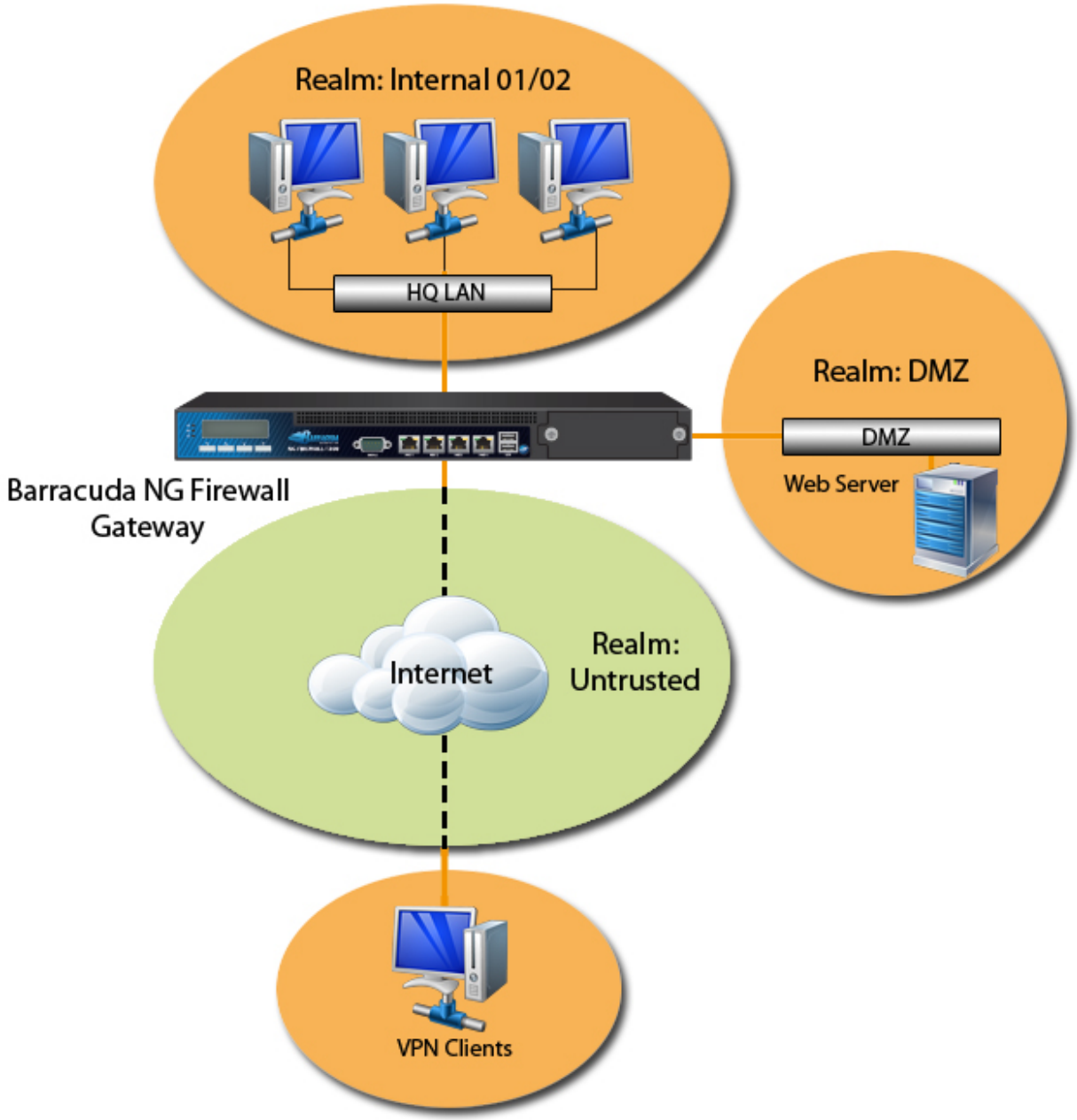
# Protected IP Count Policies

https://campus.barracuda.com/doc/43847002/

Barracuda NG Firewall VF and SF units are licensed based on the number of IP addresses being protected by the gateway. For more information, see Licensing. This article explains the algorithms that are used to count the protected IP addresses. It also provides instructions on how to specify counting policies when creating and configuring firewall rules.

**In this article:**

**Protected and Unprotected Realms - General Overview:**




## Viewing the Number of Protected IPs

To view the number of protected IP addresses for a Barracuda NG Firewall, go to the **FIREWALL** > **Dynamic** page and click the **Protected IPs** tab. The table on this page provides information on the number of active licensed IP addresses. For more information on the **FIREWALL** > **Dynamic** page, see Dynamic Page.

## Counting Policies

The following sections describe how IP addresses are counted for each type of connection.

#### General Case

Generally, the protected IP address counted is either the source or destination address, based on a comparison of the classification of incoming and outgoing interfaces. The valid preference is the following:

1. **Internal (LAN)**
2. **DMZ**
3. **Unspecified**
4. **External**

For example, if the realm weight is the same from Internal01 to Internal02, the source IP address is counted. The same applies, vice versa, from Internal02 to Internal01.

### Classification of Incoming and Outgoing Interfaces:

| Incoming | Outgoing | | | |
|---|---|---|---|---|
| | **Trusted / Internal01/02** | **DMZ** | **Unclassified** | **Untrusted** |
| **Trusted / Internal01/02** | Src | Src | Src | Src |
| **DMZ** | Dst | Src | Src | Src |
| **Unclassified** | Dst | Dst | Src | Src |
| **Untrusted** | Dst | Dst | Dst | Src |

On the **Network** page, you can specify the realm category of an IP address:

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the **IP Address Configuration** table, double-click the IP address entry and select the realm weight from the **Trust Level** list.

For more information on configuring IP addresses, see Network.

#### Uncounted IP Addresses

The following IP addresses are NOT taken into account:

- Source AND destination are site-to-site tunnel addresses (VPN relaying - VPN Tunnels in Star-

Shaped Topologies).
- Destination is a broadcast or multicast address.
- Firewall rule results in a **Block** or **Deny** action.
- Customers with legacy phion SF licenses, VPN users, and HTTP Proxy users are also not counted.

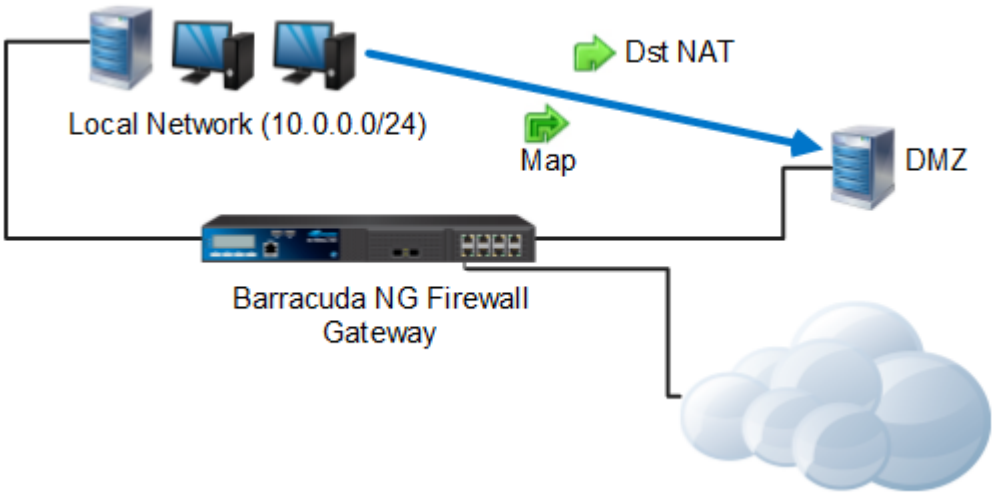
Any communication directed to the services running on the Barracuda NG Firewall gateway itself is not counted:

- Mail Gateway
- DNS Server/Forwarder
- DHCP Server

#### Redirected Destination

If a redirection of the destination IP address is performed by the firewall rule (Dst NAT or Map), the translated destination IP address is counted as protected.

### Policy for Redirected Destination:



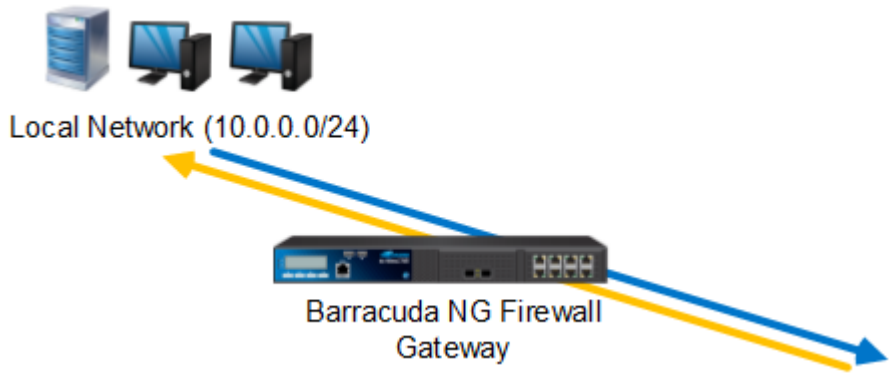

#### Site-to-Site VPN

The counting preference of protected IP addresses for Site-to-Site VPN tunnels is specified as follows:

- Source is counted as a protected IP address if the destination is routed via the tunnel.
- Destination is counted as a protected IP address if the source originates from the tunnel.

If both options apply, neither source nor destination is counted. For more information on site-to-site tunnels, see Site-to-Site VPN.

**Example Policy for Site-to-Site tunnels:**




#### Client-to-Site VPN

Each client connected to a Client-to-Site VPN counts as one protected IP address.

#### SSL VPN

The number of protected IP addresses is taken from the client database and from configured resources such as the DMZ network. For more information, see SSL VPN. Counting is specified as follows:

- Source is counted as a protected IP address if the destination is routed via the tunnel.
- Destination is counted as a protected IP address if the source originates from the tunnel.

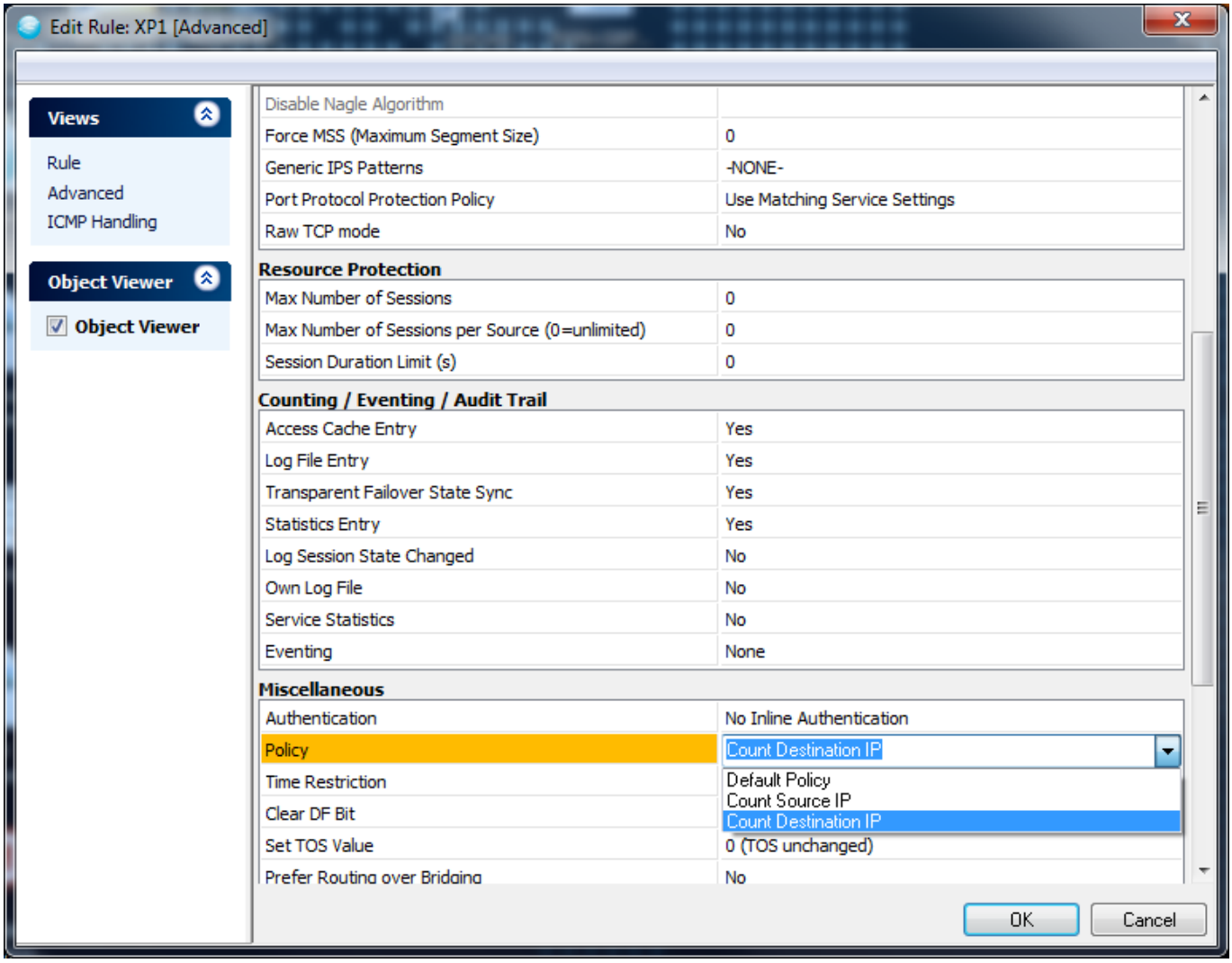
If both options apply, neither source nor destination is counted.

## Specifying Counting Policies

When creating or configuring firewall rules, you can also specify IP address counting policies in the Advanced Access Rule Settings.

1. In the left navigation pane of the firewall rule editor window, click **Advanced** from the **Views** menu.
2. In the **Miscellaneous** section, select one of the following options from the **Policy** list:
   - **Count Source IP –** Source is chosen as the protected IP address if the rule explicitly requests it.
   - **Count Destination IP –** Destination is chosen as the protected IP address if the rule explicitly requests it.

The source and destination are interchanged if the rule matches on reverse.



## Figures

1. protected_ips.jpg
2. policy_3.png
3. policy_4.png
4. edit_rule.jpg.png