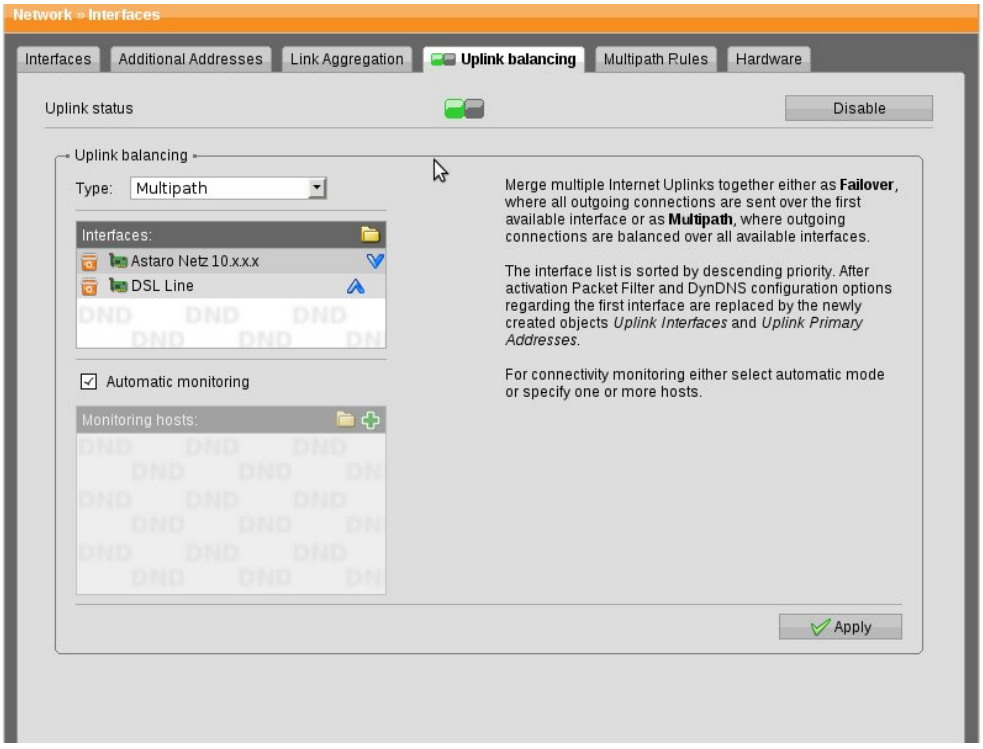
# Config Guide zu Uplink Load Balancing, Multipath und Failover

# 1. Introduction

The guides contain complementary information on the Administration Guide and the Online Help. If you are not sure whether you have the current version of this guide, you can download it from the following Internet address:
**http://www.astaro.com/kb**
If you have questions or find errors in the guide, please, contact us under the following e-mail address:
**documentation@astaro.com**
For further help use our support-forum under ...
**http://www.astaro.com**
... or use the Astaro Support offers ...
**http://www.astaro.com/support**

# 2. Uplink Balancing

With the upload balancing function you can combine more than one Internet uplink, either for having backup uplinks available or for using load balancing among multiple uplinks. Combining up to eight different uplinks is supported.




To use uplink balancing, proceed as follows:

1. **Enable uplink balancing.**
   You can either click the status icon or the Enable button.
   The status icon turns amber and the Uplink Balancing area becomes editable.

**2. Select the balancing type.**

From the Type drop-down list select the uplink type you want to use:

- **Failover:** In addition to the primary uplink interface one or more backup Internet uplinks operate in standby mode. All traffic is sent over the first active interface. In case of failure the uplink interface is automatically switched over to the next available interface.
- **Multipath:** All interfaces operate in active mode, and traffic is balanced automatically over all available interfaces. In case of failure the corresponding interface is excluded. Balancing is based on source IP address with a persistence time of one hour. If the interval between two requests from the same source IP address exceeds this interval the balancing is redecided. The traffic distribution is based on a simple round-robin algorithm.

**3. Add interfaces to use.**

Add or select at least two interfaces that should be used for uplink balancing.

Note – The sequence of the interfaces is important, especially for failover: In case of an unresponsive server the first interface following this interface is selected. You can change the interface sequence by clicking the blue arrows in the Interfaces box.

**4. (Optional) Monitoring:**

By default Automatic Monitoring is enabled to detect possible interface failures. This means that the health of all uplink balancing interfaces is monitored by having them ping a random host on the Internet at an interval of 15 seconds. If a host does not ping anymore the respective interface is regarded as dead and not used anymore for distribution.

You can define the hosts to ping by the server pool yourself:

1. **Deselect the Automatic Monitoring checkbox.**
   The Monitoring Hosts box becomes editable.
2. **Add hosts to ping.**
   Select or add one or more hosts that you want to ping instead of random hosts.

**5. Click Apply.**

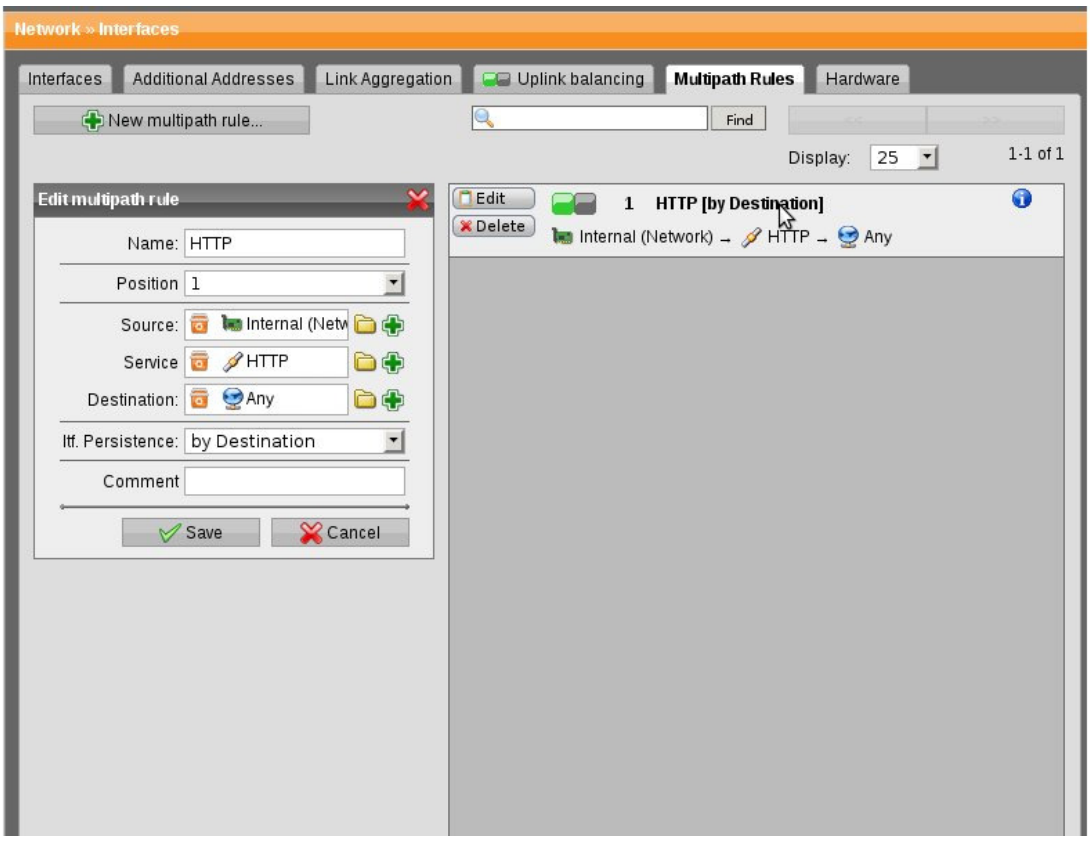
Your settings will be saved.

A new virtual network interface named Uplink Interfaces is automatically created and now available for use by other functions of the Astaro Security Gateway, e.g. IPSec rules. The virtual network interface Uplink Interfaces comprises all uplink interfaces added to the interface list.
Additionally, a new network group named Uplink Primary Addresses is automatically created and now available for use by other functions of the Astaro Security Gateway, e.g. packet filter rules. It refers to the primary addresses of all Uplink Interfaces.

In case of an interface failure, open VPN tunnels can be automatically re-established over the next available interface provided DynDNS is used or the remote server accepts the IP adresses of all uplink interfaces. As a prerequisite, the IPSec rule must use the Uplink Interfaces as Local Interface.

# 3. Multipath Rules

On the Network >> Interfaces >> Multipath Rules tab you can set rules for multipath if you use the multipath mode for uplink balancing.




To create a multipath rule, proceed as follows:

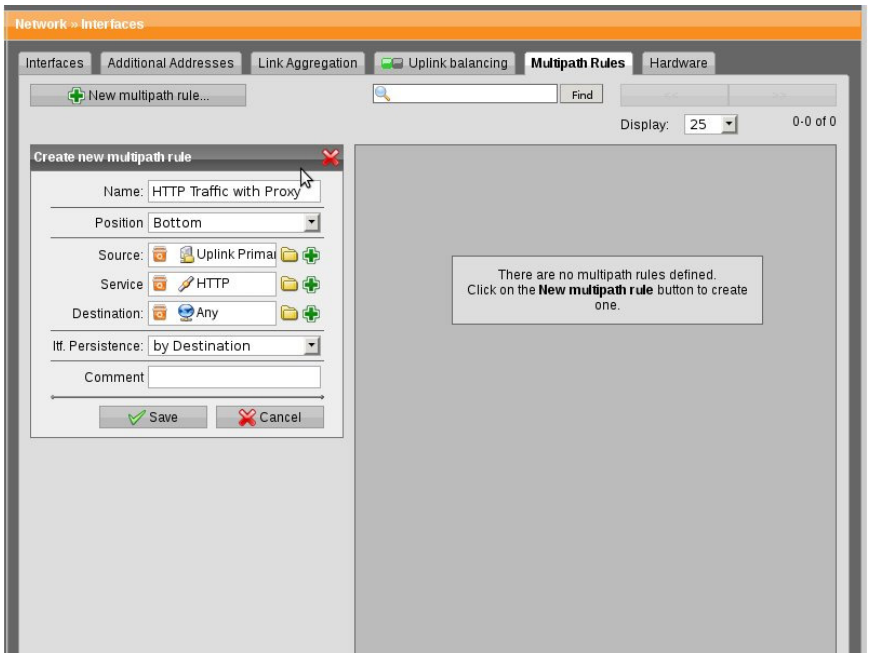
1. **On the Multipath Rules tab, click New Multipath Rule.**
   The Create New Multipath Rule dialog box opens.
2. **Make the following settings:**
   **Name:** Enter a descriptive name for the multipath rule.
   **Source:** Select or add a source IP address or network to match.
   **Service:** Select or add the network service to match.
   **Destination:** Select or add a destination IP address or network that should be used for routing.
   **Itf. Persistence:** Interface persistence is a technique which ensures that subsequent connections from a client are always routed over the same uplink interface. Persistence has a default timeout of one hour. You can decide what should be the basis for persistence:
   - **By Connection:** Each connection is balanced independently.
   - **By Source (Default):** Balancing is based on the source IP address.
   - **By Destination:** Balancing is based on the destination IP address.
   - **By Source/Destination:** Balancing is based on the source/destination IP address combination.
   - **By Interface:** Select an interface from the Bind Interface drop-down list. All traffic applying to the rule will be routed over this interface. In case of an interface failure and no other matching rules the connection falls back to default behavior.

(Optional) Comment: Add a description or other information about the multipath rule.

3. **Click Save.**
   The new multipath rule is added to the Multipath Rules list. To either edit or delete the rule, click the corresponding buttons.
4. **Enable the rule.**
   The new multipath rule is disabled by default. Click the status icon to activate the , rule. The rule is now enabled (status icon is green).

## *3.1 Example Multipath Rules*

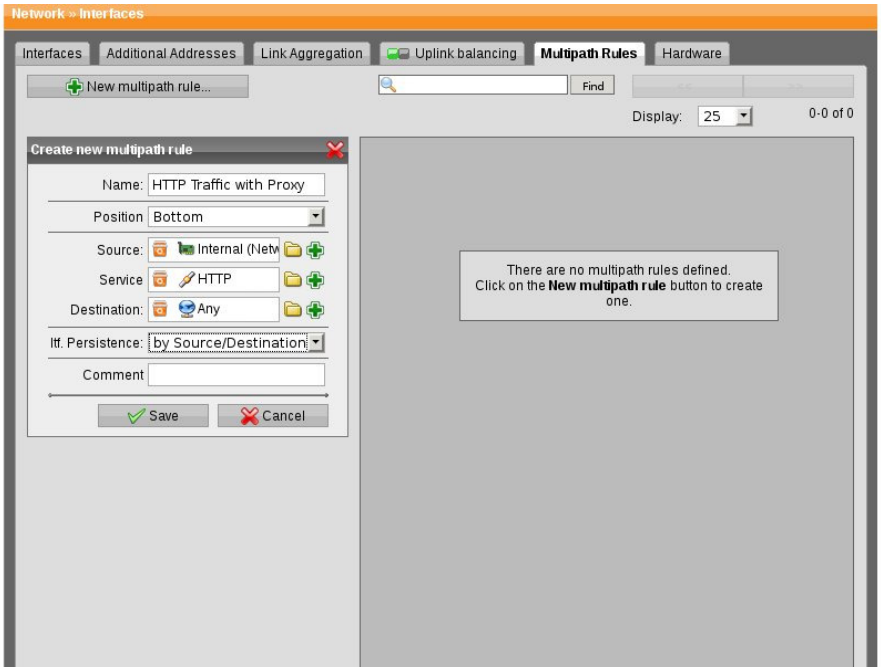
### 3.1.1 HTTP Traffic with Proxy




To create the a multipath rule, proceed as follows:

1. **On the Multipath Rules tab, click New Multipath Rule.**
   The Create New Multipath Rule dialog box opens.
2. **Make the following settings:**
   **Name:** HTTP Traffic with Proxy
   **Source:** Uplink Primary Addresses
   **Service:** HTTP
   **Destination:** Any
   **Itf. Persistence:** By Destination
   (Optional) Comment: Add a description or other information about the multipath rule.
3. **Click Save.**
   The new multipath rule is added to the Multipath Rules list. To either edit or delete the rule, click the corresponding buttons.
4. **Enable the rule.**
   The new multipath rule is disabled by default. Click the status icon to activate the , rule. The rule is now enabled (status icon is green).

## 3.1.2 HTTP Traffic without Proxy




To create the a multipath rule, proceed as follows:

1. **On the Multipath Rules tab, click New Multipath Rule.**
   The Create New Multipath Rule dialog box opens.
2. **Make the following settings:**
   **Name:** HTTP Traffic without Proxy
   **Source:** Internal (Network)
   **Service:** HTTP
   **Destination:** Any
   **Itf. Persistence:** By Source/Destination
   (Optional) Comment: Add a description or other information about the multipath rule.
3. **Click Save.**
   The new multipath rule is added to the Multipath Rules list. To either edit or delete the rule, click the corresponding buttons.
4. **Enable the rule.**
   The new multipath rule is disabled by default. Click the status icon to activate the , rule. The rule is now enabled (status icon is green).