

Tech Note

Introduction

This tech note describes how to configure secondary subnets with static ARP which allows multiple subnets to be connected to a single physical interface. Secondary subnets can be utilized in both NAT and transparent modes.

Recommended Versions

- SonicOS Enhanced 3.0.0.5 or newer

Customers with current service/software support contracts can obtain updated versions of SonicWALL firmware from the MySonicWALL customer portal at <https://www.mysonicwall.com>. Updated firmware is also freely available to customers who have registered the SonicWALL device on MySonicWALL for the first 90 days.

Caveats

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

Task List

Example #1 Default NAT Mode with secondary subnet

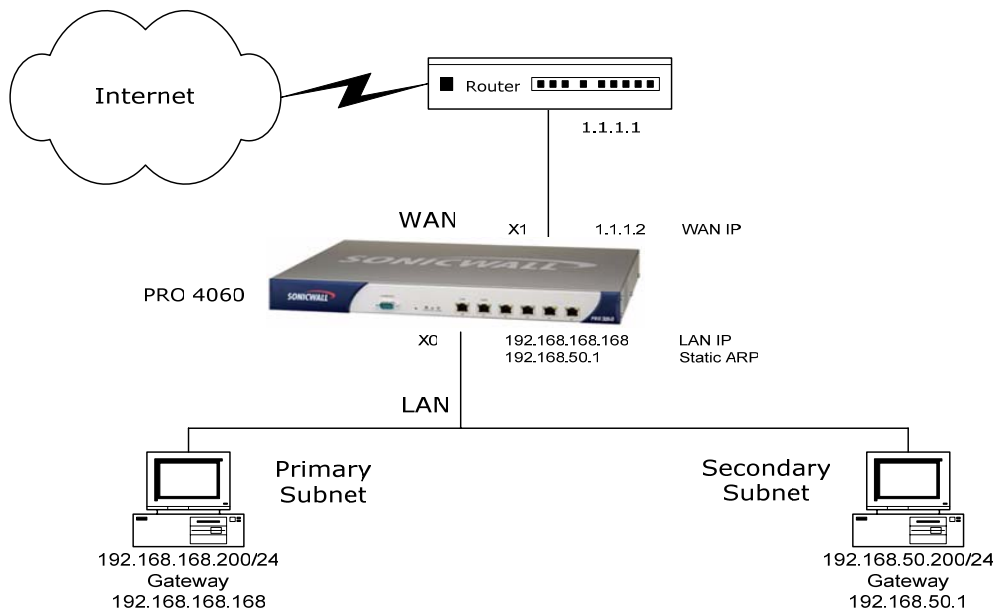
1. Create Static ARP entry for the gateway address of secondary subnet on the LAN interface
2. Create address object for secondary subnet
3. Add static route for the secondary subnet

Example #2 Transparent Mode with secondary subnet

1. Setup transparent mode on LAN interface
2. Create static ARP entry for the gateway address of secondary subnet on the WAN interface
3. Create address object for the secondary subnet
4. Create route to WAN router
5. Add static route policy for the secondary subnet

Tech Note

Example #1 Default NAT Mode with secondary subnet



Go to the 'Network > ARP' page. In the 'Static ARP Entries' section, click on the 'Add...' button to enter the IP address of the gateway of the secondary subnet.

Network > ARP Flush ARP Cache... Apply Cancel ?

Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
No Entries						

Add... Delete Delete All...

ARP Settings

ARP Cache entry timeout (minutes):

ARP Cache Items 1 to 3 (of 3)

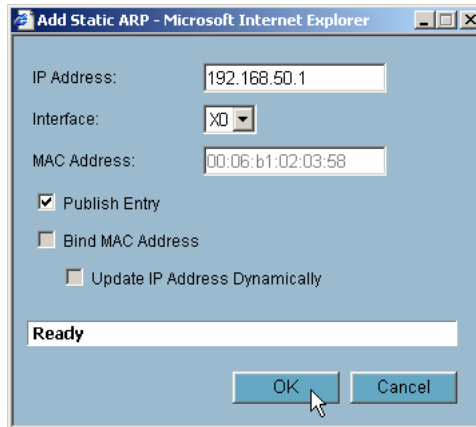
#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	1.1.1.2	Static	00:06:B1:02:03:59	X1	Permanent published	
2	192.168.168.168	Static	00:06:B1:02:03:58	X0	Permanent published	
3	192.168.168.200	Dynamic	00:C0:4F:18:2C:FA	X0	Expires in 10 minutes	

Flush Flush ARP Cache...

ARP Statistics: ARP Statistics: 3 entries, 1493 lookups, 118 failures, 1329 hits, 46 misses, 96% hit rate

Tech Note

On the 'Add Static ARP' popup page, enter the IP address that will be the gateway for the secondary subnet, in this example, enter "192.168.50.1". Then choose the interface for this secondary subnet, in this example the secondary subnet will be added to the LAN(X0) interface. Click on the radio button next to 'Publish Entry' and the MAC Address field will automatically be populated with the MAC address of the interface. Click 'OK' to continue.



The IP address will now appear in the 'Static ARP Entries' table and the 'ARP Cache' table.

The screenshot displays the ARP configuration interface with the following sections:

- Network > ARP**: Includes buttons for "Flush ARP Cache...", "Apply", "Cancel", and a help icon.
- Static ARP Entries**: A table with columns: #, IP Address, MAC Address, Interface, Published, Bind MAC, and Configure. It contains one entry for IP 192.168.50.1 on interface X0, which is published. Below the table are "Add...", "Delete", and "Delete All..." buttons.
- ARP Settings**: "ARP Cache entry timeout (minutes):" is set to 10.
- ARP Cache**: Shows "Items 1 to 4 (of 4)". The table has columns: #, IP Address, Type, MAC Address, Interface, Timeout, and Flush. It lists four entries:

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	1.1.1.2	Static	00:06:B1:02:03:59	X1	Permanent published	[Trash]
2	192.168.50.1	Static	00:06:B1:02:03:58	X0	Permanent published	[Trash]
3	192.168.168.168	Static	00:06:B1:02:03:58	X0	Permanent published	[Trash]
4	192.168.168.200	Dynamic	00:C0:4F:18:2C:FA	X0	Expires in 10 minutes	[Trash]

Below the table are "Flush" and "Flush ARP Cache..." buttons.
- ARP Statistics**: "ARP Statistics: 4 entries, 1518 lookups, 118 failures, 1353 hits, 47 misses, 96% hit rate"

Tech Note

Next, go to the 'Network > Routing' page. In the 'Route Policies' section, click on the 'Add...' button to add a new static route for the secondary subnet so that the SonicWALL will consider it valid traffic and route it properly to the correct interface. If the route is not added the SonicWALL will drop the traffic and log it as an attack.

Network > Routing ?

Route Advertisement

Routing Mode:

Interface (Zone)	Status	Configure
X0 (LAN)	Disabled	
X1 (WAN)	Disabled	
X2 (N/A)	Disabled	
X3 (N/A)	Disabled	
X4 (N/A)	Disabled	
X5 (N/A)	Disabled	

Route Policies Items to 7 (of 7)

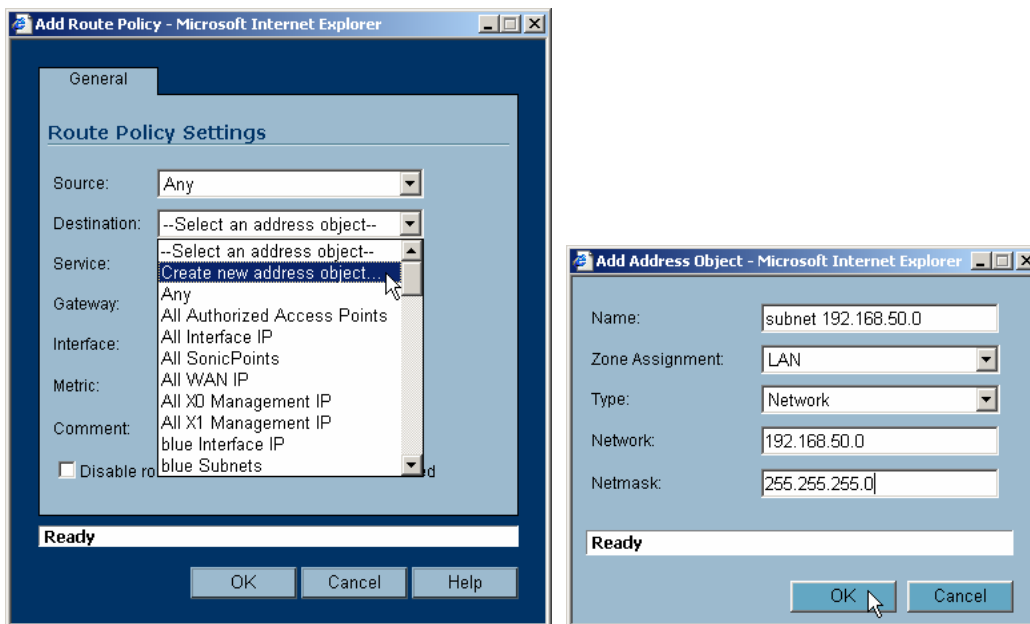
View Style: All Policies Custom Policies Default Policies

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
<input type="checkbox"/> 1	Any	WLAN Subnets	Any	0.0.0.0	X0	20	1		
<input type="checkbox"/> 2	Any	Default Gateway	Any	0.0.0.0	X1	20	2		
<input type="checkbox"/> 3	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	3		
<input type="checkbox"/> 4	Any	WAN Primary Subnet	Any	0.0.0.0	X1	20	4		
<input type="checkbox"/> 5	Any	LAN Primary Subnet	Any	0.0.0.0	X0	20	5		
<input type="checkbox"/> 6	WAN Primary Subnet	Any	Any	Default Gateway	X1	20	6		
<input type="checkbox"/> 7	Any	0.0.0.0/0	Any	192.168.168.168	X1	20	7		

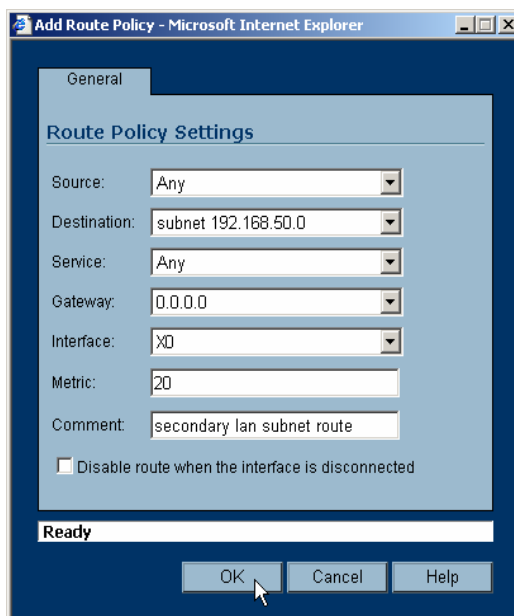
Add a new Route Policy

Tech Note

On the 'Add Route Policy' page, select "Any" as the 'Source'. In the 'Destination' field select "Create new address object" and the 'Add Address Object' page will popup. On the 'Add Address Object' page enter a name for the secondary subnet in the 'Name' field, for this example, "subnet 192.168.50.0". This secondary subnet is on the LAN(X0) interface so the 'Zone Assignment' would be "LAN". The 'Type' is "Network". The 'Network' is "192.168.50.0" with a 'Netmask' of "255.255.255.0". Click 'OK' to continue back on the 'Add Route Policy' page.



Continuing on the 'Add Route Policy' page, 'Service' is "Any", 'Gateway' is "0.0.0.0", 'Interface' is "X0" which is the LAN interface and the 'Metric' is "20" which is the default for a locally attached network. Optionally, add a 'Comment' to help identify this route policy -- in this example, "secondary LAN subnet route". Click 'OK' to finish adding the policy.



Tech Note

The new route policy now appears in the 'Route Policies' table at number 6 in this example.

The screenshot shows the SonicWall configuration interface for 'Network > Routing'. It is divided into two main sections: 'Route Advertisement' and 'Route Policies'.

Route Advertisement: Shows 'Routing Mode' set to 'Simple RIP Advertisement'. Below is a table of interfaces:

Interface (Zone)	Status	Configure
X0 (LAN)	Disabled	
X1 (WAN)	Disabled	
X2 (N/A)	Disabled	
X3 (N/A)	Disabled	
X4 (N/A)	Disabled	
X5 (N/A)	Disabled	

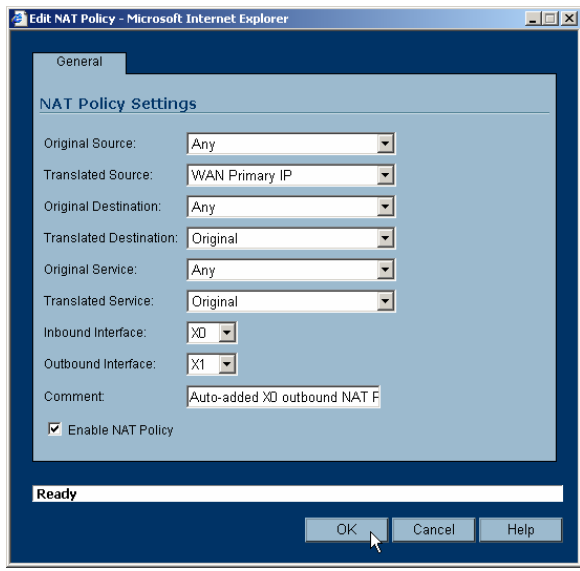
Route Policies: Shows a table of 8 policies. Policy #6 is highlighted in yellow, and its comment 'secondary lan subnet route' is visible in a tooltip. The table columns are: #, Source, Destination, Service, Gateway, Interface, Metric, Priority, Comment, and Configure.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	WLAN Subnets	Any	0.0.0.0	X0	20	1		
2	Any	Default Gateway	Any	0.0.0.0	X1	20	2		
3	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	3		
4	Any	WAN Primary Subnet	Any	0.0.0.0	X1	20	4		
5	Any	LAN Primary Subnet	Any	0.0.0.0	X0	20	5		
6	Any	subnet 192.168.50.0	Any	0.0.0.0	X0	20	6	secondary lan subnet route	
7	WAN Primary Subnet	Any	Any	Default Gateway	X1	20			
8	Any	0.0.0.0/0	Any	192.168.168.168	X1	20	8		

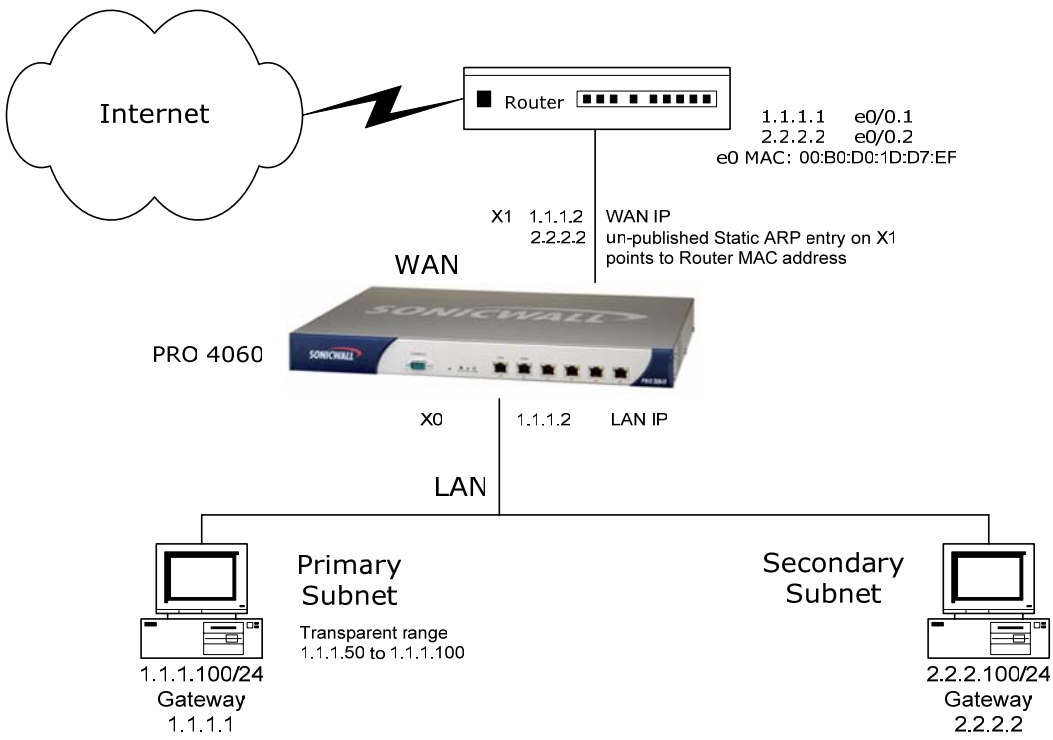
At the bottom of the 'Route Policies' section, there are buttons for 'Add...', 'Delete', and 'Delete All'.

Tech Note

The secondary subnet uses the general Access Rule and NAT Policy of the parent interface. In this example, the default general Access Rule and NAT policy of the X0(LAN) interface will allow traffic from the secondary subnet to the WAN zone. It is possible to create more specific Access Rules and NAT Policies for the secondary subnets if required. Shown below is the default NAT Policy for LAN to WAN traffic.



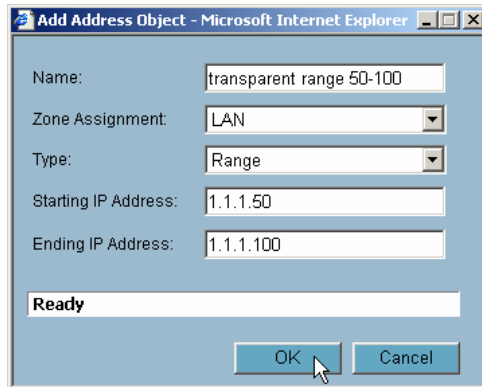
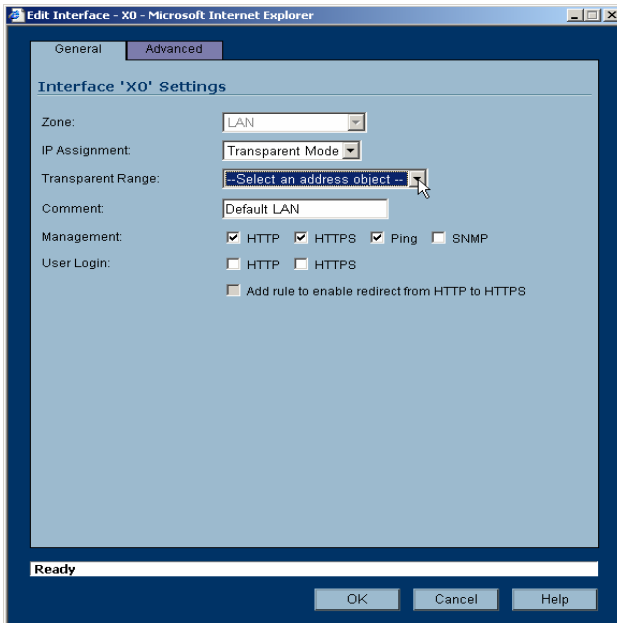
Example #2 Transparent Mode with secondary subnet



Tech Note

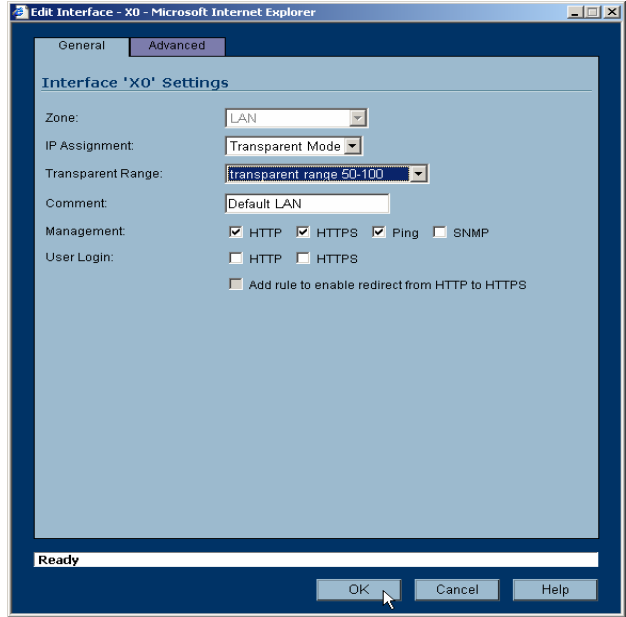
In transparent mode the WAN(X1) interface should be configured before the LAN(X0) interface. Be prepared to change the IP address of the management computer if it is connected to the LAN(X0) interface.

On the 'Network > Interfaces' page, configure the X0(LAN) interface to Transparent Mode. On the 'Edit Interface' page select "Transparent Mode" for 'IP Assignment' and select "Create new address object" for the 'Transparent Range' field. This will pop up the 'Edit Address Object' page. Create a new Address Object named "transparent range 50-100". The zone assignment will be "LAN" and type will be "Range". The starting address will be "1.1.1.50" and the ending IP address will be "1.1.1.100". Click 'OK' to continue.

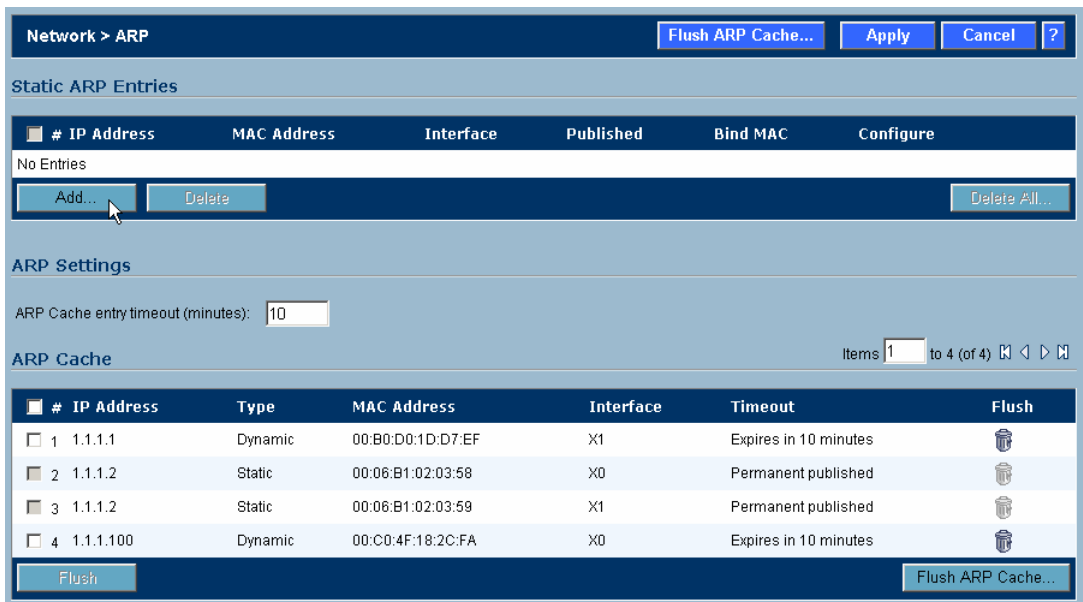


Tech Note

This brings you back to the 'Edit Interface' page. Click 'OK' to continue. Be prepared to change the IP address of the management computer at this point if it is connected to the LAN(X0) interface to an IP address from the transparent range address object that was just created.



Go to the 'Network > ARP' page. In the 'Static ARP Entries' section, click on the 'Add...' button to enter the IP address of the gateway of the secondary subnet. Since the gateway is the router connected to the WAN interface, the MAC address of router will be used to create the static ARP entry. The secondary subnet gateway is not bound to the SonicWALL – it just passes through the SonicWALL to the upstream router.



Tech Note

On the 'Add Static ARP' popup page, enter the IP address that will be the gateway for the secondary subnet, in this example, enter "2.2.2.2". Then choose the interface for the gateway of the secondary subnet, in this example the gateway of the secondary subnet will be on the WAN(X1) interface. Enter the MAC Address of the router interface connected to the WAN(X1) interface that acts as the gateway for the secondary subnet, in this example, "00:B0:D0:1D:D7:EF".

NOTE: Do not select the 'Publish Entry' radio button, as doing so will cause the SonicWALL to respond to ARP queries for 2.2.2.2, in effect replacing the MAC Address of the router with the MAC address of the WAN(X1) interface. Click 'OK' to continue.

IP Address: 2.2.2.2
Interface: X1
MAC Address: 00:B0:D0:1D:D7:EF
 Publish Entry
 Bind MAC Address
 Update IP Address Dynamically
Ready
OK Cancel

The IP address will now appear in the 'Static ARP Entries' table and the 'ARP Cache' table. Since the same physical interface of the router is used for the gateway of both the primary and secondary subnets, the MAC address of the router interface is associated with both gateway IP addresses. The SonicWALL then resolves both gateway IP addresses to the same MAC address of the router interface.

Network > ARP [Flush ARP Cache...] [Apply] [Cancel] [?]

Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
<input type="checkbox"/> 1	2.2.2.2	00:b0:d0:1d:d7:ef	X1			[Refresh] [Delete]

[Add...] [Delete] [Delete All...]

ARP Settings

ARP Cache entry timeout (minutes): 10

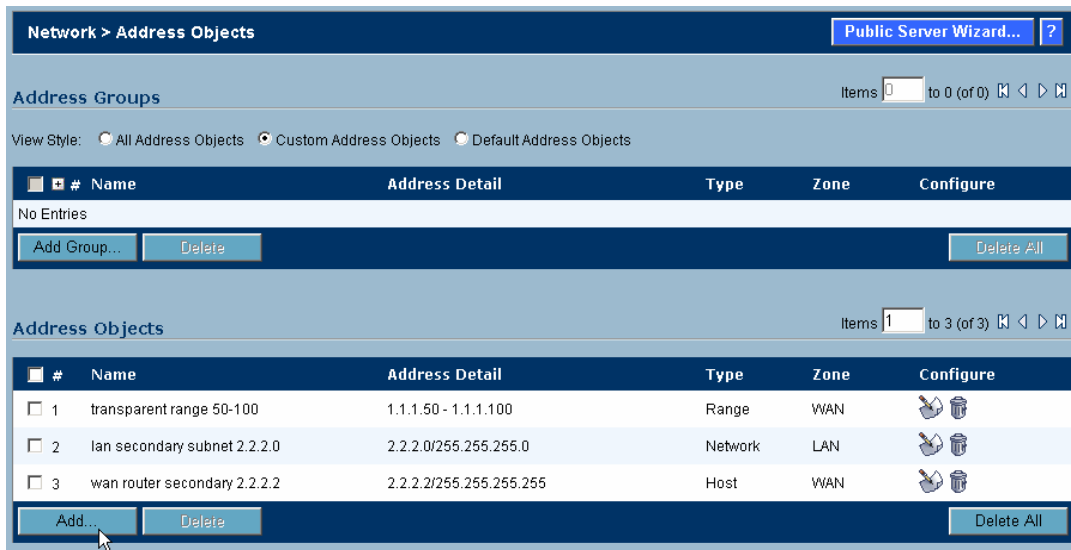
ARP Cache Items 1 to 5 (of 5) [Refresh] [Left] [Right] [Refresh]

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
<input type="checkbox"/> 1	1.1.1.1	Dynamic	00:B0:D0:1D:D7:EF	X1	Expires in 10 minutes	[Trash]
<input checked="" type="checkbox"/> 2	1.1.1.2	Static	00:06:B1:02:03:58	X0	Permanent published	[Trash]
<input checked="" type="checkbox"/> 3	1.1.1.2	Static	00:06:B1:02:03:59	X1	Permanent published	[Trash]
<input type="checkbox"/> 4	1.1.1.100	Dynamic	00:C0:4F:18:2C:FA	X0	Expires in 10 minutes	[Trash]
<input checked="" type="checkbox"/> 5	2.2.2.2	Static	00:B0:D0:1D:D7:EF	X1	Permanent	[Trash]

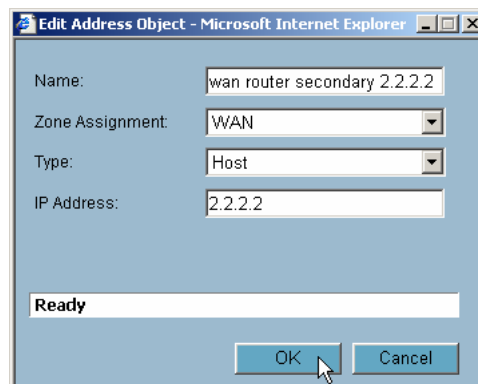
[Flush] [Flush ARP Cache...]

Tech Note

Now create the address objects to be used in the routing policies. First create the 'Address Object' for the secondary interface on the WAN router (2.2.2.2). Then create the address object for the secondary subnet (2.2.2.0/24) on the LAN interface. Go to the 'Network > Address Objects' and click on the 'Add...' button in the 'Address Objects' section. The 'Add Address Object' page will then pop up.



The first address object will be named "wan router secondary 2.2.2.2" and it will be used to represent the secondary interface of the router connected to the WAN interface. The 'Zone Assignment' is "WAN". The 'Type' is "Host" and the 'IP Address' is "2.2.2.2". Click 'OK' to finish and then click on the 'Add...' button again to create a second address object.



Tech Note

The second address object will be named "lan secondary subnet 2.2.2.0" and it will be used to represent the secondary subnet (2.2.2.0/24) connected to the LAN interface. The 'Zone Assignment' is "LAN". The 'Type' is "Network". The 'Network' is "2.2.2.0" and the 'Netmask' is "255.255.255.0". Click 'OK' to finish.

Microsoft Internet Explorer - Edit Address Object

Name: lan secondary subnet 2.2.2.0

Zone Assignment: LAN

Type: Network

Network: 2.2.2.0

Netmask: 255.255.255.0

Ready

OK Cancel

Next, go to the 'Network > Routing' page. The new route policies are for the secondary subnet so that the SonicWALL will consider it valid traffic and be able to route it properly. If the route policy is not added the SonicWALL will drop the traffic and log it as an attack.

Route Policies Items 1 to 10 (of 10) < > <>

View Style: All Policies Custom Policies Default Policies

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
<input checked="" type="checkbox"/> 1	transparent range 50-100	LAN Primary IP	Any	0.0.0.0	X0	20	1		
<input type="checkbox"/> 2	Any	WLAN Subnets	Any	0.0.0.0	X0	20	2		
<input checked="" type="checkbox"/> 3	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	3		
<input checked="" type="checkbox"/> 4	Any	Default Gateway	Any	0.0.0.0	X1	20	4		
<input type="checkbox"/> 5	Any	wan router secondary 2.2.2.2	Any	0.0.0.0	X1	20	5		
<input checked="" type="checkbox"/> 6	Any	transparent range 50-100	Any	0.0.0.0	X0	20	6		
<input checked="" type="checkbox"/> 7	Any	WAN Primary Subnet	Any	0.0.0.0	X1	20	7		
<input type="checkbox"/> 8	Any	lan secondary subnet 2.2.2.0	Any	0.0.0.0	X0	20	8		
<input checked="" type="checkbox"/> 9	WAN Primary Subnet	Any	Any	Default Gateway	X1	20	9		
<input checked="" type="checkbox"/> 10	Any	0.0.0.0/0	Any	1.1.1.1	X1	20	10		

Add... Delete Delete All

Tech Note

The first route policy is for the secondary interface of the router. In the 'Route Policies' section, click on the 'Add...' button and the 'Edit Route Policy' page will popup. On the 'Edit Route Policy' page, select "Any" as the 'Source'. In the 'Destination' field select the "wan router secondary 2.2.2.2" address object previously created. The 'Service' is "Any", 'Gateway' is "0.0.0.0", 'Interface' is "X1" which is the WAN interface and the 'Metric' is "20" which is the default for a locally attached network. Optionally add a 'Comment' to help identify this route policy. Click 'OK' to finish adding the policy.

Then click the 'Add...' button again to add the next route policy.

General

Route Policy Settings

Source: Any

Destination: wan router secondary 2.2.2.2

Service: Any

Gateway: 0.0.0.0

Interface: X1

Metric: 20

Comment:

Disable route when the interface is disconnected

Ready

OK Cancel Help

The next route policy is for the secondary subnet on the LAN interface. On the 'Edit Route Policy' page, select "Any" as the 'Source'. In the 'Destination' field select the "lan secondary subnet 2.2.2.0" address object previously created. The 'Service' is "Any", 'Gateway' is "0.0.0.0", 'Interface' is "X0" which is the WAN interface and the 'Metric' is "20" which is the default for a locally attached network. Optionally add a 'Comment' to help identify this route policy. Click 'OK' to finish adding the policy.

General

Route Policy Settings

Source: Any

Destination: lan secondary subnet 2.2.2.0

Service: Any

Gateway: 0.0.0.0

Interface: X0

Metric: 20

Comment: secondary lan subnet route

Disable route when the interface is disconnected

Ready

OK Cancel Help

Tech Note

The new route policies now appear in the 'Route Policies' table at number 5 & 8 in this example. The SonicWALL now knows how to route traffic to and from the secondary subnet.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	transparent range 50-100	LAN Primary IP	Any	0.0.0.0	X0	20	1		
2	Any	WLAN Subnets	Any	0.0.0.0	X0	20	2		
3	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	3		
4	Any	Default Gateway	Any	0.0.0.0	X1	20	4		
5	Any	wan router secondary 2.2.2.2	Any	0.0.0.0	X1	20	5		
6	Any	transparent range 50-100	Any	0.0.0.0	X0	20	6		
7	Any	WAN Primary Subnet	Any	0.0.0.0	X1	20	7		
8	Any	lan secondary subnet 2.2.2.0	Any	0.0.0.0	X0	20	8		
9	WAN Primary Subnet	Any	Any	Default Gateway	X1	20	9		
10	Any	0.0.0.0/0	Any	1.1.1.1	X1	20	10		

NAT Policies and Access Rules

The default NAT policies and Access Rules will support multiple subnets of the same type without modification. This means that the defaults will support either example #1 or example #2 (NAT mode or Transparent Mode). So in both examples, the default policies will work without adjustment.

If the mixed mode operation of NAT and Transparent Mode is required, the default policies will not be sufficient. More specific NAT Policies and Access Rules will need to be created to support a mixed mode operation of NAT and Transparent Mode.

Tighter or custom security translations also require more specific NAT policies and Access Rules to be created as the defaults are generalized.

Version 1.1
20 July 2005

