Hostname (DNS Resolvable) Network Objects

https://campus.barracuda.com/doc/73719273/

Hostname or DNS-based network objects are network objects where the IP addresses are determined by DNS resolution. This is useful if you must create access rules where the source or destination are dynamically assigned IP addresses. The Firewall service resolves the hostname and uses up to 24 IPv4 or up to 17 IPv6 addresses, in the order they were returned, in the network object. These IP addresses are then used by the firewall service when matching traffic against access rules using hostname network objects. The resolved IP addresses are cached internally until the **DNS Lifetime** set in the network object expires (default 600 seconds). If the hostname is not resolvable, or the DNS server is currently not available, the access rule never matches. Hostname network objects can be used in both the host and forwarding firewall rulesets. Creating hostname network objects directly in the access rule using **explicit** is not possible.

Limitations and Drawbacks

There are several limitations and drawback to using hostnames in network objects:

- The firewall itself must be able to resolve the DNS entries. For more information, see How to Configure DNS Settings.
- Only explicit host names can be used. E.g., `www.barracuda.com`
- A maximum of 24 IP addresses per network object can be resolved.
- The IP addresses are entered into the network object in the order the DNS response is received. In the extreme case of 24 IPv4 and 17 IPv6 addresses, this may lead to the network object containing only iPv4 or IPv6 addresses.
- To use more than 512 hostname network objects, you must increase the **Max DNS Entries** in the General Firewall configuration.
- Using a hostname network object in a **BLOCK** access rule is not recommended because the rule will never match if the DNS server is not available or if the hostname is not resolvable.
- When a non-resolvable object is used in a rule, rules cannot be matched or processed correctly. Hostname objects become non-resolvable when they refer to a non-existent host name or the DNS server is unavailable.
- Active sessions are not re-evaluated when DNS resolution changes; sessions are re-evaluated only when the rule itself is modified. To establish new connections with updated DNS entries, you must manually terminate persistent sessions on the **Firewall > Live** page.
- When the firewall is started or restarted, it can take up to 10 seconds until DNS resolution is provided for all configured hostname network objects. Because the firewall is already active, the traffic that you want to be handled by the rule with the added hostname object can be matched to another rule instead.
- Changes to a DNS record between DNS lookups cause the access rules to match on the wrong IP addresses.

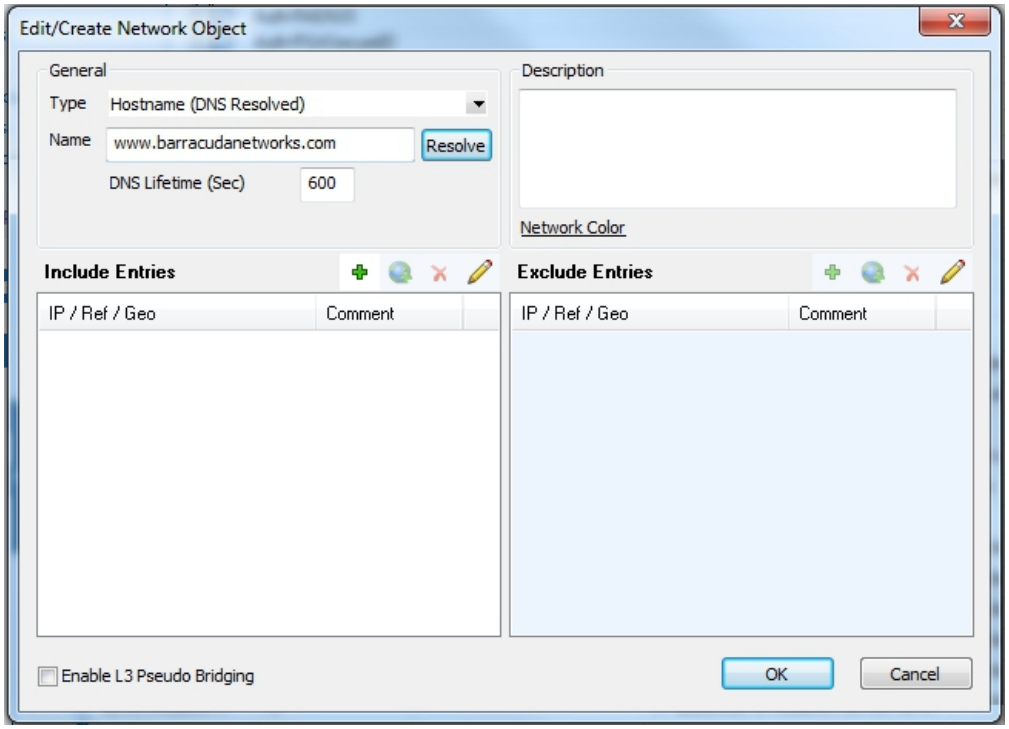
Creating Hostname Network Objects

You can create hostname objects:

- In the Local Firewall ruleset.
- In the Forwarding Firewall ruleset.
- As global, range-specific, or cluster-specific firewall objects.

Hostname objects cannot be created as explicit source or destination objects in access rules.

To create a hostname network object, select **Hostname (DNS resolved)** from the **Type** list in the **Network Object** window. Consider the following detail configuration options:



You can configure the following parameters:

- **Type** – The type defines specific object characteristics. Network objects of type Hostname expect specification of an explicit DNS resolvable hostname in the **Name** field below.
  After the object has been created, its type cannot be changed.

- **Name** – In this field, insert the DNS resolvable name the object is to be created for.
- **Description** – In this field, insert a significant object description.

The specified name is also the name of the network object. The object name may be changed retroactively.

- **Resolve** – The functionality of this button is purely informational. Click it to execute a DNS query for the hostname inserted in the **Name** field. The result of the query is displayed in the IP field in the **Entry** section. Note that the query is executed using the DNS server(s) known to the client running Barracuda Firewall Admin and NOT using the DNS server(s) known to the CloudGen Firewall running the firewall service.
- **DNS Lifetime (Sec)** – The DNS Lifetime defines the interval after which you must refresh DNS entries for network objects of type **Hostname** that are configured for use in currently effective access rules (default: 600 s). Setting to a lower value than 30 seconds might cause problems in network object lists containing a huge number of hostname objects. DNS entries may also be refreshed manually in **FIREWALL** > **Dynamic** > **Dynamic Rules**.

  The DNS Lifetime has no effect on actively established connections, even if the DNS resolution of a network object that is currently used in an access rule changes. In this case, to force a refresh, you must terminate the active session in order to enable a new connection establishment using the updated DNS entry.
- The **Include** and **Exclude Entries** sections may be used to restrict a network object and to force a condition to match explicitly or to exclude it from being part of it. For example, if a DNS hostname entry www.domain.com matches four DNS A-records pointing to the IP addresses 10.0.6.1, 10.0.8.1, 10.0.8.2 and 10.0.8.3, and you want connection requests to always point to addresses residing in the 10.0.8.0/24 network, but never be addressed to the IP address 10.0.8.3, the following values need to be configured in the corresponding fields: Section **Included Entry**: IP 10.0.8.0/24, section **Excluded Entry**: IP 10.0.8.3. The configuration stated above will be processed as follows, when it is utilized in an access rule: Connection requests may be addressed to IP addresses living in the network 10.0.8.0/24, but they may not address the excluded IP address 10.0.8.3.

Using Hostname Network Objects

You can use hostname objects as:

- **Source/Destination** in rules within the Forwarding Firewall.
- **Source/Destination** in rules within the Local Firewall.
- **Reference** in the **Entry** list of generic network objects.

You cannot reference hostname objects in other network object types.

Monitoring Network Objects of Type Hostname

DNS queries addressed to the DNS server configured in the box settings are triggered when a

hostname network object is created. You can view these queries in the following places:

> In all views but the **Dynamic Rules** tab, DNS resolution is retrieved using the DNS server(s) known to the client running Barracuda Firewall Admin and NOT using the DNS server(s) known to the CloudGen Firewall running the firewall service.

- In the **Entries** column in the network object list.
- In the **Rule Object** list when the hostname object configured in the rule is used.
- In the **Source/Destination** window querying the rule object list when the hostname object is currently used.
- In the **Rule Tester**.
- In the **Dynamic Rules** tab of the **Firewall Monitoring** Interface.

Site-specific Network Objects

Site-specific network objects can be used to share single access rulesets for branch offices with a template-based network layout. This type of object inherits its content from the IP address or IP network defined in the virtual server's **Server Properties** of a branch office.

Figures

1. net_host_new.png