How to Create Interface Groups

https://campus.barracuda.com/doc/73719284/

Processing of access rules does not necessarily need to be associated with the physical network environment on the box level of a CloudGen Firewall. On systems equipped with multiple network interfaces, you can explicitly define specific interfaces for usage when a rule comes into action.

An interface group specifies the interface that the source address is allowed to use. When you create access rules, you can use predefined groups, or if you want to reference custom interfaces that are not in the default list, you can create custom interface groups. For each rule an interface may be assigned to origin and destination of the connection request when selected in the Connection Objects settings.

Predefined Interface Groups

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. From the left menu, expand the **Firewall Objects** menu and select **Interface Groups**.

The following predefined network interface objects are available for selection:

- **Any** – With this setting the first interface matching the request is utilized for the connection in accordance with routing configuration. The packet source is not verified. Reply packets might be forwarded through another interface, if multiple interfaces capable of doing so are available. Not to check the physical source of packets might sometimes be needed in very special configurations.
  For security reasons do not use this setting without explicit need.
- **Matching** (default) – This setting ensures that arriving packets are processed through the same interface, which will forward the corresponding reply packets. Source and destination addresses are thus only reversed. This method aims at preventing a network attack, in which an attacker might try using internal addresses from outside the internal network (IP spoofing).
  With eventing activated (parameter **IP Spoofing** set to **yes**), IP spoofing identification will trigger the events FW IP Spoofing Attempt Detected [4014] and FW Potential IP Spoofing Attempt [4015].
- **RAM, ADSL, DHCP, ISDN, SERIAL, 3G, ...** – Explicitly restricts rule processing to the specified dynamic network interface (if installed and configured).

Create an Interface Group

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual***

server **> Assigned Services > Firewall > Forwarding Rules**.

2. Click **Lock**.
3. Right-click the table and select **New**.
4. In the **Edit/Create an Interface Group** window, enter a descriptive **Name** for the interface group.
5. From the **Interface** drop-down list, select your desired option:
   - **match** (default) **–** This setting ensures that arriving packets are processed through the same interface, which will forward the corresponding reply packets. Source and destination addresses are thus only reversed. This method aims at preventing a network attack, in which an attacker might try using internal addresses from outside the internal network (IP spoofing).

     With eventing activated (parameter **IP Spoofing** set to **yes**), IP spoofing identification will trigger the events FW IP Spoofing Attempt Detected [4014] and FW Potential IP Spoofing Attempt [4015].
   - **any** – With this setting the first interface matching the request is utilized for the connection in accordance with routing configuration. The packet source is not verified. Reply packets might be forwarded through another interface, if multiple interfaces capable of doing so are available. Not to check the physical source of packets might sometimes be needed in very special configurations.

     For security reasons do not use this setting without explicit need.
   - **eth0 - 4** – Lets you select a specific port.
   - **dhcp** – Explicitly restricts rule processing to the specified dynamic network interface (if installed and configured).
6. Click **Add** to add the interface to the list.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.