Knowledge Base

Configuring Multiple WAN Subnets Using Static ARP with SonicOS Enhanced

Last Updated: 12/6/2018 ***13568*** *Views* ***97*** *Users found this article helpful*

Description

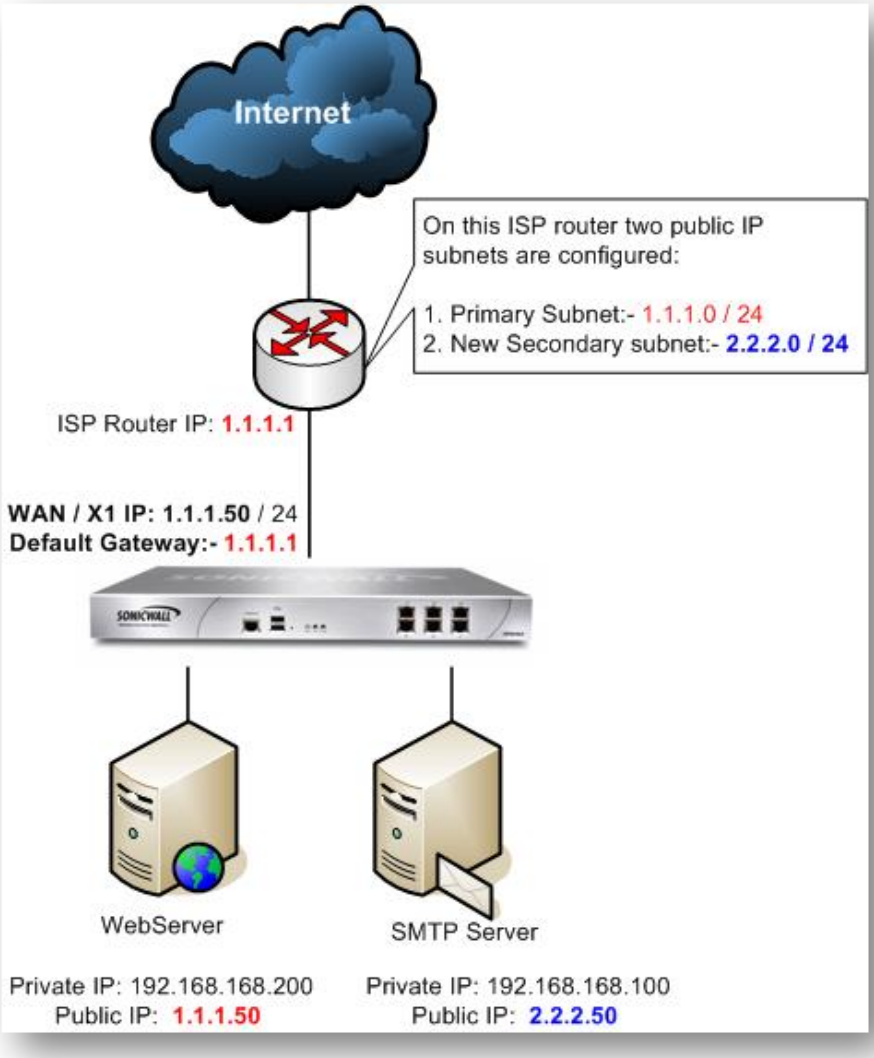
It is not currently possible to directly assign more than a single IP address to a primary or secondary WAN interface, but the SonicWall appliance is capable of answering on behalf of a 1-2-1 NAT policy set up for a network resource. This would be useful in environments where an ISP has assigned a customer multiple dissimilar public IP subnet blocks, and the customer wishes to use IP addresses from these blocks to provide access to internal network resources. One solution is to have the ISP configure upstream routing to point these subnets to the fixed IP address of the primary or secondary WAN interfaces of the SonicWall. An alternative is to configure static ARP and routing on the SonicWall to respond to a second IP subnet. You would do this by configuring a Static ARP entry for the secondary WAN subnet and adding a route for that subnet to the routing table.

Resolution

ISP provided primary subnet configured on the X1 (WAN) interface: **1.1.1.0/24.**

Additional block of IP addresses provided by the ISP: **2.2.2.0/24.**

SMTP Server in the LAN to be accessed from outside using **2.2.2.50**



Procedure:

Step 1: Create a Static ARP entry for the new network **2.2.2.0 / 24**.

Step 2: Create a Static Route

Step 3: Configuring a smtp server behind sonicWALL with the new WAN subnet.

Step 1 : Creating a Static ARP entry

1. Login to the SonicWall Management Interface.

2. Navigate to the **Network | ARP** page and click on the **ADD** button.

- **IP Address: 2.2.2.1** (specify an IP address from the additional subnet)

- **Interface:** WAN / X1 (because the additional subnet resides on the WAN interface)

- **Publish Entry -** Enabling this option causes the SonicWall to respond to ARP queries for the specified IP address with the SonicWall's MAC address. This box must be checked when creating additional subnets.

3. Click **OK.**

Step 2: Creating a Static Route

4. Navigate to the **Network | Routing** page.

5. Click on the **Add** button. Create the following new route policy

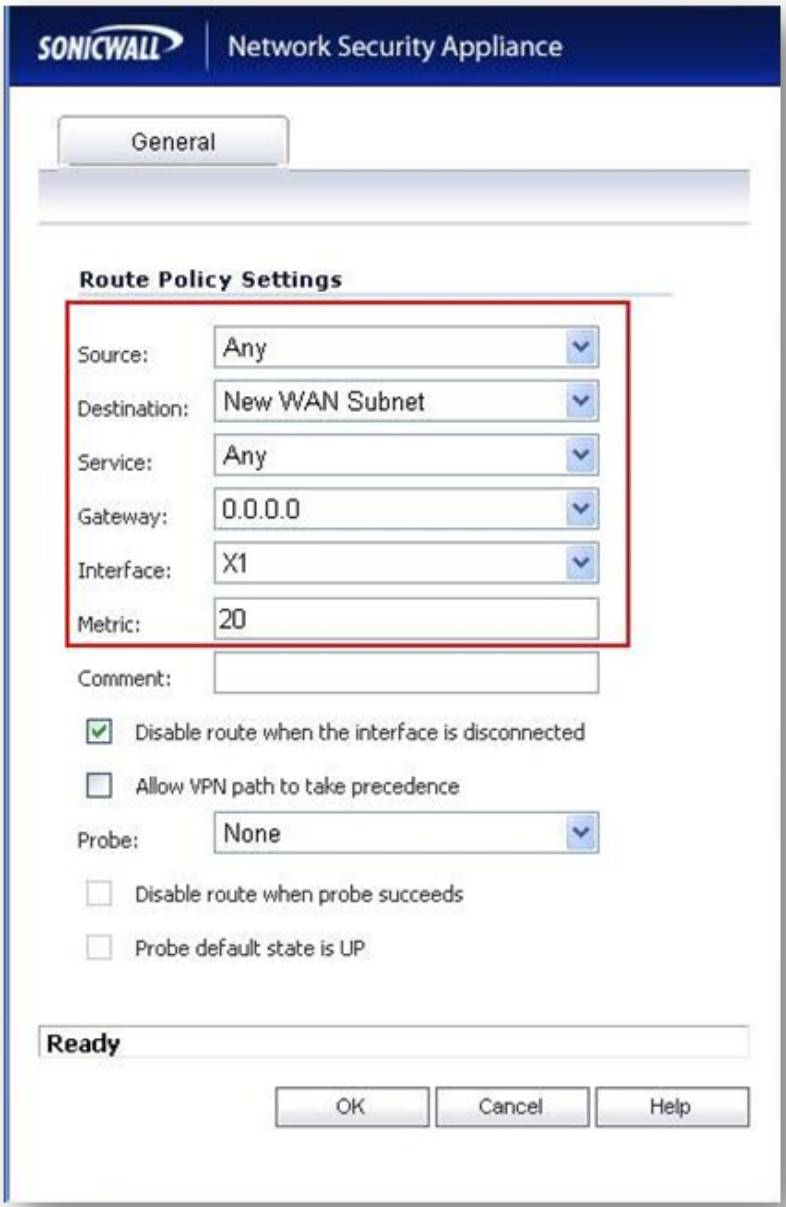
Creating a new **Address Object**

Name: the Address Object for your secondary subnet

Zone: WAN

Type: Network

Network: Enter the Network ID of the Secondary subnet



The final static route policy setting

Source: Any

Destination : New WAN Subnet

Service : Any

Gateway: 0.0.0.0

Interface: X1

Metric: 20

Secondary subnets can be utilized in both NAT and Transparent Modes (https://support.sonicwall.com/kb/SW5979).

NOTE: The SonicWall will not respond to HTTP/HTTPS management traffic on a published Static ARP IP address.

Step 3: Configuring a smtp server behind sonicWALL with the new WAN subnet

The SMTP server at 192.168.168.100 will be NATed to 2.2.2.50 ip address when going out to the internet. Likewise, the SMTP server can be access from the outside using IP Address 2.2.2.50.

1. Create a **public** and a **private** address object for the **SMTP** server

2. Configure an **Inbound NAT Policy** under **Network | NAT** Policies.

Adding appropriate NAT Policies

Original Source: **Any**

Translated Source: **Original**

Original Destination: **SMTP Server_Public**

Translated Destination: **SMTP Server_Private**

Original Service: **SMTP**

Translated Service: **Original**

Inbound Interface: **Any**

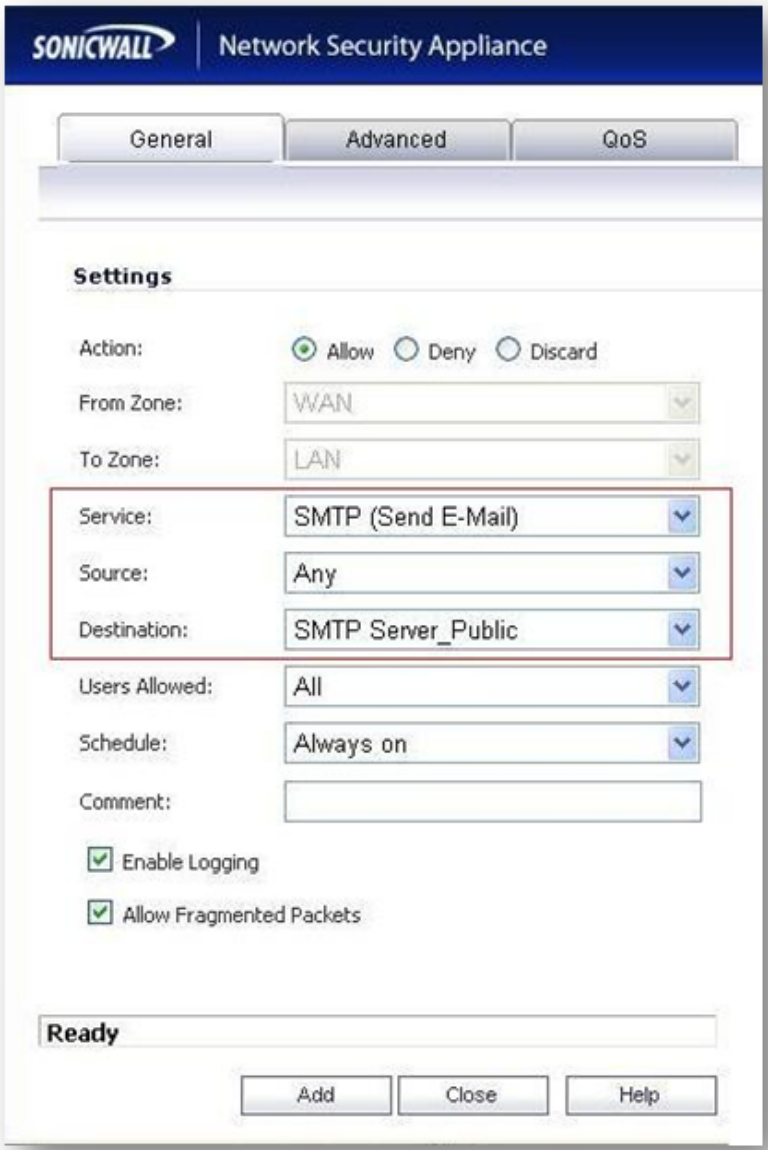
Outbound Interface: **Any**

Comment: Webserver behind SonicWall.

Enable NAT Policy: **Checked**

Create a reflexive policy: **Checked**

3. Create an **Access Rule** allowing inbound **SMTP** access



Action:**Allow**

From Zone:**WAN**

To Zone:**LAN**

Service: **SMTP**

Source: **Any**

Destination: **SMTP Server_Public**

Users Allowed: **All**

Schedule: **Always on**

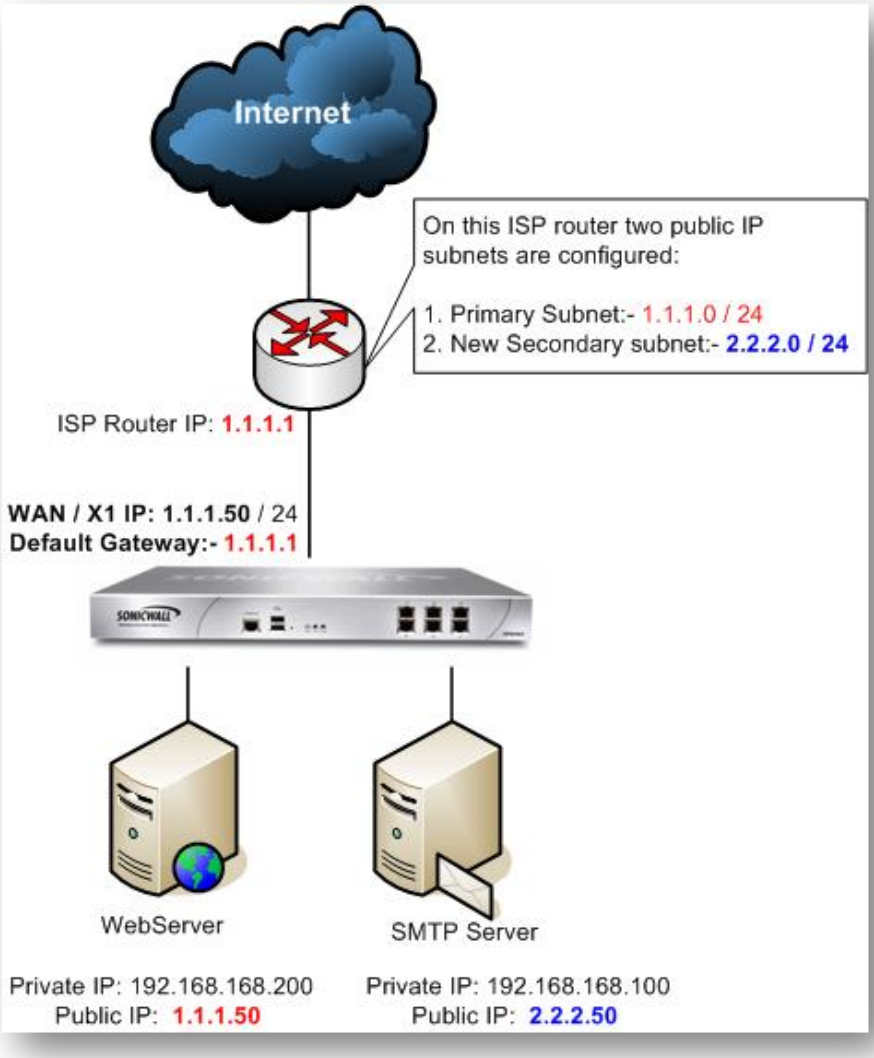
Enable Logging: **checked**

Allow Fragmented Packets: **checked**

Resolution for SonicOS 6.5 and Later

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

ISP provided primary subnet configured on the X1 (WAN) interface: **1.1.1.0/24**.
Additional block of IP addresses provided by the ISP: **2.2.2.0/24.**
SMTP Server in the LAN to be accessed from outside using **2.2.2.50**

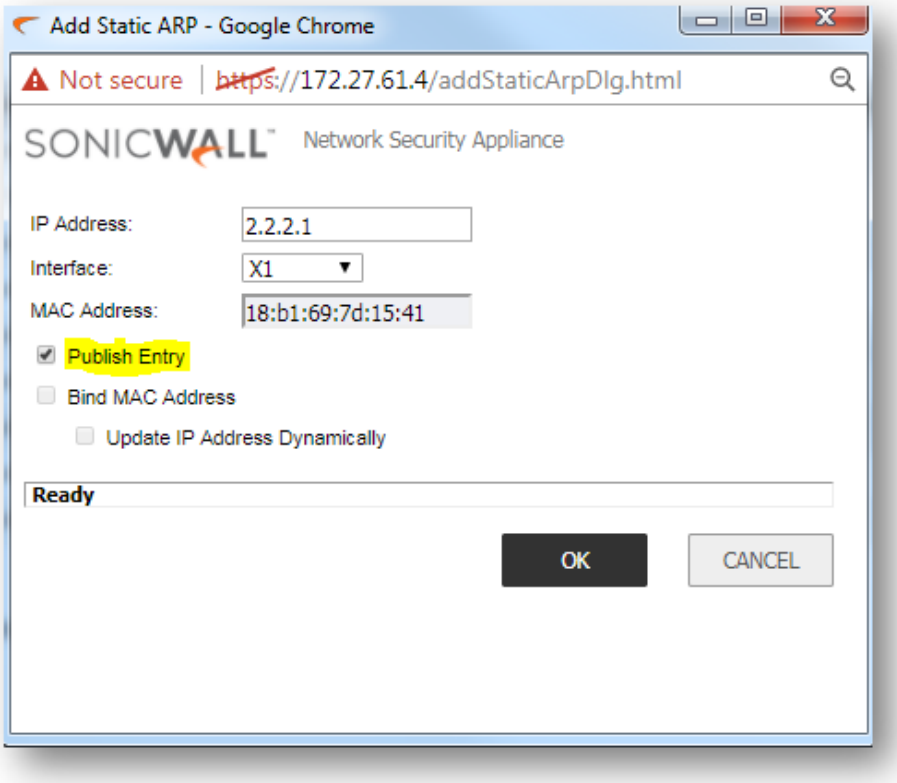


Procedure:

Step 1: Create a Static ARP entry for the new network **2.2.2.0 / 24**.
Step 2: Create a Static Route
Step 3: Configuring a smtp server behind sonicWALL with the new WAN subnet.

Step 1 : Creating a Static ARP entry

1. Login to the SonicWall Management interface.
2. Click on **MANAGE** on the top bar and navigate to the **Network | ARP** page and click on the **OK** buttonand then hit **ACCEPT** button at the bottom.



- **IP Address: 2.2.2.1** (specify an IP address from the additional subnet)

- **Interface:** WAN / X1 (because the additional subnet resides on the WAN interface)

- **Publish Entry -** Enabling this option causes the SonicWall to respond to ARP queries for the specified IP address with the SonicWall's MAC address. This box must be checked when creating additional subnets.

3. Click **OK.**

Step 2: Creating a Static Route

4. Navigate to the **Network | Routing** page.
5. Click on the **Add** button**.** Create the following new route policy

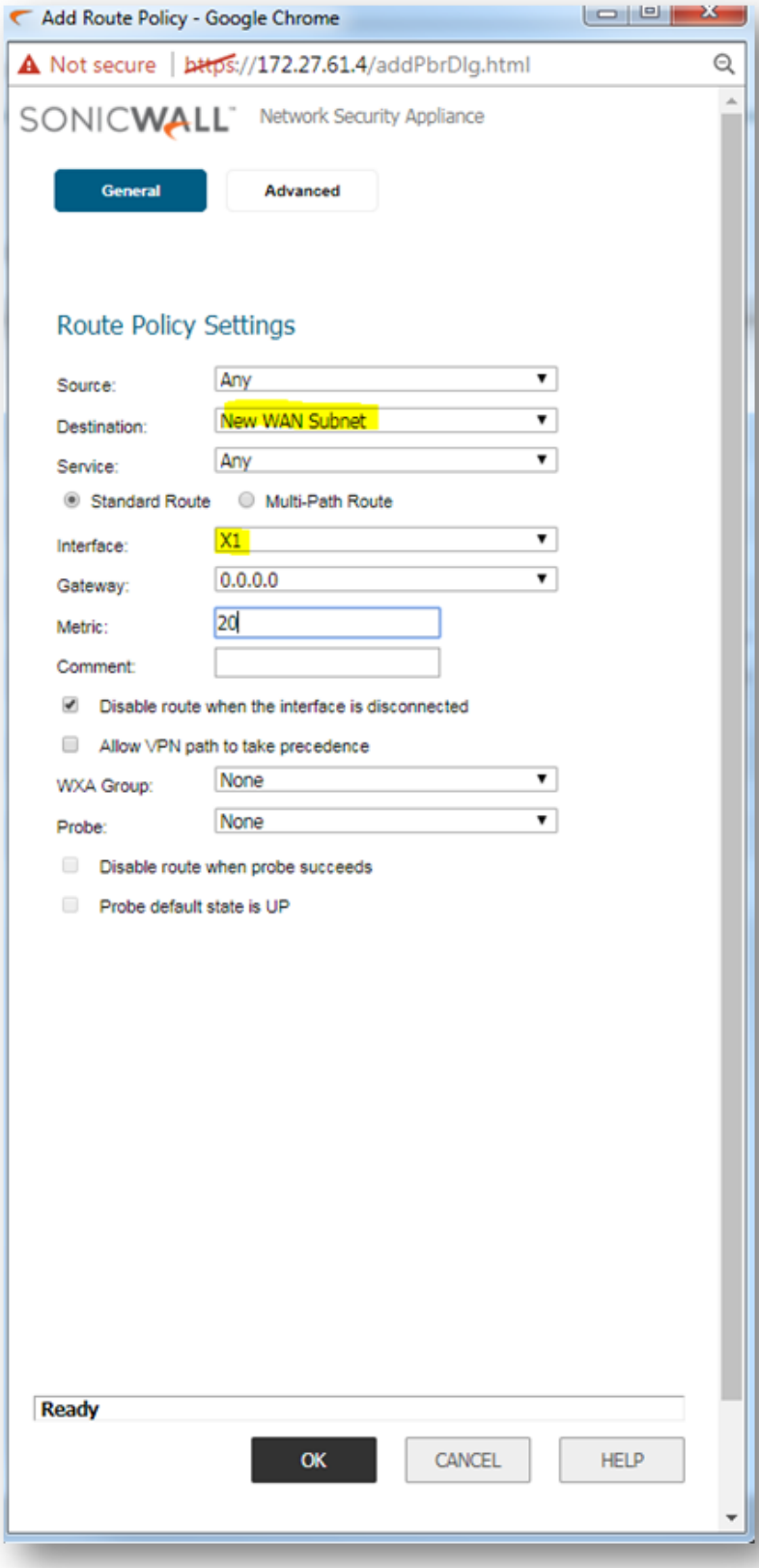
Creating a new **Address Object**

Name: the Address Object for your secondary subnet

Zone: WAN

Type: Network

Network: Enter the Network ID of the Secondary subnet



The final static route policy setting

Source: Any
Destination : New WAN Subnet
Service : Any
Gateway: 0.0.0.0
Interface: X1
Metric: 20

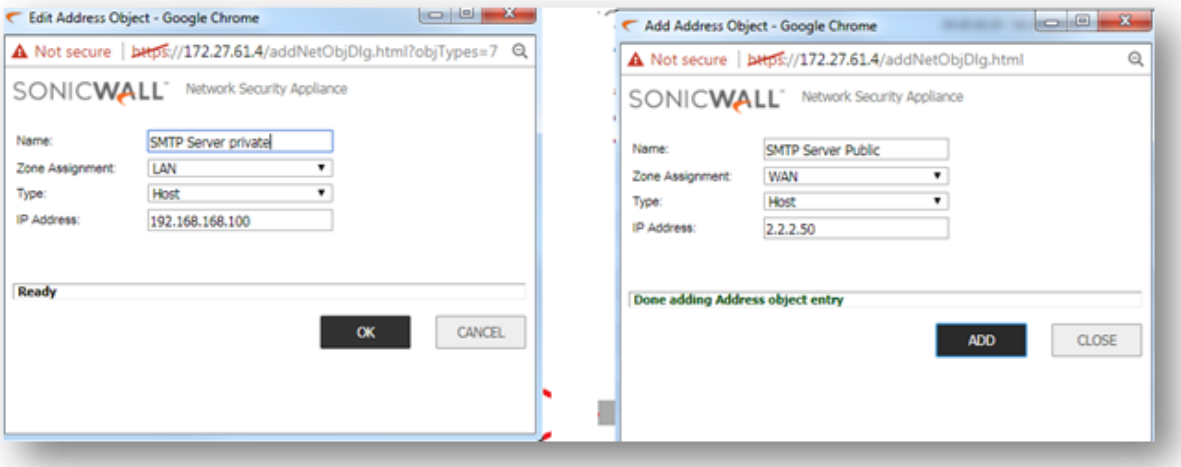
Secondary subnets can be utilized in both NAT and Transparent Modes (https://support.sonicwall.com/kb/SW5979).

NOTE: The SonicWall will not respond to HTTP/HTTPS management traffic on a published Static ARP IP address.

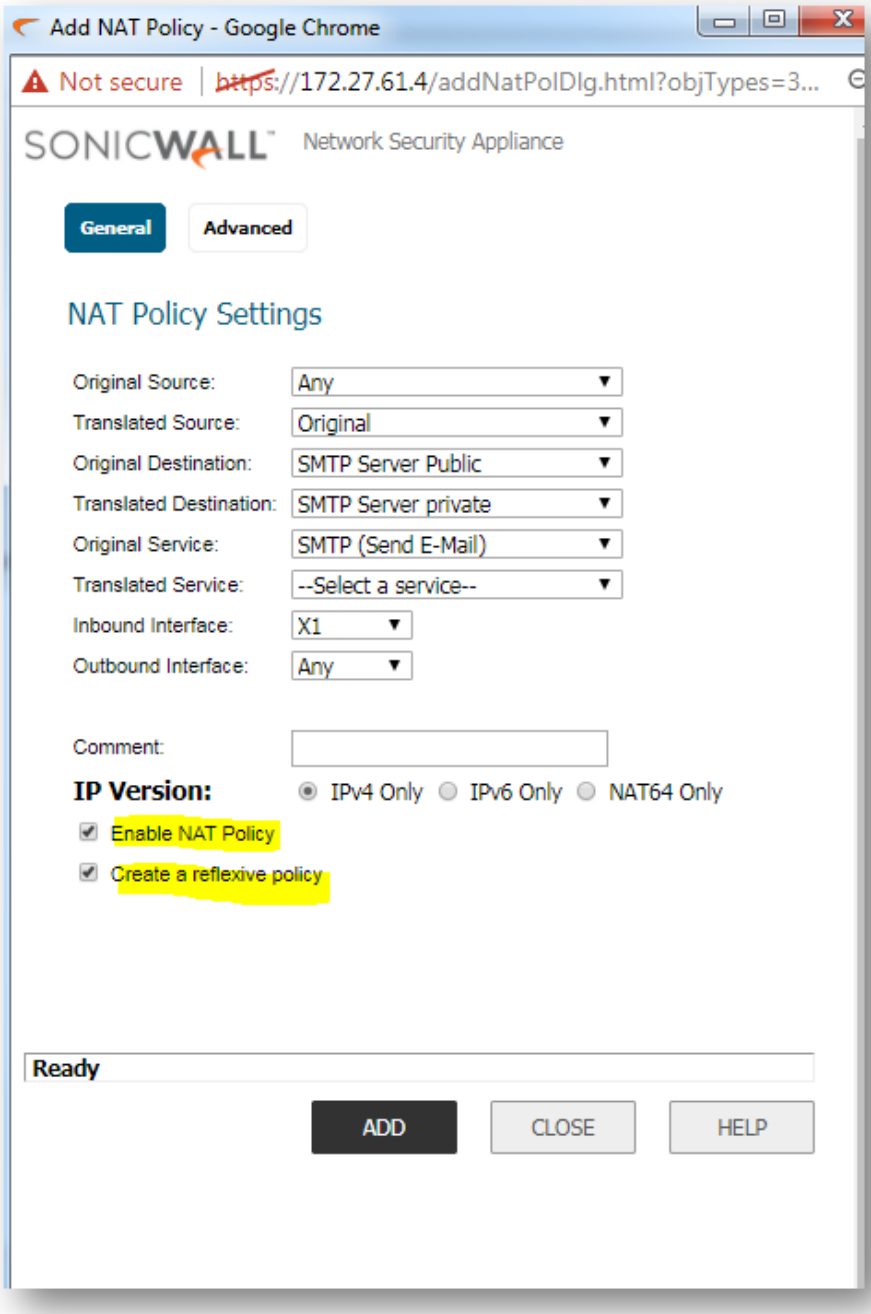
Step 3: Configuring a smtp server behind sonicWALL with the new WAN subnet

The SMTP server at 192.168.168.100 will be NATed to 2.2.2.50 ip address when going out to the internet. Likewise, the SMTP server can be access from the outside using IP Address 2.2.2.50.

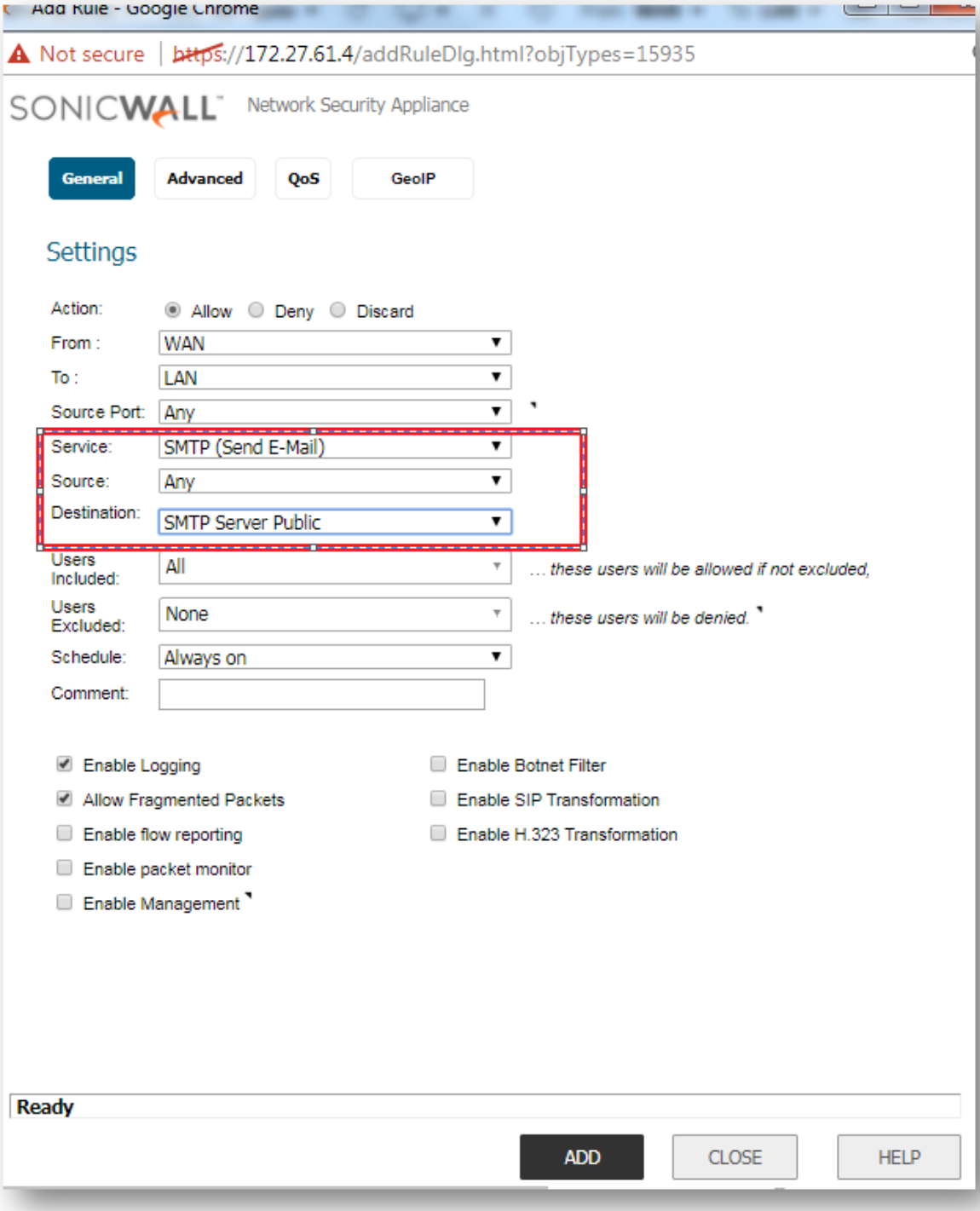
1. Create a **public** and a **private** address object for the **SMTP** server (For the same, please navigat to **Objects | Address Objects**)



2. Configure an **Inbound NAT Policy** under **Rules | NAT** Policies.



3. Create an **Access Rule** allowing inbound **SMTP** access



Action:**Allow**

From Zone:**WAN**
To Zone:**LAN**
Service: **SMTP**
Source: **Any**
Destination: **SMTP Server_Public**

Users Allowed: **All**
Schedule: **Always on**
Enable Logging: **checked**
Allow Fragmented Packets: **checked**

Categories

Firewalls>SonicWall TZ Series , Firewalls>SonicWall NSA Series , Firewalls>SonicWall SuperMassive 9000 Series , Firewalls>SonicWall SuperMassive E10000 Series

Not Finding Your Answer?

REQUEST NEW KNOWLEDGE BASE ARTICLE

Was This Article Helpful?

Yes No

Customers (/en-us/footer-menu/customers)

How To Buy (/en-us/footer-menu/customers/how-to-buy)

Free Trials (/en-us/footer-menu/customers/free-trials)

Loyalty & Trade-In Programs (/en-us/footer-menu/customers/loyalty-trade-in-program)

MySonicWall.com (/en-us/footer-menu/customers/mysonicwall-com)

SonicWall and GDPR (/en-us/footer-menu/customers/gpdr)

Support (/en-us/footer-menu/support)

Knowledge Base (/en-us/footer-menu/support/knowledge-base)

Video Tutorials (/en-us/footer-menu/support/video-tutorials)

Technical Documentation (/en-us/footer-menu/support/technical-documentation)

SonicWall Services (/en-us/footer-menu/support/professional-services)

Support Services (/en-us/footer-menu/support/support-services)

Training and Certification (/en-us/footer-menu/support/sonicwall-training-certification)

Contact Support (/en-us/footer-menu/support/contact-support)

Stay Connected (/en-us/footer-menu/stay-connected)

(https://www.facebook.com/SonicWall/)

(https://twitter.com/SonicWALL)

(https://www.linkedin.com/company-beta/4926/)

(https://www.youtube.com/user/SonicWALL

(https://www.instagram.com/sonicwall_inc/

Blog (/en-us/footer-menu/stay-connected/blog)

Privacy (/privacy) Legal (/legal)