Network Objects

https://campus.barracuda.com/doc/53248547/

Use network objects to reference networks, IPv4 and IPv6 addresses, hostnames, geolocation objects, MAC addresses, or interfaces when you create access rules. MAC address and interface are optional components that are evaluated only when the network object is used in the source of an access rule. For all other uses, these optional parameters are ignored. A network object can also include other existing network objects. Network objects are stored in the Host and Forwarding firewall. If the F-Series Firewall is managed by a NextGen Control Center, it also inherits all network objects in the **Global**, **Range**, and **Cluster Firewall Object** stores.

Access rule management is simplified with the use of network objects instead of explicit IP addresses. For example, if an IP address changes, you do not have to edit it in every rule that references it; you only need to change the IP address in the network object. The IP address is then automatically updated for every rule that references the network object.

Unified networks objects cannot contain both IPv4 and IPv6 addresses. For more information, see IPv6.

Network Object Types

A network object can consist of the following:

- **Generic IPv4 Network Objects** – You can add network addresses of all types. All default network objects are generic IPv4 network objects.
- **Single IP Address** – A single IP address.
- **List of IP Addresses** – Multiple single IP addresses and/or references to other single IP address objects. For example: `10.0.10.1, 10.0.10.10, 10.0.10.127`
- **Single Network Address** – A single network. For example: `10.0.10.0/25`
- **List of Network Addresses** – Any combination of multiple networks, IP addresses, and/or references to other network address objects. For example: `10.0.10.0/25, 172.16.0.10`
- **Hostname (DNS Resolved)** – A single DNS-resolvable hostname. For example: `myhost.test.com`

  If the hostname used in the network object is not resolvable, any access rules that use it will never be matched to traffic. For a detailed description of configuration options, see Hostname (DNS Resolvable) Network Objects.
- **Single IPv6 Address** – A single IPv6 address.
- **List of IPv6 Addresses** – Multiple IPv6 addresses and/or references to other single IPv6 address objects.

- **Single IPv6 Network** – A single IPv6 network.
- **List of IPv6 Networks** – Any combination of multiple IPv6 networks, IPv6 IP addresses, and/or references to other IPv6 network address objects.
- **Excluded Entries** – Specific networks that are excluded from the network object.
  For transparency and consistency, other network objects cannot be referenced in the **Excluded Entry** section.
- **Enable L3 Pseudo Bridging** – When bridging is activated on an interface, host routes and PARPs are automatically created by the NextGen Firewall F-Series. In this section, you can specify the information required for this task. The Bridging section is available only in the **Local Networks** list of the Forwarding Firewall service. Select **Bridging enabled** (Advanced Settings) from the list (default: **Bridging not Enabled**) if you want to configure bridging details.
  The configuration options in the Bridging section are only applicable for layer 3 bridging. For more information, see How to Configure Layer 3 Bridging.

  - **Interface Address Reside** – The name of the interface on which bridging is to be enabled (for example, eth1).
  - **Parent Network** – The superordinate network from which the bridged interface has been separated.
  - **Introduce Routes** – Introduces host routes to the IP addresses to be separated automatically from the superordinate network (IP addresses listed in the network object).
  - **Restrict PARP to Parent Network** – Restricts the proxy ARP to answering ARP requests only within the parent network.

Network objects cannot be deleted if they are referenced by other objects. You can delete network objects when they are only referenced in configuration files. Before you delete a network object, verify that it is not used anywhere. The **Referenced By** column in the **Network Objects** listing displays where a network object is currently referenced.

Create Network Objects

Create network objects that refer to IP addresses, other network objects, and / or networks. Network objects are re-usable, which means that you can use one object in as many rules as required.

For more information, see How to Create Network Objects.

Hostname Network Objects

Hostname (DNS resolvable) network objects can be used in access rules where the source or

destination IP addresses are dynamically assigned. In hostname network objects, IP addresses are determined by DNS resolution.

For more information, see Hostname (DNS Resolvable) Network Objects.

Geolocation-based Network Objects

Geolocation-based network objects allow administrators to create access rules based on the physical location of the source or destination IP address and network.

For more information, see How to Create a Geo Location based Network Object.

Wildcard Network Objects

Wildcard network objects determine which parts of an IP address are evaluated. This is useful for IP addresses that cannot be covered by network objects using subnets masks.

For more information, see How to Create Wildcard Network Objects.

Custom External Network Objects

When creating custom external network objects, you can import a file containing a list of IP addresses or networks. You can also create a cronjob to automatically trigger a periodic import process.

For more information, see Custom External Network Objects.

Import Network Objects

Static network objects can be imported and updated from a CSV file that contains the network object data in plain text. You can import firewall objects in the Forwarding, Host, or Distributed Firewall and on the NextGen Control Center.

For more information, see How to Import Network Objects from a CSV File.

For F-Series Firewalls in the Public Cloud

If your F-Series Firewall is running in the public cloud (AWS or Azure), the following dynamic network objects are created and filled automatically as long as Cloud Integration is configured:

- **CloudBox.PrivateIp** – Contains the internal IP address.
- **CloudBox.LocalSubnet** – Contains the internal network address.
- **CloudBox.PublicIp**– 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.