Hostname (DNS Resolvable) Network Objects

https://campus.barracuda.com/doc/43846939/

You can use hostnames in a network object. This might be needed in contexts where the remote network uses a dynamic IP address and can only be reached by hostname. The Firewall service resolves and uses the first 24 IP addresses in the network object. The firewall rule set uses these resolved IP addresses when evaluating rules. If the hostname is not resolvable or the DNS server is currently not available, the access rule will never match.

In this article:

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

- Only explicit host names can be used. For example: `www.barracuda.com`
- A maximum of 24 IP addresses can be resolved
- Using a hostname network object in a **BLOCK** access rule is not recommended.
- 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.

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.

To use hostname network objects, you must specify a DNS server in the **DNS Server IP** field in the **Box Settings** file (How to Configure DNS Settings).

Using DNS resolvable host names in firewall rule sets can cause problems because of the following:

- IP addresses that are allocated to DNS host names might change.
- A DNS record might contain multiple IP addresses.

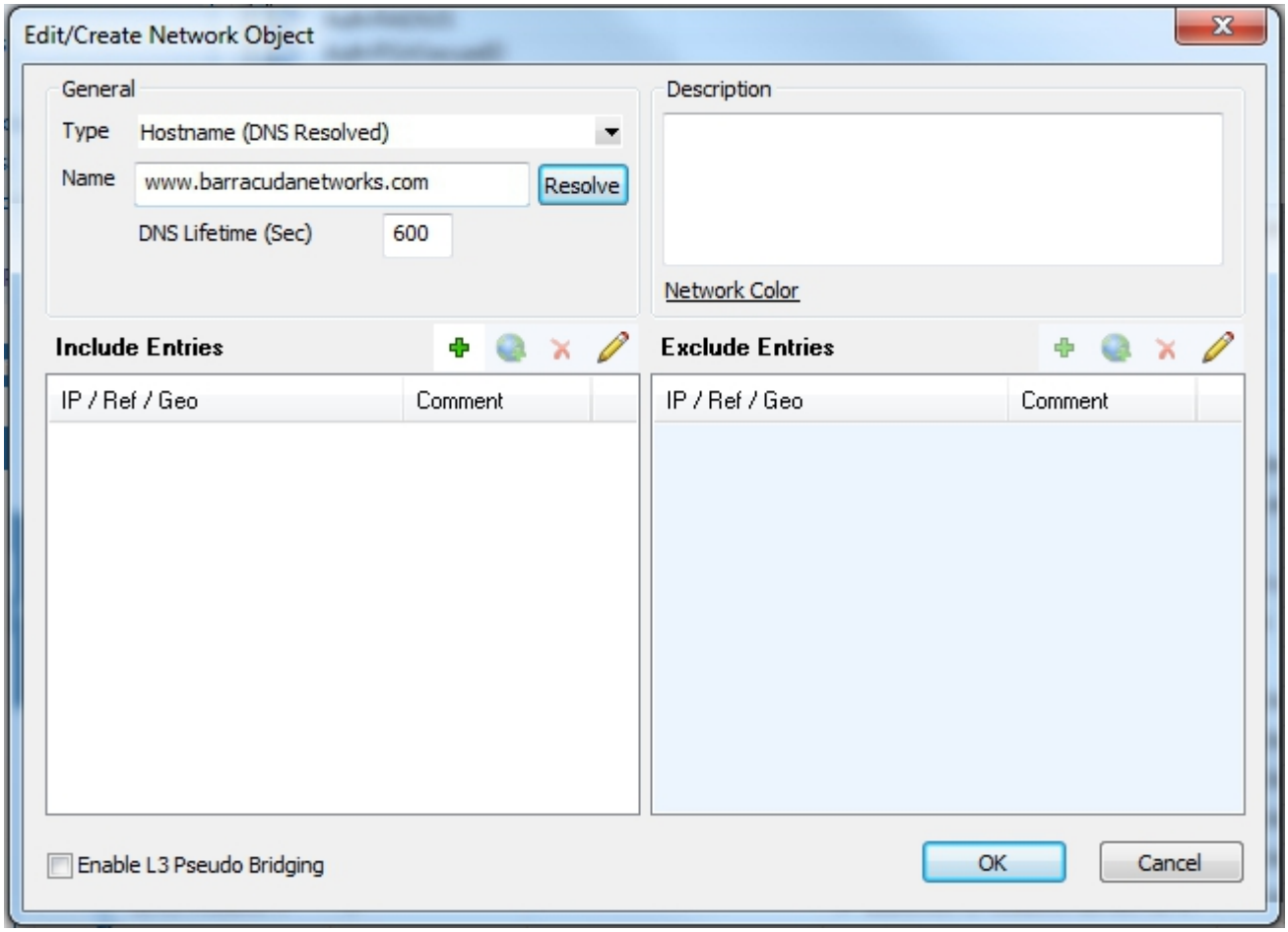
Creating Hostname Network Objects

You can create hostname objects:

- In the Local Firewall rule set.
- In the Forwarding Firewall rule set.
- 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 host name in the **Name** field below.
  Once the object has been created its type cannot be changed.

- **Name** – Into this field insert the DNS resolvable name the object is to be created for.
- **Description** – Into this field insert a significant object description.
  The specified name is the name of the network object at the same time. 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 host name inserted into 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 the graphical administration tool Barracuda NG Admin and NOT using the DNS server(s) known to the Barracuda NG Firewall running the firewall service.

- **DNS Lifetime (Sec)** – The DNS Lifetime defines the interval after which to 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 a access rule changes. In this case to force a refresh terminate the active session in order to enable 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 host name 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 it is wanted that connection requests must always point to addresses residing in the 10.0.8.0/24 network, but must 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 a 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 the graphical administration tool Barracuda NG Admin and NOT using the DNS server(s) known to the Barracuda NG 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 firewall rule sets for branch offices with 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