PPTP, used for the VPN connection.

Tools

System Log
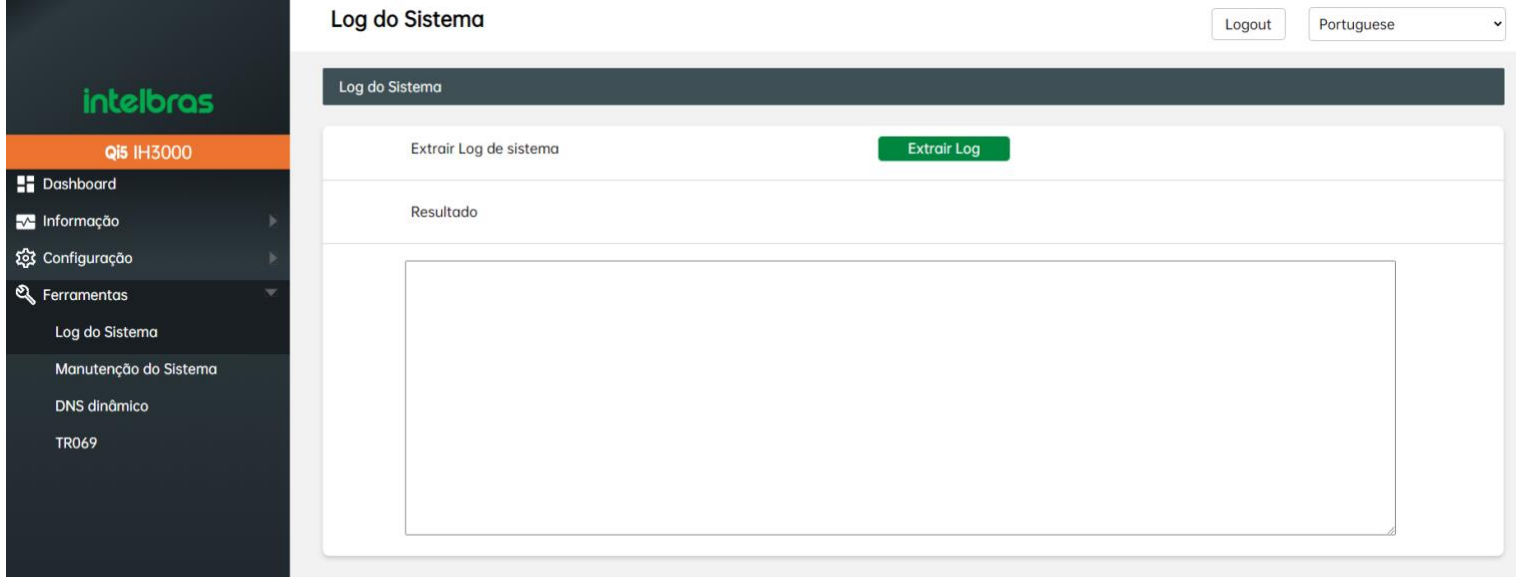
On this screen you can enable the system log, which contains information about the router's usage.

System Maintenance
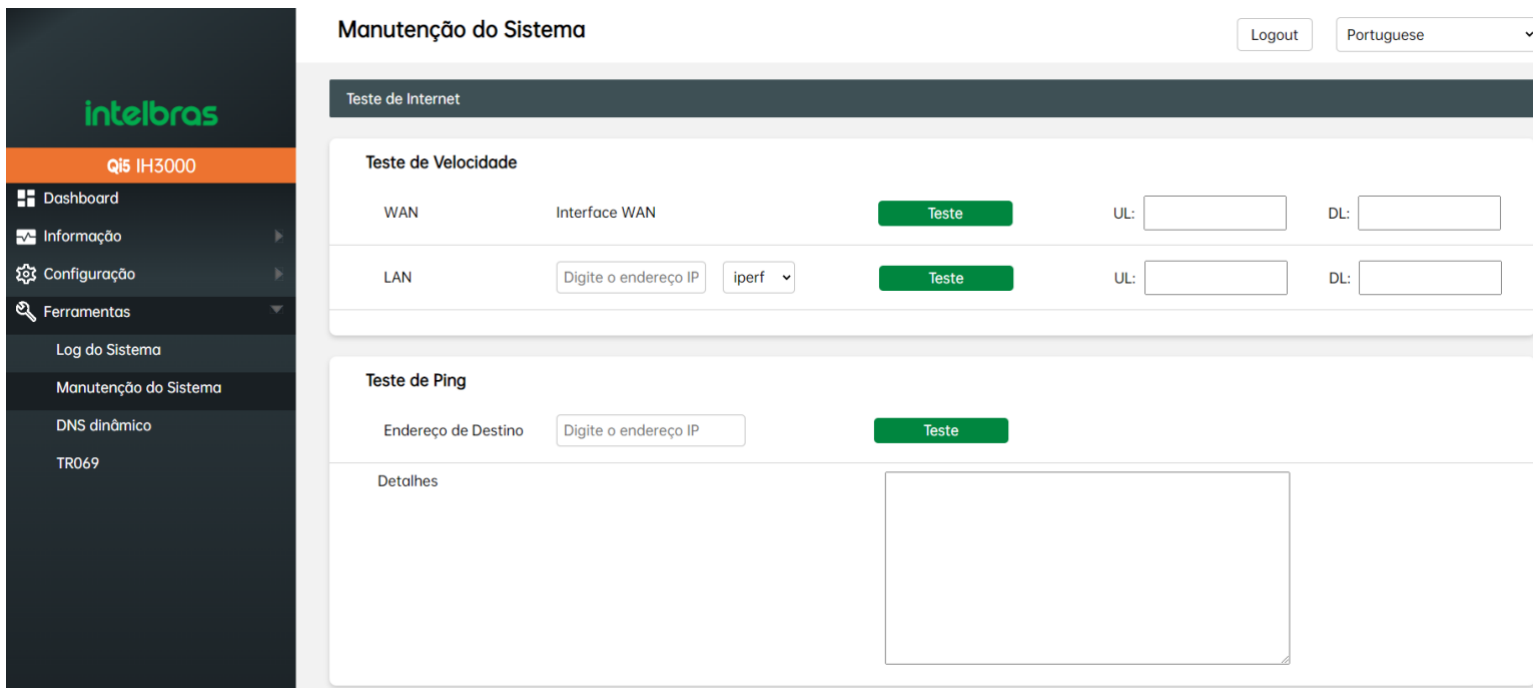
On this screen, you can perform a WAN and LAN speed test, as well as a ping test to see if the router can find the destination.

Dynamic DNS
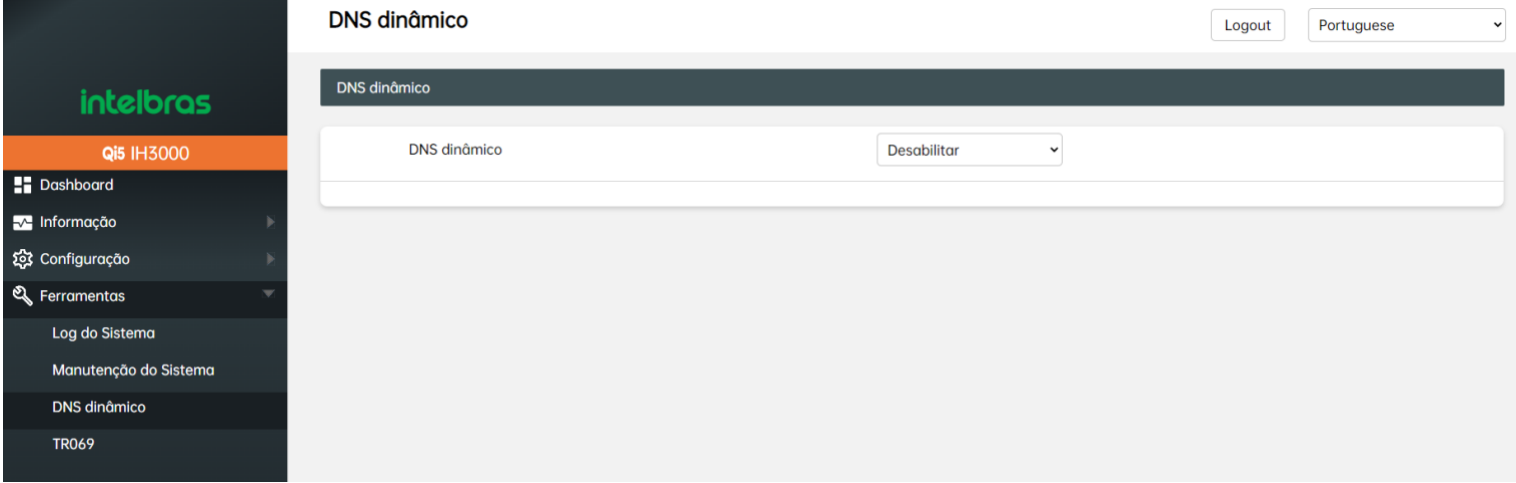
On this screen, you can configure the dynamic DNS.

* Intelbras does not provide DDNS service, but you can configure a third-party service on the IH 3000.

WARRANTY TERMS

For your convenience, please fill in the information below, as only with the presentation of this together with the purchase invoice of the product, you will be able to use the benefits that are guaranteed to you.

Client Name:

Client Signature:

Invoice No:

Date of purchase:

Model:

Serial No:

Retailer:

It is hereby stated that this contractual warranty is granted under the following conditions:

1. All parts and components of the product are guaranteed against any manufacturing defects that may arise, for a period of 1 (one) year - comprising of 3 (three) months of legal guarantee plus 9 (nine) months of contractual guarantee -, starting from the date of purchase of the product by the Consumer, as stated on the purchase invoice, which is an integral part of this agreement throughout the national territory. This contractual guarantee covers the replacement of parts and components that present manufacturing defects. If it is not determined to be a manufacturing defect, but rather a defect(s) resulting from improper use, the Consumer will bear these expenses.

2. The product´s installation should be done according to the Product Manual and/or Installation Guide. If your pro- duct requires installation and configuration by a qualified technician, look for a competent and specialized professional, considering that the costs for these services are not included in the product's price.

3. If a defect is found, the Consumer must immediately contact the nearest Authorized Service, as listed by the manufacturer - only they are authorized to examine and repair the defect during the warranty period provided here. If this is not respected, this warranty will lose its validity, as it will be characterized as a violation of the product.

4. In the event that the Consumer requests home assistance, they must go to the nearest Authorized Service to inquire about the technical visit fee. If it is necessary to remove the product, the resulting expenses, such as transportation and security costs to and from the product, will be the Consumer´s responsibility.

5. The warranty will totally lose its validity in the occurrence of any of the following hypotheses: a) if the defect is not of manufacturing, but caused by the Consumer or by third parties not related to the manufacturer; b) if the damage to the product comes from accidents, disasters, nature agents (lightning, flooding, landslides, etc.), humidity, voltage in the electrical network (overvoltage caused by accidents or excessive fluctuations in the network), installation/use in disagreement with the user's manual or resulting from the natural wear and tear of the parts and components; c) if the product has suffered chemical, electromagnetic, electrical or animal (insects, etc.) influence; d) if the product's serial number has been tampered with or scraped; e) if the device has been breached.

6. This warranty does not cover data loss, therefore it is recommended, if applicable to the product, that the Consumer make a backup copy of the data on the product on a regular basis.

7. Intelbras is not responsible for the installation of this product, nor for any attempts of fraud and/or sabotage of its products. Keep the software updates and applications used up-to-date, if relevant, as well as the network protections required for protection against intrusions (hackers). The equipment is guaranteed against vices within its normal conditions of use, and it is important to be aware that, because it is electronic equipment, it is not free of frauds and scams that may interfere with its correct operation.

These are the conditions of this Supplementary Warranty Agreement, and Intelbras S/A reserves the right to change the general, technical, and aesthetic characteristics of its products without prior notice.

All images in this manual are illustrative.

Product benefited by the Computer Law.

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br (http://forum.intelbras.com.br)

Suporte via chat: intelbras.com.br/suporte-tecnico (http://www.intelbras.com.br/suporte-tecnico)

Suporte via e-mail: suporte@intelbras.com.br

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001

www.intelbras.com.br (http://www.intelbras.com.br)

Indústria Brasileira