How to Create a Destination NAT Access Rule

https://campus.barracuda.com/doc/72515927/

A Dst NAT access rule redirects traffic that is sent to an external IP address to a destination in the internal network. The following example shows a Dst NAT rule allowing HTTP and HTTPS access from the Internet to a server in the DMZ (172.16.0.10). The redirect target can be a single IP address or hostname, or a network object. Hostnames and IP addresses can be appended with a port number to redirect the traffic to a different port.

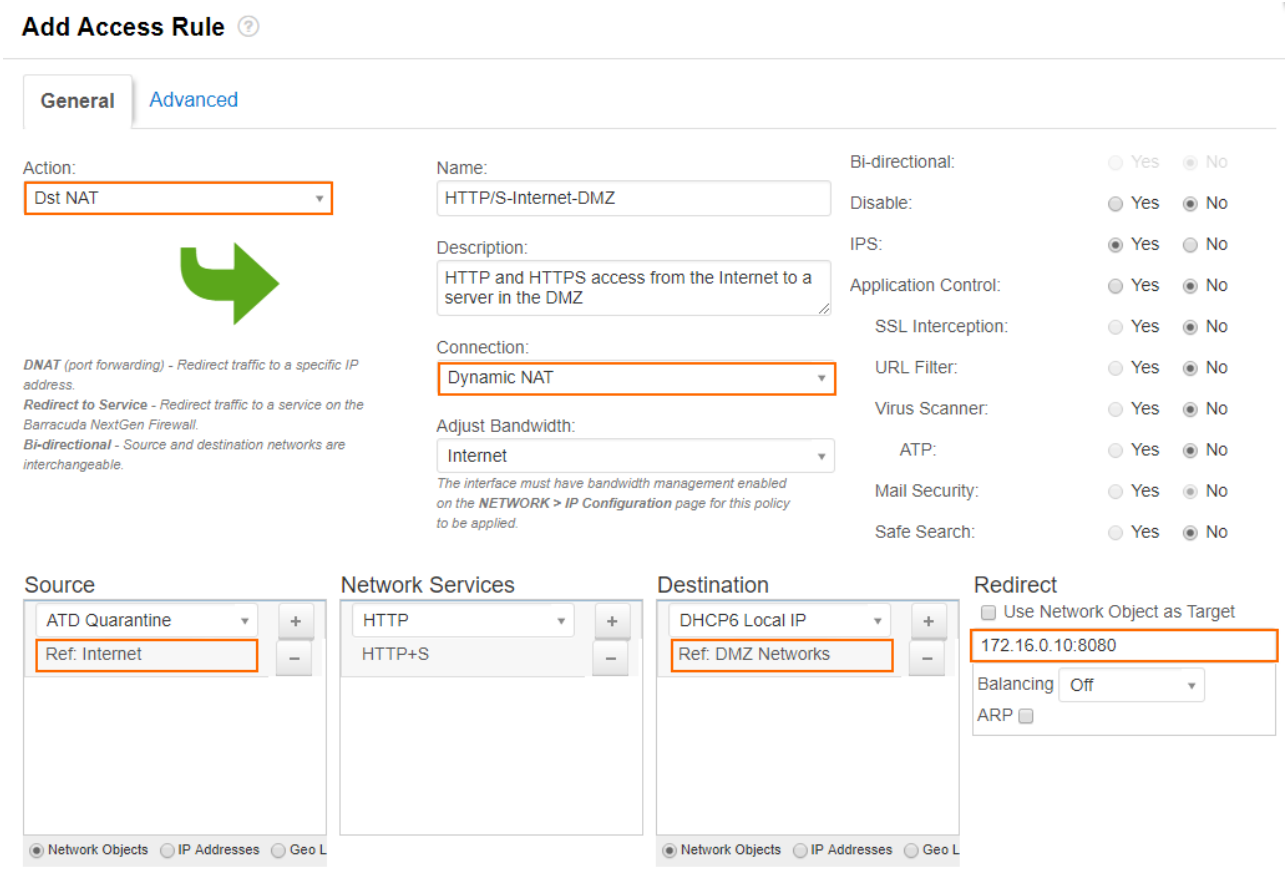
Create a Dst NAT Access Rule

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule** to create a new rule. The **Add Access Rule** window opens.
3. Select **Dst NAT** as the action.
4. Enter a **Name** for the rule. E.g., `LAN-DMZ`
5. Specify the following settings that must be matched by the traffic to be handled by the access rule, and click **+** after each entry:
   - **Connection** – Select the connection method. For more information, see Connection Objects.
   - **Source** – The source addresses of the traffic.
   - **Network Services** – Select a service object, or select **Any** for this rule to match for all services.
   - **Destination** – The destination address(es) of the traffic.
   - **Redirect** – The redirection target. You have the following options to define the target:
     - Enter one IP address with or without a specific port. If you append a port to the IP address, the firewall maps the external port to that of the internal server (port 80 to port 8080). For example, `172.16.0.10` or `172.16.0.10:8080`.
     - Enter one hostname or FQDN with or without a specific port. The firewall must be configured to be able to resolve the hostname.
     - Enter a space-delimited list of up to 32 IP addresses.
     - Select the **Use Network Object as Target** check box, and select a network object from the drop-down list that appears. If the network object contains multiple IP addresses, only the first IP address is used.

       Do not use network objects containing hostnames (DNS objects). The firewall does not redirect traffic to a hostname or FQDN.

     If you have defined multiple target IP addresses, select how the firewall distributes the traffic between the IP addresses. Select the Balancing mode:
     - **Fallback** – The connection is redirected to the first available IP address in the list.
     - **Cycle** – New incoming TCP connections are distributed evenly over the available IP addresses in the list on a per-source-IP-address basis. The same redirection target is used for all subsequent connections of the source IP address. UDP connections are redirected to the first IP address and not cycled.
6. (optional) Configure **Advanced** settings. For more information, see Advanced Access Rule

Settings.



7. Click **Save**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

Additional Matching Criteria

- **Valid for Users** – For more information, see User Objects.
- **Apply only during this time** – For more information, see Schedule Objects.

Additional Policies

- **IPS** – For more information, see Intrusion Prevention System (IPS).
- **Application Control** – For more information on Application Control features, see Application Control.
- **Adjust Bandwidth** – For more information, see Traffic Shaping.

Figures

1. dnat_rule.png