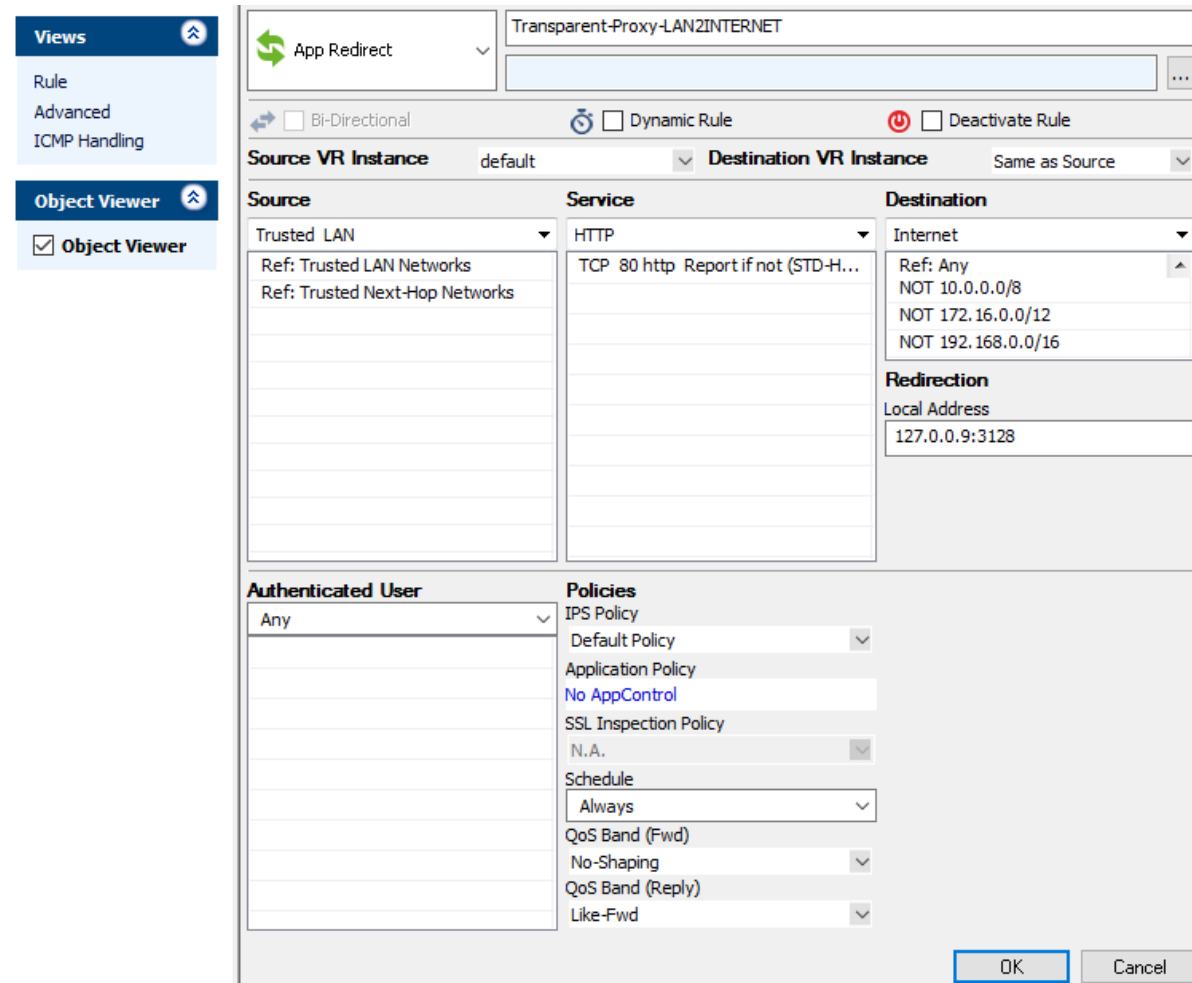


## How to Create an App Redirect Access Rule

<https://campus.barracuda.com/doc/79462925/>

The **App Redirect** access rule rewrites the destination IP address and forwards the traffic to service running on the CloudGen Firewall. For example, you can use an app redirect rule transparently redirect all web traffic over the HTTP proxy service.




The screenshot shows the configuration for an App Redirect rule named "Transparent-Proxy-LAN2INTERNET". The rule is configured with the following settings:

- Source VR Instance:** default
- Destination VR Instance:** Same as Source
- Source:** Trusted LAN (References: Trusted LAN Networks, Trusted Next-Hop Networks)
- Service:** HTTP (Protocol: TCP, Port: 80, Report if not (STD-H...))
- Destination:** Internet (References: Any, NOT 10.0.0.0/8, NOT 172.16.0.0/12, NOT 192.168.0.0/16)
- Redirection:** Local Address: 127.0.0.9:3128
- 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

Buttons for "OK" and "Cancel" are visible at the bottom right of the configuration window.

### Create an App Redirect 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 **App Redirect** as the action.
5. Enter a **Name** for the rule. For example, Transparent -Proxy -LAN2INTERNET.
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.
7. Enter the **Redirection** IP address and optional port as the **Local Address**. For example, 127.0.0.9:3128 for the HTTP proxy service.
  8. Click **OK**.
  9. 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.
  10. 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, 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\_AppRedirect.png
2. FW\_Rule\_Add01.png

© Barracuda Networks Inc., 2019 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.