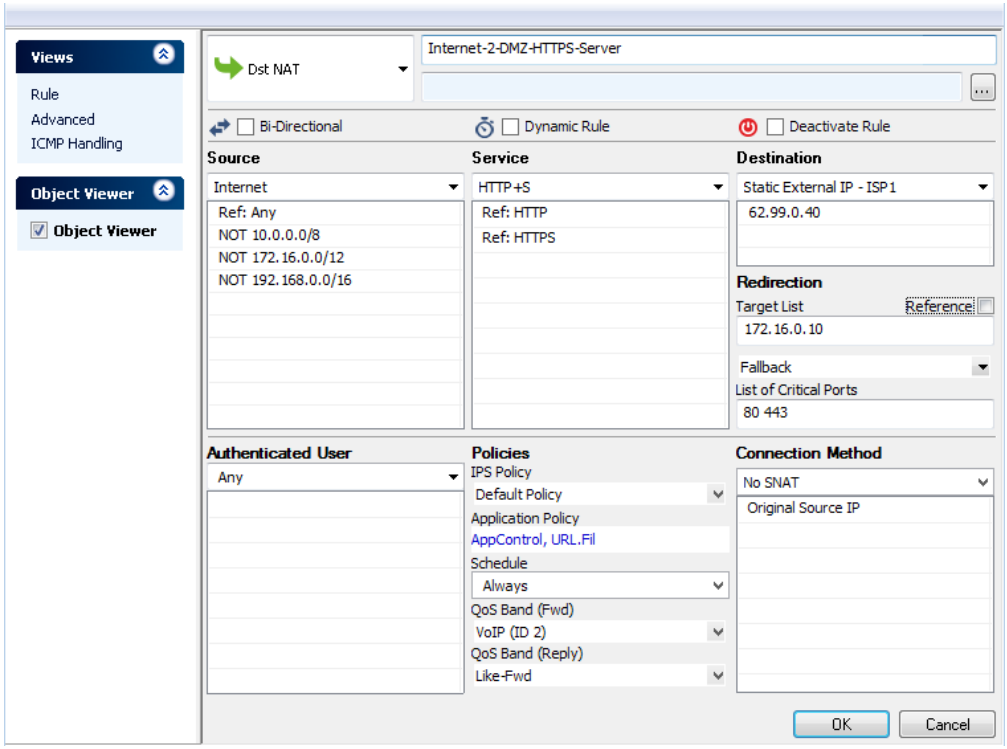
How to Create a Destination NAT Access Rule

https://campus.barracuda.com/doc/53248332/

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 **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > 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 F-Series 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.
  - **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.
- **List of Critical Ports** – Enter a space-delimited list of ports used.
- **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.
- **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