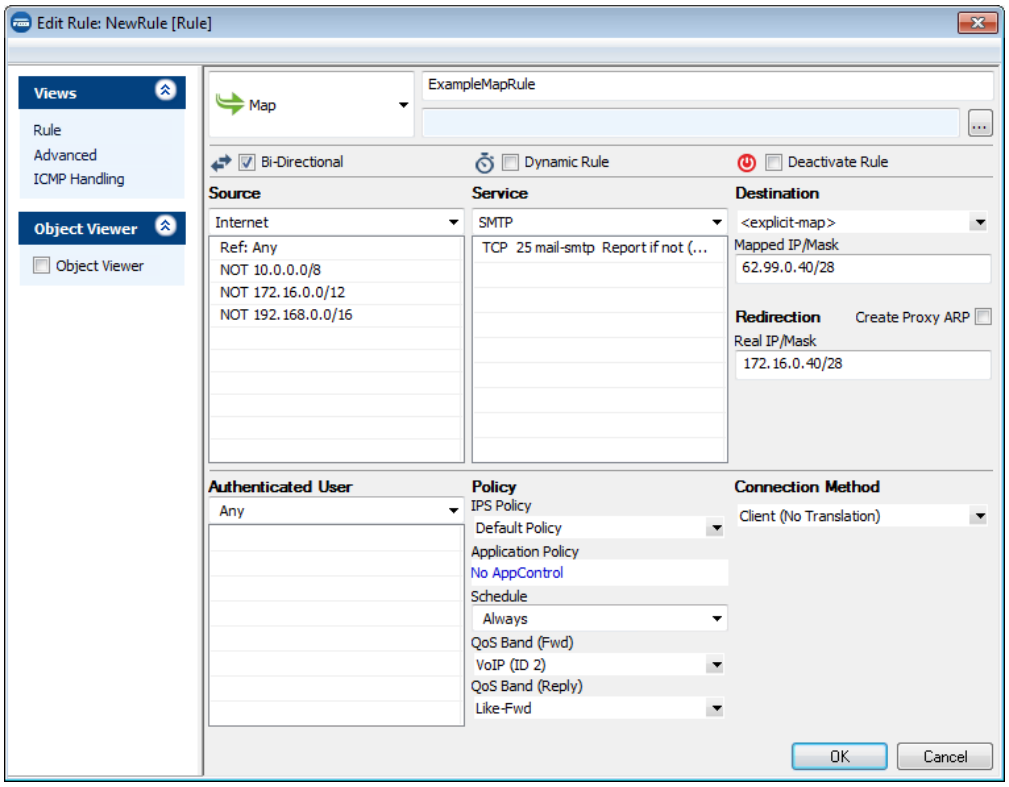
How to Create a Map Access Rule

A **Map** access rule rewrites incoming network ranges or IP address to destination networks or IP ranges, just like a Dst NAT rule does for a single IP address. You can use a NAT Table as an object for the **Destination** and/or **Connection** settings.

Ensure that the **Destination** network is the same size or smaller than the network used to redirect the request. Otherwise, the firewall wraps the larger source network into the smaller redirection network.



Create a Map 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 rule set, or right-click the rule set and select **New > Rule**.

4. Select **Map** as the action.
5. Enter a **Name** for the rule. For example, `ExampleMapRule`.
6. Select the the **Bi-Directional** check box.
7. Specify the following settings that must be matched by the traffic that to be handled by the access rule:
   - **Source** – The source addresses of the traffic. For example, select **Internet**.
   - **Destination** – Enter the destination network, or select a NAT table Connection object.
   - **Service** – Select a service object, or select **Any** for this rule to match for all services.
8. Enter the **Redirection** IP address or network. This is the network range that the connections will be rewritten to.
9. If the redirection IP network is not physically present on a network interface, select the **Create Proxy ARP** check box. For the example above, proxy ARP is not needed.

10. From the **Connection Method** list, select **Client (No Translation)**.
11. Click **OK**.
12. 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.
13. Click **Send Changes** and **Activate**.

Additional Matching Criteria

- **Authenticated User** – For more information, see User Objects.
- **Connection Method** – For more information, see Connection 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