Firewall Objects

https://campus.barracuda.com/doc/98210250/

Firewall objects are named collections that represent specific networks, services, applications, user groups or connections. You can use the firewall objects that are preconfigured on the Barracuda CloudGen Firewall, but you can also create custom firewall objects depending on your requirements. Firewall objects are re-usable which means that you can use one firewall object in as many rules as required. The following section explains the available firewall objects and contains articles on how to create the different firewall objects for use in your access and application rules.

Advantages of Firewall Objects

Using firewall objects gives you the following advantages:

- Each firewall object has a unique name that is more easily referenced than, for example, an IP address or a network range.
- Maintenance of the access and application rule set is simplified. When you update a firewall object, the changes are automatically updated in every rule that refers to this object.

Firewall Object Types

The following types of firewall objects and policies are available for use and configuration:

- **Connection Objects** – The egress interface and source (NAT) IP address for traffic matching an access rule.
  For more information, see Connection Objects.
- **Proxy ARPs** – Resolve MAC addresses not physically on the CloudGen Firewall to the corresponding IP addresses.
  For more information, see Proxy ARPs.
- **Network Objects** – Networks, IP addresses, geolocation, host names, or interfaces when configuring firewall rules.
  For more information, see Network Objects.
- **Named Networks** – Transfer subnetting information and reserved IP addresses to the firewall configuration in a human-readable form. Named Networks can be used for both ruleset evaluation and visualization.
  For more information, see Named Networks.
- **Service Objects** – TCP/UDP ports for a service.
  For more information, see Service Objects.
- **User Objects** – Lists of users and/or user groups for use within firewall rules.
  For more information, see User Objects.

- **Schedule Objects** – Time restriction or scheduling tables that can be applied to access rules on an hourly, weekly, or calendar date basis.
  For more information, see Schedule Objects.
- **Interface Groups** – A specific interface or interface group containing one of more interfaces.
  For more information, see How to Create Interface Groups.
- **Applications** – Lists of applications and/or sub-applications when creating application aware firewall rules.
  For more information, see Application Objects and Application Control.
- **URL Filter** – Access restrictions for web sites. The CloudGen Firewall provides a predefined list of URL categories that are available for block-listing and allow-listing.
  For more information, see How to Create a URL Filter Policy Object and How to Create a URL Filter Match Object.
- **File Content Policies** – Filter files downloads or email attachments based on their file type, name or MIME type.
  For more information, see How to Create File Content Policies.
- **User Agent Policies** – Filter web traffic based on the information contained in the user agent string.
  For more information, see How to Create User Agent Policies.