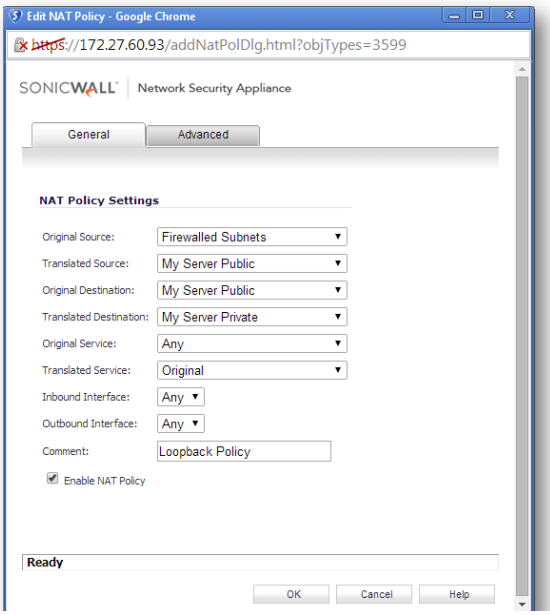
How to Create a Loop-back in SonicWall Router/Firewall Appliance

This instructional is for adding a loop-back (also known as NAT Reflection, NAT Loop-back, Hair-pinning, etc.) used to provide access to NMPSFA public websites from behind the firewall, specifically, the .12.0 network (public Wi-Fi). It may be used in lieu of split-brain DNS on the .11.0 network, or any network behind the firewall. Login to the SonicWall Appliance as Administrator, and then complete the steps below.

Create a NAT Policy

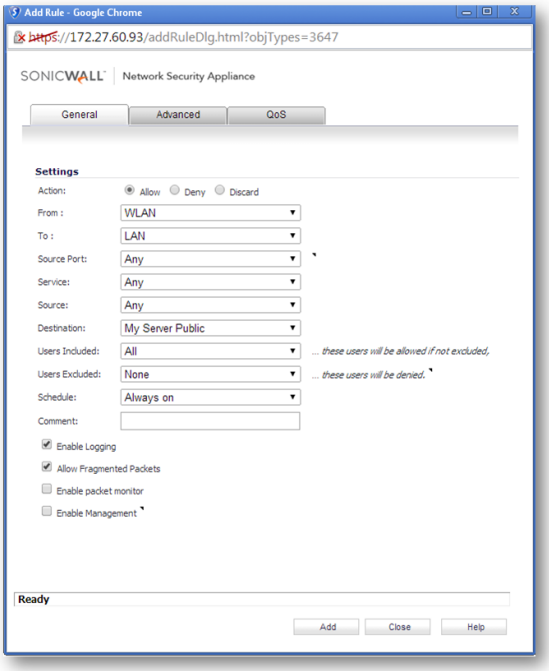
1. Go to **NETWORK > NAT POLICIES**
2. Click **ADD** and choose the following settings:



- **Name:** [Policy Name]
- **Original Source**: Firewalled Subnets
- **Translated Source**: [Server] Public
- **Original Destination**: [Server] Public
- **Translated Destination**: [Server] Public
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface:** Any
- **Outbound Interface**: Any
- **Comment**: [Optional]
- **IP Version**: IPv4 Only
- **Enable NAT Policy**: Checked

Create Firewall Access Rule

1. Go to **FIREWALL > ACCESS RULES**
2. Click on **ADD** and choose the following settings:



- **Policy Name:** [Policy Name]
- **Action:** Allow
- **From Zone:** X2:V300
- **To Zone:** LAN
- **Source port:** Any
- **Service:** Any
- **Source:** Any
- **Destination:** [Server] Public
- **Users Allowed:** All
- **Users Excluded:** None
- **Schedule:** Always on
- **Priority:** Retain original priority
- **Comment**: [Optional]
- **Enable Logging:** Checked
- **Allow Fragmented Packets:** Checked

Conventions

1. [Server] = Name of the Server Address Object, like PSCOC Public, e.g.)
2. [Policy Name] = A name to describe the policy
3. [Optional} = not required

Written by: K. Gray 09SEP19 (Rev. 1)
Source: https://www.sonicwall.com/support/knowledge-base/configuring-access-to-server-behind-a-sonicwall-from-wlan-zone-to-lan-using-public-ip-address/170505446809573/