

TechNote

SonicOS

Configuring WAN Failover & Load-Balancing

Introduction

This new feature for SonicOS 2.0 Enhanced gives the user the ability to designate one of the user-assigned interfaces as a Secondary or backup WAN port. The Secondary WAN port can be used in a simple 'active/passive' setup, where traffic is only routed through the Secondary WAN port if the Primary fixed WAN port is down and/or unavailable. In this technote, we will refer to this feature as 'basic failover'. It can also be used in a more dynamic 'active/active' setup, where the user can choose a method of dividing outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port. This latter feature will be referred to as 'load balancing'.

Note: WAN Failover & Load-Balancing is only available in SonicOS Enhanced, and is not available in SonicOS Standard or earlier SonicWALL firmware 6.x releases.

Caveats

- When using the WAN Failover & Load-Balancing feature, please upgrade the SonicWALL to SonicOS Enhanced 2.0.1.5 or newer; earlier versions had issues that have been resolved with this release
- Although this technote uses a SonicWALL TZ170 for example purposes, the concepts and methods apply to a SonicWALL PRO2040, PRO3060, or PRO4060 device with SonicOS Enhanced installed
- WAN Failover & Load-Balancing applies outbound-initiated traffic only; it cannot be used to perform inbound load-balancing functions such as what a content switch or load-balancing appliance provides
- Make sure that the device has the proper NAT policies for the secondary WAN interface -- an incorrect or missing NAT Policy for the Secondary WAN port is the most common problem seen when configuring WAN Failover & Load-Balancing
- It is not currently possible to configure source-based or service-based static routes in SonicOS 2.0 and force specific outbound traffic out a particular WAN port; this capability will be introduced in SonicOS 2.5, which is expected to be released in late Q2 2004
- The Primary and Secondary WAN ports cannot be on the same IP subnet; each WAN connection must be on unique IP subnets in order to work properly
- For specific situations, it's possible to use an external DDNS service and client to map an internal server to the Primary and Secondary WAN IP addresses using a single fully-qualified domain name, when using basic active/passive failover – configuration examples are at the end of this technote.
- As noted, WAN Failover & Load-Balancing is currently only available in SonicOS Enhanced firmware.

Task List

- Configure an interface as Secondary WAN port
- Configure/Check NAT Policy for Secondary WAN port
- Activate WAN Failover/Load-Balancing
- Choose WAN Failover/Load-Balancing method
- Optional Step – Set Probe Monitoring
- Optional Step – Integrate DDNS Service and Client

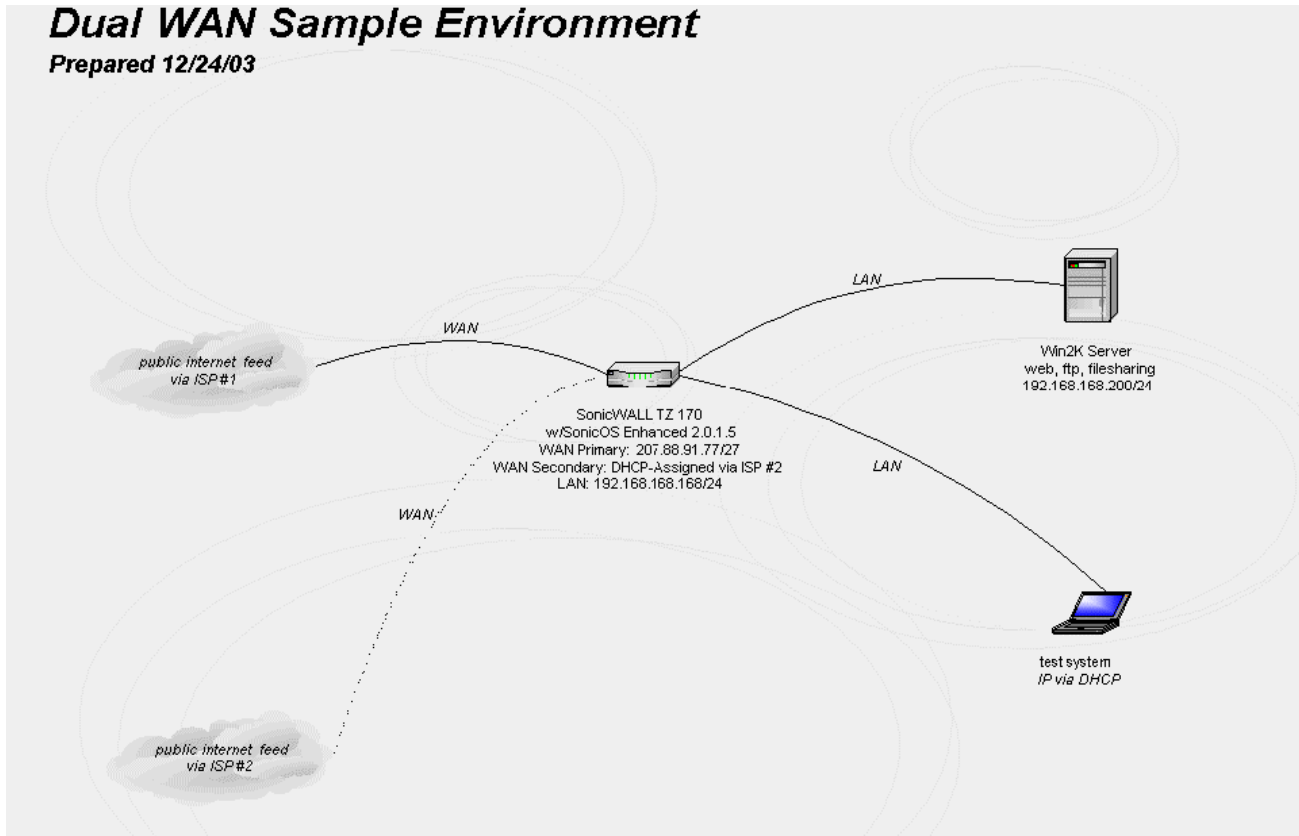


Tech Note

Sample Environment

Dual WAN Sample Environment

Prepared 12/24/03



Setup Steps

On 'Network > Interfaces' page, configure the chosen port to be in WAN zone, and enter in the correct address settings provided by the Secondary ISP. In the example, our TZ170 is acquiring its secondary WAN address dynamically from ISP #2, using DHCP.

The screenshot shows the 'Interface 'X2' Settings' dialog box in the SonicWALL configuration interface. The 'Advanced' tab is selected. The 'Zone' is set to 'WAN' and 'IP Assignment' is set to 'DHCP'. The 'Host Name' field is empty. The 'Comment' field contains 'backup DSL Line'. Under 'Management', 'HTTP' is unchecked, 'HTTPS' is checked, 'Ping' is checked, and 'SNMP' is unchecked. Under 'User Login', 'HTTP' and 'HTTPS' are both unchecked. The 'IP Address', 'Subnet Mask', 'Gateway (Router) Address', 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3' fields all contain '0.0.0.0'. The 'Lease Expires' field contains '2004-02-02 21:36:33'. At the bottom of the dialog are 'Renew', 'Release', and 'Refresh' buttons. Below the dialog is a status bar showing 'Ready' and 'OK', 'Cancel', and 'Help' buttons.

If the SonicWALL is running SonicOS 2.0.1.5 Enhanced or newer, please note that the tab next to 'General' has changed to read 'Advanced', whereas in earlier versions it read 'Ethernet'. In 2.0.1.5 and newer, any interface added to the WAN zone will by default create a NAT Policy allowing internal LAN subnets to NAT out this Secondary WAN interface (see example on next page).

Tech Note

The screenshot shows the 'Ethernet Settings' dialog box in SonicWALL. It has two tabs: 'General' and 'Advanced'. The 'General' tab is active. Under 'Ethernet Settings', 'Link Speed' is set to 'Auto Negotiate'. 'Use Default MAC Address' is selected with the value '00:06:B1:04:02:26'. 'Interface MTU' is set to '1500'. There are checkboxes for 'Fragment non-VPN outbound packets larger than this Interface's MTU' (unchecked) and 'Ignore Don't Fragment (DF) bit' (checked). The 'Bandwidth Management' section has 'Enable Bandwidth Management' unchecked and 'Available Interface Bandwidth (Kbps)' set to '20,000,000'. The 'NAT Policy Settings' section has 'Create default NAT Policy automatically' checked. At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

If the SonicWALL is running a version of Enhanced prior to 2.0.1.5, you will need to manually create the NAT Policy for the Secondary WAN interface in order for the SonicWALL to successfully route traffic through it. To create the policy, go to the 'Network > NAT Policies' page and create a rule like the one below, specifying either 'Any' or 'LAN Subnets' as the 'Original Source', and the address object corresponding to the chosen interface as the 'Translated Source' (see example below).

The screenshot shows the 'Edit NAT Policy' dialog box in a Microsoft Internet Explorer browser window. The 'General' tab is active. It contains several dropdown menus: 'Original Source' (Any), 'Translated Source' (X2 IP), 'Original Destination' (Any), 'Translated Destination' (Original), 'Original Service' (Any), and 'Translated Service' (Original). 'Inbound Interface' is set to 'LAN' and 'Outbound Interface' is set to 'OPT'. There is a checked 'Enable' checkbox. Below is a 'Comment' section with a text box containing 'Backup NAT Policy'. At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

On 'Network > WAN Failover & LB' page, check the 'Enable Load Balancing' checkbox and click on the 'Apply' button. Adjust the interface settings per your environment, although defaults will probably suffice (i.e. check the interface every 5 seconds to make sure it's up, deactivate the interface after 3 missed intervals of 5

Tech Note

seconds, and reactivate the interface after 3 successful intervals of 5 seconds). An example is below:

The screenshot displays the SonicWall configuration interface for WAN Failover & Load Balancing. The left sidebar shows the navigation menu with 'Network' selected. The main content area is titled 'WAN Failover & Load Balancing' and includes the following settings:

- Enable Load Balancing
- Primary WAN Interface: WAN
- Secondary WAN Interface: X2
- Check Interface every: 5 seconds
- Deactivate Interface after: 3 missed intervals
- Reactivate Interface after: 3 successful intervals
- Enable Probe Monitoring (with a 'Configure...' button)

Below these settings is the 'Outbound Load Balancing Method' section, where 'Basic Active/Passive Failover' is selected. A checkbox for 'Preempt and fallback to Primary WAN when possible' is checked. The 'Per Connection Round-Robin' method is also visible but not selected.

On the right side, there is a 'WAN Load Balancing Statistics' table:

WAN Load Balancing Statistics		
WAN Interface Statistics	WAN	X2
Link Status:	Link Up	Link Up
Load Balancing State:	Active - Available	Available
Probe Monitoring:	Disabled	Disabled
New Connections:	4259	0
Total Connections:	91202	0
Rx Unicast Packets:	1153271	365
Rx Bytes:	82934244	43720
Tx Unicast Packets:	219113	4
Tx Bytes:	61844338	3830
Tx Current Percentage:	97	3
Tx Current Throughput (KB/s):	16	0

At the bottom of the configuration window, a status message reads: 'Status: The configuration has been updated.'

You will need to choose a WAN Failover & Load-Balancing method. By default, the SonicWALL will select 'Basic Active/Passive Failover' as the method. In the current release of SonicOS Enhanced, there are four Load Balancing Methods in SonicOS Enhanced:

1. **Basic Active/Passive Failover** -- when selected, the SonicWALL will only send traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. The SonicWALL is set to use this as the default load balancing method. If the Primary WAN fails, then the SonicWALL will revert to this method instead of the ones described below. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode). This item has an associated 'Preempt and fail back to Primary WAN when possible' checkbox that, when selected, will cause the SonicWALL to switch back to sending its traffic across the primary WAN when it resumes responding to the SonicWALL's checks (the WAN's physical link is restored, or the logical probe targets on the WAN port resume responding).
2. **Per Destination Round-Robin** -- when selected, the SonicWALL will load-balance outgoing traffic on a per-destination basis. This is a simple load balancing method and, though not very granular, allows the user to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed). The SonicWALL will need to examine outbound flows for uniqueness in source IP and destination IP and make the determination as to which interface to send the traffic out of and accept it back on. Please note this feature will be overridden by specific static route entries.
3. **Spillover-Based** -- when selected, the user can specify when the SonicWALL starts sending traffic through the Secondary WAN interface. This method allows the administrator to control when and if the Secondary interface is even used. This method will be used when users do not really want outbound traffic sent across the Secondary WAN unless the Primary WAN is overloaded. The SonicWALL has a non-GUI-exposed hold timer set to 20 seconds – if the sustained outbound traffic across the Primary WAN interface exceeds the user-defined Kbps exceeds this, then the SonicWALL will spill outbound traffic to the Secondary WAN interface (on a per-destination basis). The user entry box should not have a default entry and be left empty for the user. Please note this feature will be overridden by specific static route entries.

Tech Note

4. Percentage-Based -- when selected, the user can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces. This method allows the user to actively utilize both Primary and Secondary WAN interfaces. Only one entry box is required (percentage for Primary WAN), as the SonicWALL will auto-populate a non-user-editable entry box with the remaining percentage assigned to the Secondary WAN interface. Please note this feature will be overridden by specific static route entries.

Optional – Enable Probe Monitoring

If Probe Monitoring is not activated, the SonicWALL device will perform physical monitoring only on the Primary and Secondary WAN interfaces – meaning it will only mark a WAN interface as failed if the interface is disconnected, or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios, i.e. routing issues with your ISP, or an upstream router that is no longer passing traffic. For example, if the WAN interface is connected to a hub or switch, and the router providing the connection to the ISP (also connected to this hub or switch) were to fail, the SonicWALL will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

Enabling Probe Monitoring allows the SonicWALL device to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem. And, when using this feature, it will continue to do physical monitoring as well.

If Probe Monitoring is activated and the settings are left blank, the SonicWALL will perform an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router will cause the SonicWALL to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform truly reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred since many devices on the public Internet now actively drops or blocks ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the SonicWALL will assume that the link is usable and continue to send traffic across it.

Quick explanation of the AND/OR Logic:

- The AND option requires that both the Probe Target and the Optional Probe Target are active and responding for the link to be considered up. Both the Probe Target and the Optional Probe Target must have valid entries, or the SonicWALL will mark the link as failed and remove it from service. Use this method when you wish to do a 'deep check'.
- The OR option requires that only one of the Probe Targets are active and responding for the link to be considered up. The Optional Probe Target is not required when using the OR logic.

To configure Probe Monitoring, go to the 'Network > WAN Failover & LB' page. Check the box next to 'Enable Probe Monitoring', and click on the 'Configure...' button. From the pop-up that appears, enter in the settings you wish to use as probe targets. In the example below, the SonicWALL is configured to perform an ICMP ping on a server located on the public Internet as its Primary WAN Probe Target, and to perform an ICMP ping on a different server located on the public Internet as its Secondary WAN Probe Target. When done,



Tech Note

click on the 'OK' button to save and activate the changes.

The screenshot shows a configuration window titled "Primary WAN Probe Settings" and "Secondary WAN Probe Settings". Each section has a "Probe Target" dropdown menu set to "Ping (ICMP)", an "IP Address" text box, and a "Port" text box. In the Primary section, the IP Address is "4.2.2.1" and the Port is "80". In the Secondary section, the IP Address is "4.2.2.2" and the Port is "80". Below each section is an "OR" dropdown menu. At the bottom of the window, there is a "Ready" status bar and three buttons: "OK", "Cancel", and "Help".

Optional – Implementing a DDNS Service and Client

In the following example, we'll be configuring a SonicWALL device connected to two different ISPs to provide access to a single internal webserver via a single fully-qualified domain name (FQDN), utilizing the free public DDNS service from DynDNS, and a third-party DDNS Client (in this case, 'DirectUpdate') running on the internal webserver. The webserver will be accessed using the SonicWALL's WAN IP addresses, and will not have its own unique public IP addresses.

Using this setup, the DDNS Client will perform scheduled checks to ensure that the IP address registered to the FQDN has not changed; in the event that the Primary WAN fails and the Secondary WAN becomes active, the DDNS Client will detect this, and will automatically change the IP address associated with the FQDN on DynDNS's servers. This ensures that external users out on the public Internet can always access an internal server with only a single FQDN, regardless of what WAN interface is being used.

Before we begin, please note that this only works with the basic failover method, and does not work with any of the active/active load-balancing methods.

Steps:

Configure the SonicWALL for basic failover, using the steps outlined in previous sections of this technote.

If you do not already have one, create a free account at <http://www.dyndns.org/services/dyndns/>. During the account creation process, you will need to provide an email address that DynDNS can contact you at to verify the account creation (they will provide full details for activating the free account in this email).

Log into DynDNS using your account, go to the 'Dynamic DNS' section, and click on 'Add Host'. On the page that appears, create the FQDN you wish to use (for example, 'siebelweb.dyndns.org'), enter in the Primary WAN IP address of the SonicWALL, and click on the 'Add Host' button. This creates the record that the DDNS Client will then update to reflect which WAN interface is currently active.

Tech Note

Obtain and install a DDNS Client on the internal webserver. In this example, we'll be using 'DirectUpdate', which can be downloaded from <http://www.directupdate.net/> (it's shareware, and costs only \$15 to register). Once the software installs, you will need to configure it with the DynDNS account information. Launch the 'DirectUpdate' admin program and click on the 'Status' page. Next to 'Accounts:', click on the 'Create' button. In the pop-up button that appears, choose 'dyndns.org (dynamic)' from the drop-down list, enter in your DynDNS account and password, then click on the 'OK' button. Check the box next to 'Force update every 28 days to keep the account active'. Click on the 'Edit Detection Settings' button, and set it to check the IP every 60 seconds. When done with these settings, close the program to save and activate the changes.

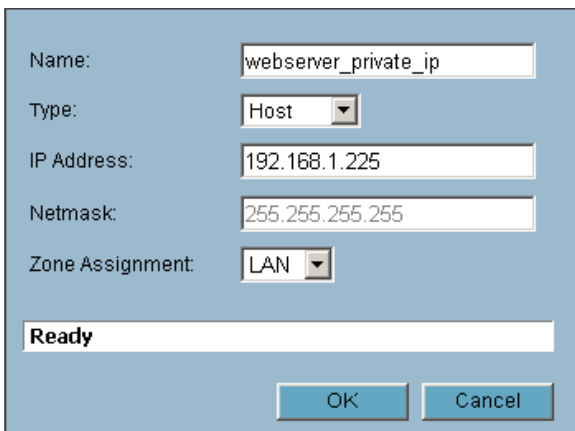
Next, we need to configure the firewall policy in the SonicWALL for access to server against WAN IP and Secondary WAN IP (example, WWW server on port 80) Go to the 'Firewall > Access Rules' page. Click on the policy edit icon for 'WAN > LAN' to bring up the security policy for WAN to LAN. On the page that appears, click on the 'Add...' button and create a policy allowing HTTP access from 'Any' Source to 'All WAN IP' Destination (see example on next page). When done, click on the 'OK' button to save and activate the security policy.

The screenshot shows the 'Advanced' tab of a SonicWALL firewall policy configuration window. The 'Action' is set to 'Allow'. The 'Service' is 'HTTP', 'Source' is 'Any', 'Destination' is 'All WAN IP', 'Users Allowed' is 'All', and 'Schedule' is 'Always on'. 'Logging' is checked. A comment field contains 'allow public access to webserver'. The status bar shows 'Ready'.

Now, create an address object for the internal webserver. Go to the 'Network > Address Objects' page and click on the 'Add...' icon at the bottom of the page. In the pop-up that appears, assign the webserver a name, select 'Host' from the drop-down, enter in the webserver's private internal IP address, and select 'LAN' from

Tech Note

the drop-down. When done, click on the 'OK' button to save and activate the change. An example is below.

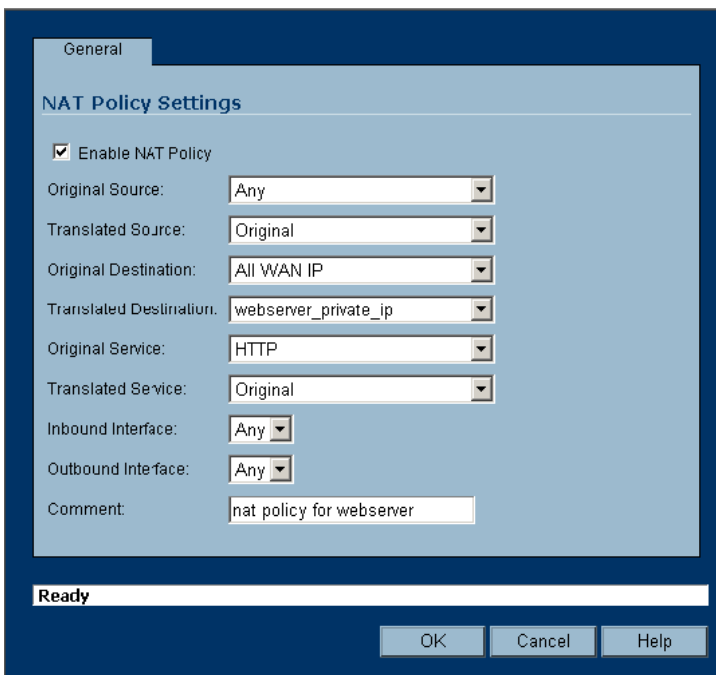


A configuration dialog box with a light blue background. It contains the following fields:

- Name:
- Type:
- IP Address:
- Netmask:
- Zone Assignment:

At the bottom, there is a status bar with the text "Ready" and two buttons: "OK" and "Cancel".

Finally, create a NAT Policy to bind the WAN IP addresses of the SonicWALL to the internal private IP address of the webserver. An example is below.



A configuration dialog box titled "NAT Policy Settings" with a dark blue header. The "General" tab is selected. It contains the following fields:

- Enable NAT Policy
- Original Source:
- Translated Source:
- Original Destination:
- Translated Destination:
- Original Service:
- Translated Service:
- Inbound Interface:
- Outbound Interface:
- Comment:

At the bottom, there is a status bar with the text "Ready" and three buttons: "OK", "Cancel", and "Help".

Test connectivity from an external source by accessing the internal webserver using the custom FQDN you created on the DynDNS site. If you cannot access it, check the previous steps and try again. Once you have successfully tested connectivity using the Primary WAN, disconnect it and allow the SonicWALL to fail over to the Secondary WAN interface. From an internal system, verify that you can access sites on the public Internet, to make sure the Secondary WAN is indeed active and passing traffic. Wait 5-10 minutes, and check access to the internal webserver from an external source – you should be able to access the internal webserver again, even though the SonicWALL is running on the Secondary WAN interface. Note: your system may cache the initial DNS resolution of the Primary WAN IP address; if you're using the same

Tech Note

external system to test, it may be necessary to reboot, or wait a while before testing.

Last Edited: May 2008