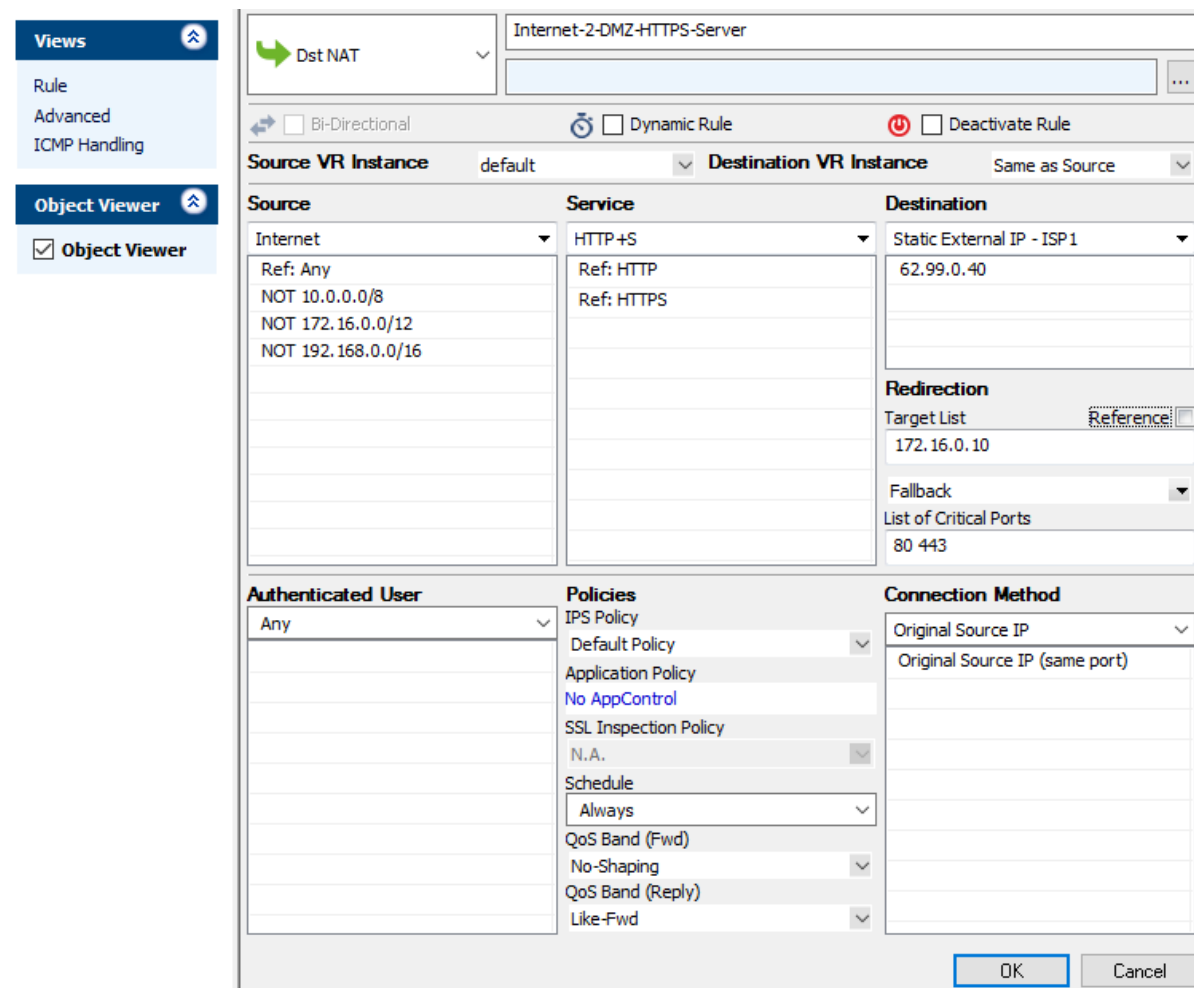


How to Create a Destination NAT Access Rule

<https://campus.barracuda.com/doc/96026196/>

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.



The screenshot shows the configuration window for a Destination NAT Access Rule. The rule is named "Internet-2-DMZ-HTTPS-Server". The configuration is as follows:

Source	Service	Destination
Internet	HTTP+S	Static External IP - ISP1
Ref: Any	Ref: HTTP	62.99.0.40
NOT 10.0.0.0/8	Ref: HTTPS	
NOT 172.16.0.0/12		
NOT 192.168.0.0/16		

Redirection

Target List: 172.16.0.10

Fallback: List of Critical Ports

80 443

Authenticated User

Any

Policies

IPS Policy: Default Policy

Application Policy: No AppControl

SSL Inspection Policy: N.A.

Schedule: Always

QoS Band (Fwd): No-Shaping

QoS Band (Reply): Like-Fwd

Connection Method

Original Source IP

Original Source IP (same port)

Buttons: OK, Cancel

Create a Dst NAT Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.



4. Select **Dst NAT** as the action.
5. Enter a **Name** for the rule. For example, Internet-2-DMZ-HTTPS-Server.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
 - **Source** – The source addresses of the traffic.
 - **Destination** – The destination addresses of the traffic.
 - **Service** – Select a service object, or select **Any** for this rule to match for all services.
 - **Target List** – 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 a space-delimited list of up to 32 IP addresses.
 - Click the **Reference** 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.
 - **Fallback/Cycle** – If you have defined multiple target IP addresses, select how the firewall distributes the traffic between the IP addresses.

This option is not selectable when a reference is defined as the redirection target. If failover or cycle is desired, you must configure the target without reference.

 - **Fallback** – The connection is redirected to the first available IP address in the list. This option prioritizes TCP sessions.
 - **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. New TCP connections and new UDP sessions are distributed evenly.
 - **List of Critical Ports** – Enter a space-delimited list of ports used. By default, the available/unavailable policy considers all ports of the allowed rule services. If a connection to such a port fails, the target is marked unavailable and the rest of the targets are used as the new list. If there are entries in the critical ports list, only failed connections to these ports lead to a state change of the respective target from available to unavailable. Separate multiple critical port entries with a space.
 - **Connection Method** – For more information, see [Connection Objects](#).
7. Click **OK**.
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.
9. Click **Send Changes** and **Activate**.

Additional Matching Criteria

- **Authenticated User** – For more information, see [User Objects](#).

Additional Policies

- **IPS Policy** – For more information, see [Intrusion Prevention System \(IPS\)](#).
- **Application Control** – For more information on all Application Control features, see [Application Control](#).
- **SSL Inspection Policy** – For more information, see [SSL Inspection in the Firewall](#).
- **Schedule Objects** – For more information, see [Schedule Objects](#).
- **QoS Band (Fwd) or QoS Band (Reply)** – For more information, see [Traffic Shaping](#).

Figures

1. FW_DNAT.png
2. FW_Rule_Add01.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.