

Knowledge Base

[ALL SUPPORT](#)

Ask a question or enter a search term

SEARCH

Configuring Multiple WAN Subnets Using Static ARP with SonicOS Enhanced

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

Description

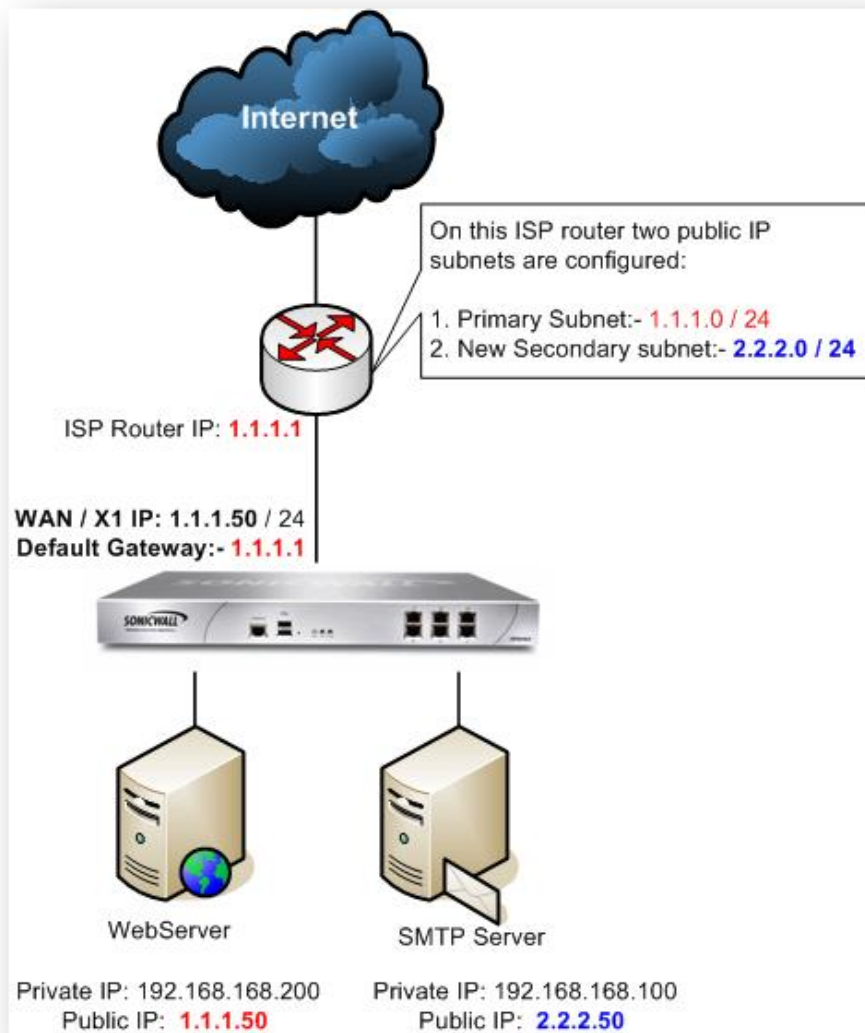
It is not currently possible to directly assign more than a single IP address to a primary or secondary WAN interface, but the SonicWall appliance is capable of answering on behalf of a 1-2-1 NAT policy set up for a network resource. This would be useful in environments where an ISP has assigned a customer 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.



The screenshot shows the 'Network Security Appliance' window with the 'ARP' configuration page. A red rectangle highlights the 'IP Address' field (2.2.2.1), the 'Interface' dropdown (X1), and the 'MAC Address' field (00:17:c5:28:92:e1). Below these fields are three checkboxes: 'Publish Entry' (checked), 'Bind MAC Address' (unchecked), and 'Update IP Address Dynamically' (unchecked). At the bottom, there is a 'Ready' status bar and 'OK' and 'Cancel' buttons.

- **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

 Network Security Appliance

General

Route Policy Settings

Source: Any

Destination: New WAN Subnet

Service: Any

Gateway: 0.0.0.0

Interface: X1

Metric: 20

Comment:

☒ Disable route when the interface is disconnected

☐ Allow VPN path to take precedence

Probe: None

☐ Disable route when probe succeeds

☐ Probe default state is UP

Ready

OK

Cancel

Help

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



The screenshot shows the 'Add' dialog for a new address object in the SonicWall Network Security Appliance. The 'Name' field is 'SMTP Server_Private', 'Zone Assignment' is 'LAN', 'Type' is 'Host', and 'IP Address' is '192.168.168.100'. The 'Ready' status bar is at the bottom, and 'OK' and 'Cancel' buttons are at the bottom right.



The screenshot shows the 'Add' dialog for a new address object in the SonicWall Network Security Appliance. The 'Name' field is 'SMTP Server_Public', 'Zone Assignment' is 'WAN', 'Type' is 'Host', and 'IP Address' is '2.2.2.50'. The 'Ready' status bar is at the bottom, and 'Add' and 'Close' buttons are at the bottom right.

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

Adding appropriate NAT Policies

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

The screenshot shows the SonicWall Network Security Appliance configuration interface. At the top, there are three tabs: "General", "Advanced", and "QoS". The "General" tab is selected. Below the tabs, there is a "Settings" section. The "Action" is set to "Allow" (selected with a radio button). The "From Zone" is set to "WAN" and the "To Zone" is set to "LAN". The "Service" is set to "SMTP (Send E-Mail)", the "Source" is set to "Any", and the "Destination" is set to "SMTP Server_Public". These three settings are highlighted with a red box. The "Users Allowed" is set to "All" and the "Schedule" is set to "Always on". There is a "Comment" field. Below the "Settings" section, there are two checkboxes: "Enable Logging" and "Allow Fragmented Packets", both of which are checked. At the bottom, there is a "Ready" status bar and three buttons: "Add", "Close", and "Help".

SonicWall | Network Security Appliance

General Advanced QoS

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From Zone: WAN

To Zone: LAN

Service: SMTP (Send E-Mail)

Source: Any

Destination: SMTP Server_Public

Users Allowed: All

Schedule: Always on

Comment:

☒ Enable Logging

☒ Allow Fragmented Packets

Ready

Add Close Help

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**

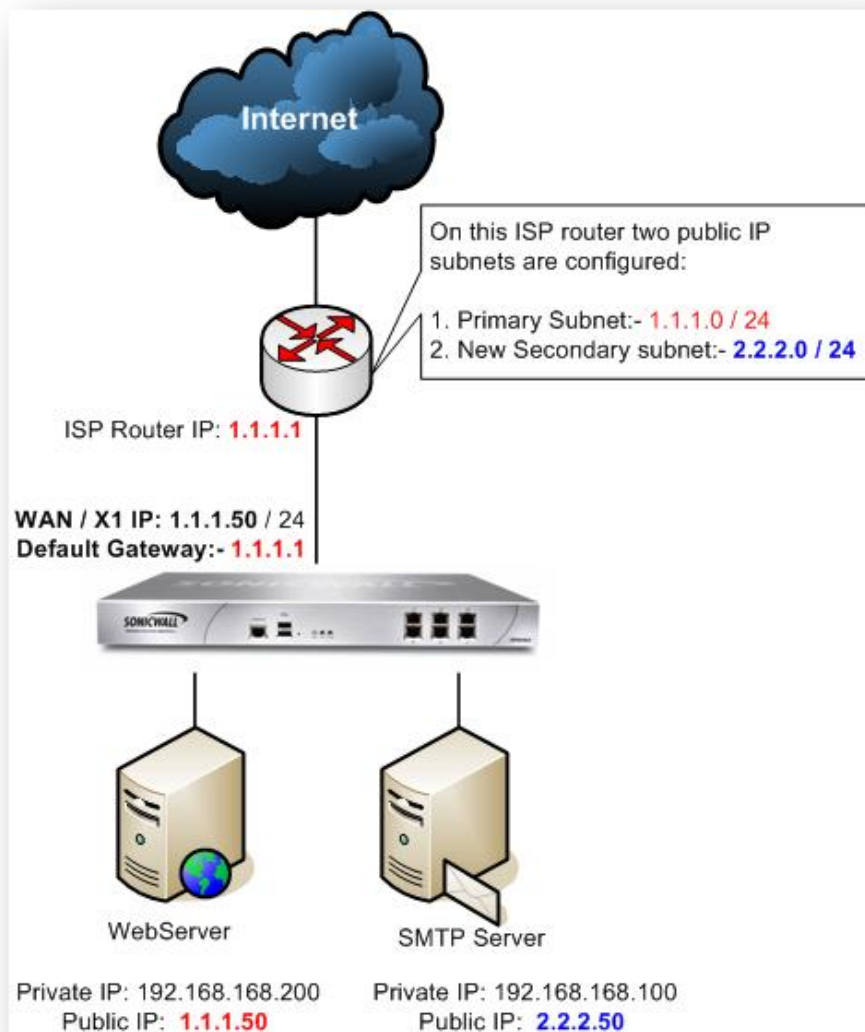
Resolution for SonicOS 6.5 and Later

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** button and then hit **ACCEPT** button at the bottom.

Add Static ARP - Google Chrome

Not secure | <https://172.27.61.4/addStaticArpDlg.html>

SONICWALL™ Network Security Appliance

IP Address: 2.2.2.1

Interface: X1

MAC Address: 18:b1:69:7d:15:41

☒ Publish Entry

☐ Bind MAC Address

☐ Update IP Address Dynamically

Ready

OK CANCEL

- **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

Add Route Policy - Google Chrome

Not secure | <https://172.27.61.4/addPbrDlg.html>

SONICWALL™ Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: New WAN Subnet

Service: Any

☒ Standard Route ☐ Multi-Path Route

Interface: X1

Gateway: 0.0.0.0

Metric: 20

Comment:

☒ Disable route when the interface is disconnected

☐ Allow VPN path to take precedence

WXA Group: None

Probe: None

☐ Disable route when probe succeeds

☐ Probe default state is UP

Ready

OK CANCEL HELP

The final static route policy setting

Source: Any

Destination: New WAN Subnet

Service : Any

Gateway: 0.0.0.0

Interface: X1

Metric: 20

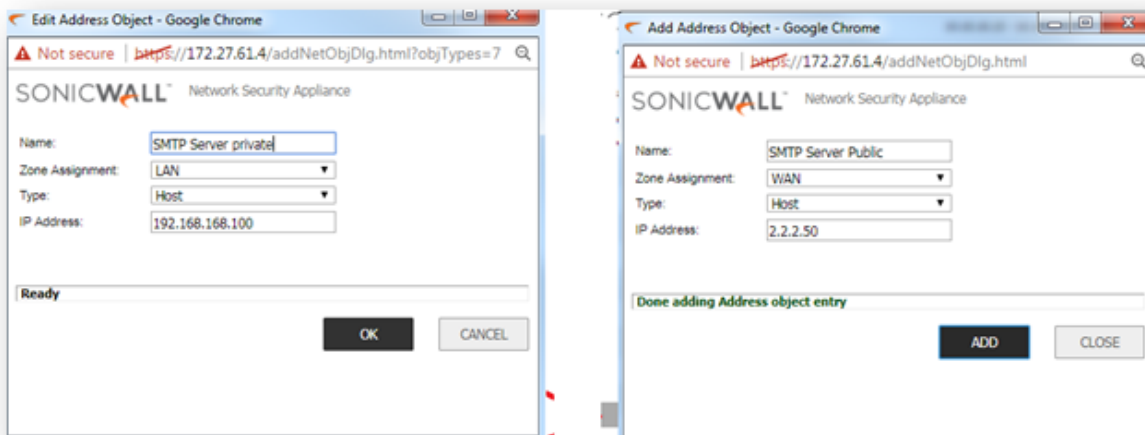
Secondary subnets can be utilized in both NAT and Transparent Modes (<https://support.sonicwall.com/kb/SW5979>).

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**.

Add NAT Policy - Google Chrome

Not secure | <https://172.27.61.4/addNatPolDlg.html?objTypes=3...>

SONICWALL™ Network Security Appliance

General Advanced

NAT Policy Settings

Original Source: Any ▼

Translated Source: Original ▼

Original Destination: SMTP Server Public ▼

Translated Destination: SMTP Server private ▼

Original Service: SMTP (Send E-Mail) ▼

Translated Service: --Select a service-- ▼

Inbound Interface: X1 ▼

Outbound Interface: Any ▼

Comment:

IP Version: ☒ IPv4 Only ☐ IPv6 Only ☐ NAT64 Only

☒ Enable NAT Policy

☒ Create a reflexive policy

Ready

ADD CLOSE HELP

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

Add Rule - Google Chrome

Not secure | <https://172.27.61.4/addRuleDlg.html?objTypes=15935>

SONICWALL™ Network Security Appliance

General Advanced QoS GeolP

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From : WAN

To : LAN

Source Port: Any

Service: SMTP (Send E-Mail)

Source: Any

Destination: SMTP Server Public

Users Included: All ... these users will be allowed if not excluded,

Users Excluded: None ... these users will be denied.

Schedule: Always on

Comment:

☒ Enable Logging ☐ Enable Botnet Filter

☒ Allow Fragmented Packets ☐ Enable SIP Transformation

☐ Enable flow reporting ☐ Enable H.323 Transformation

☐ Enable packet monitor

☐ Enable Management

Ready

ADD CLOSE HELP

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

[About SonicWall \(/en-us/footer-menu/about-sonicwall\)](#)

[Contact \(/en-us/footer-menu/about-sonicwall/contact\)](#)

[Careers \(/en-us/footer-menu/about-sonicwall/careers\)](#)

[Leadership \(/en-us/footer-menu/about-sonicwall/leadership\)](#)

[News \(/en-us/footer-menu/about-sonicwall/news\)](#)

[Press Kit \(/en-us/footer-menu/about-sonicwall/press-kit-media-tools\)](#)

[Awards \(/en-us/footer-menu/about-sonicwall/awards\)](#)

[Products \(/en-us/footer-menu/products\)](#)

[Firewalls \(/en-us/footer-menu/products/firewalls\)](#)

[Advanced Threat Protection \(/en-us/footer-menu/products/advanced-threat-protection\)](#)

[Remote Access \(/en-us/footer-menu/products/remote-access\)](#)

[Email Security \(/en-us/footer-menu/products/email-security\)](#)

[Solutions \(/en-us/footer-menu/solutions\)](#)

[Advanced Threats \(/en-us/footer-menu/solutions/advanced-threats\)](#)

[Industries \(/en-us/footer-menu/solutions/industries\)](#)

[Service Providers \(/en-us/footer-menu/solutions/service-providers\)](#)

[Customers \(/en-us/footer-menu/customers\)](/en-us/footer-menu/customers)

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

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

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

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

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

[Support \(/en-us/footer-menu/support\)](/en-us/footer-menu/support)

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

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

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

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

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

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

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

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



[\(https://www.facebook.com/SonicWall/\)](https://www.facebook.com/SonicWall/)



[\(https://twitter.com/SonicWALL\)](https://twitter.com/SonicWALL)



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



[\(https://www.youtube.com/user/SonicWALL\)](https://www.youtube.com/user/SonicWALL)



[\(https://www.instagram.com/sonicwall_inc/\)](https://www.instagram.com/sonicwall_inc/)

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