
Custom External Network Objects

<https://campus.barracuda.com/doc/43846871/>

If you have a file containing a list of IP addresses or networks, you can import them automatically or manually into the external network objects. On Barracuda NextGen F-Series Firewalls running in the public cloud, these objects are automatically filled in with information gathered from the cloud provider.

File Format

- IP addresses must be written in CIDR notation.
- IP addresses must be separated by one whitespace.
- limited to 10.000 IP addresses per file.

In this article

Before You Begin

An admin account with full shell access is required.

Importing External IP File on a Stand-alone F-Series Firewall

Step 1. Copy the File to the F-Series Firewall





1. Copy the file containing the IP addresses to **/var/phion/home/**. Use a temporary file format to ensure that only data of completely copied files are imported into the network objects. E.g., `addresses.dirty`
2. Rename the file after the copy process:

```
# mv -f /var/phion/home/addresses.dirty /var/phion/home/addresses
```

Step 2. Import the File into a Custom External Object

On the command line enter `/opt/phion/bin/CustomExternalAddrImport -i /var/phion/home/addresses -o` in the **Command** section. E.g., `/opt/phion/bin/CustomExternalAddrImport -i /var/phion/home/addresses -o 1` to import into the **Custom External Object 1** .

Check the **CustomExternalImport** firewall log file to verify the import was successful. You can also open the **FIREWALL > Forwarding Rules** page and click on **Networks**.

| | | | | |
|---|-----------------------|---|-------------------------------|---|
|  | CustomExternalObject1 | 0 | 192.168.200.200 , 10.0.10.... | An externally provided set of addresses |
|  | CustomExternalObject2 | 0 | | An externally provided set of addresses |
|  | CustomExternalObject3 | 0 | | An externally provided set of addresses |
|  | CustomExternalObject4 | 0 | | An externally provided set of addresses |

The IP addresses and networks in the custom external network objects are not displayed on the **CONFIGURATION > Full Configuration > Virtual Servers > your virtual server > Firewall > Firewall Rules** page. Directly on the firewall go to **FIREWALL > Forwarding Rules** to see the content of the dynamic network objects.

Step 3. (Optional) Create a Cron Job for Import

Create a cron job to automatically trigger a periodic import process.

1. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > System Scheduler**.
2. Click **Lock**.
3. In the left menu, click **Daily Schedule**.
4. Click **+** to add an **Interhour Schedule** job.
5. Enter the **Name**, and click **OK**.
6. Enter `/opt/phion/bin/CustomExternalAddrImport -i /var/phion/home/addresses -o` in the **Command** section.
7. For High Availability setups, add `-h` to execute the CustomExternalAddrImport binary located in `/opt/phion/bin` and import the IP addresses to the Custom Network Object with the index number **1**. E.g., **CustomExternalObject1**
8. Select **every** from the **Minutely Schedule** drop-down list and enter the period for the **Run Every...Minutes** parameter.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

On an F-Series Firewall in the Public Cloud

If your F-Series Firewall is running in the public cloud (AWS or Azure), the custom external network objects will be automatically filled with:

- Custom external object number 1 contains the internal IP address.
- Custom external object number 2 contains the internal network address.

- Custom external object number 3 contains the external IP address.

If you are using multiple virtual network interfaces in AWS, only information for the first interface will be imported. The IP addresses will also be automatically synced to the Control Center.

On a Barracuda NextGen Control Center

Configure a cron job on the Control Center to copy the addresses file to the `/var/phion/home/` directory of your managed firewalls. Copying the files through the management tunnels does not require separate authentication as the Control Center already has a trust relationship established with the remote firewalls. On the managed firewalls create another cron job to import the addresses file every 5 minutes.

- On the Control Center, create a cron job to regularly copy the addresses file to the managed firewalls.
- On the managed firewalls, create a cron job to import the addresses.
- Do not use the **h** (HA synchronization flag)
- The predefined external objects can be copied into the global objects database and then be used throughout the firewall configuration.

Figures

1. Bild 268.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.