Firewall Objects

https://campus.barracuda.com/doc/41103452/

Firewall objects are named collections that represent specific networks, services, applications, user groups or connections when creating access rules. You can use the firewall objects that are preconfigured on the Barracuda NextGen Firewall X-Series, 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 firewall objects that are available for use and configuration on the NextGen Firewall X-Series and contains articles on how to create the different firewall objects for your access 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 e.g. an IP address or a network range.
- Maintenance of the access 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 are available for use and configuration:

- **Network Objects** — Reference networks, IP addresses, or interfaces when configuring firewall access rules.
- **URL Policy Objects** — (requires a Barracuda Web Security Subscription) Reference access restrictions for web sites. The NextGen Firewall X-Series provides a predefined list of URL categories that are available for blacklisting and whitelisting.
- **Service Objects** — Create service objects to reference TCP/UDP ports for a service.
- **Connection Objects** — Reference the egress interface and source (NAT) IP address for traffic matching a firewall access rule.
- **NAT Objects** — Map IP addresses from one IP address range to another, e.g., to let two subnets communicate with each other.
- **User Objects** — Reference lists of users and/or user groups for use within access rules.
- **Schedule Objects** — Configure time restriction or scheduling tables that can be applied to access rules on an hourly, weekly or calendar date basis.
- **Application Objects** — Reference lists of web applications and/or sub-applications when creating application aware firewall access rules. For more information, see Application Control.