Firewall Objects

https://campus.barracuda.com/doc/72516535/

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 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.

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 ruleset 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.
- **Network Objects** – Networks, IP addresses, geolocation, host names, or interfaces when configuring firewall rules.
  For more information, see Network Objects.
- **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.
- **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 websites. The CloudGen Firewall provides a predefined list of URL categories that are available for blacklisting and whitelisting.
  For more information, see How to Create a URL Filter Policy Object.