SonicOS Enhanced 4.0: NAT Load Balancing

This document describes how to configure the Network Address Translation (NAT) & Load Balancing (LB) features in SonicOS Enhanced 4.0.

- Feature Overview, page 1
- Using NAT Load Balancing, page 4
- Troubleshooting NAT Load Balancing, page 10
- Appendix: Details of Load Balancing Algorithms, page 11

Feature Overview

This section provides an introduction to the NAT Load Balancing feature. It contains the following subsections:

- NAT LB Mechanisms, page 2
- Which NAT LB Method Should I Use?, page 3
- Caveats, page 3

Network Address Translation (NAT) & Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP & LB feature on the SonicWALL appliance. While both features can be used in conjunction, WAN ISP & LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

This document details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or SonicWALL SSL-VPN appliances. This Virtual IP may be independent of the SonicWALL appliance or it may be shared, assuming the SonicWALL appliance itself is not using the port(s) in question.

The examples in this document use two SonicWALL PRO 4100 appliances in high-availability mode, two generic Web servers, and two SonicWALL SSL-VPN 2000 appliances. Please note that it is not necessary to have two appliances to perform NAT/LB – it is just another layer of protection that can be easily added to your environment to assure uptime to critical internal resources that have high uptime requirements (typically a driving factor in load balancing systems in the first place).
Please note that the load balancing capability in SonicOS Enhanced 4.0, while fairly basic, will satisfy the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence, and health-check mechanisms are advised to use a dedicated third-party load balancing appliance (prices run from US$4,000 to US$25,000 per device).

**NAT LB Mechanisms**

NAT load balancing is configured on the **Advanced** tab of a NAT policy.

SonicOS offers the following NAT methods:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.

- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.

- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (e.g. when you want to precisely control how traffic from one subnet is translated to another).

- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.

- **NAT Method** – This drop-down allows the user to specify one of five load balancing methods: Sticky IP, Round Robin, Block Remap, Symmetric Remap, or Random Distribution. For most purposes, Sticky IP is preferred.
• **Enable Probing** – When checked, the SonicWALL will use one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the SonicWALL can direct traffic away from a non-responding resource, and return traffic to the resource once it has begun to respond again.

### Which NAT LB Method Should I Use?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Deployment Example</th>
<th>NAT LB Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribute load on server equally without need for persistence</td>
<td>External/ Internal servers (i.e. Web, FTP, etc.)</td>
<td>Round Robin</td>
</tr>
<tr>
<td>Indiscriminate load balancing without need for persistence</td>
<td>External/ Internal servers (i.e. Web, FTP, etc.)</td>
<td>Random Distribution</td>
</tr>
<tr>
<td>Requires persistence of client connection</td>
<td>E-commerce site, Email Security, SSL-VPN appliance (Any publicly accessible servers requiring persistence)</td>
<td>Sticky IP</td>
</tr>
<tr>
<td>Precise control of remap of source network to a destination range</td>
<td>LAN to DMZ Servers</td>
<td>Block Remap</td>
</tr>
<tr>
<td>Precise control of remap of source network and destination network</td>
<td>Internal Servers (i.e. Intranets or Extranets)</td>
<td>Symmetrical Remap</td>
</tr>
</tbody>
</table>

### Caveats

- The NAT Load Balancing Feature is only available in SonicOS Enhanced 4.0 and newer.
- Only two health-check mechanisms at present (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms at present (Sticky IP only).
- No “sorry-server” mechanism at present if all servers in group are not responding.
- No “round robin with persistence” mechanism at present.
- No “weighted round robin” mechanism at present.
- No method for detecting if resource is strained, at present.
- While there is no limit to the number of internal resources the SonicWALL appliance can load-balance to, and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+resources) may impact performance.
Using NAT Load Balancing

This section contains the following subsections:

- NAT Load Balancing Topology, page 4
- Prerequisites, page 4
- Configuring NAT Load Balancing, page 5

NAT Load Balancing Topology

Figure 1 shows the topology for the NAT load balancing network.

Prerequisites

The examples shown in the Tasklist section on the next few pages utilize IP addressing information from a demo setup – please make sure and replace any IP addressing information shown in the examples with the correct addressing information for your setup. Also note that the interface names may be different.

It is strongly advised that you enable logging for all categories, and enable name resolution for logging.
To enable logging and alerting, log into the SonicWALL’s Management GUI, go to Log > Categories, choose Debug from the drop-down next to Logging Level, choose All Categories from the drop-down next to View Style, check the boxes in the title bar next to Log and Alerts to capture all categories, and click on the Apply button in the upper right hand corner to save and activate the changes. For an example, see the screenshot below. Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

To enable log name resolution, go to Log > Name Resolution, choose DNS then NetBios from the Name Resolution Menu drop-down list, and click on the Apply button in the upper right hand corner to save and activate the changes. For an example, see the screenshot below.

### Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1. Create address objects.
2. Create address group.
3. Create inbound NAT LB Policy.
4. Create outbound NAT LB Policy.
5. Create Firewall Rule.
6. Verify and troubleshoot the network if necessary.
To complete this configuration, perform the following steps:

**Step 1  Create Network Objects** -- Go to the Network > Address Objects page in the Management GUI and create the network objects for both of the internal Web servers, and the Virtual IP (VIP) on which external users will access the servers.

**Step 2  Create Address Group** -- Now create an address group named **www_group** and add the two internal server address objects you just created.
Using NAT Load Balancing

**Step 3** Create Inbound NAT Rule for Group -- Now create a NAT rule to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method. For an example see the screenshot below.

**Note** Do not save the NAT rule just yet.

![SonicOS Enhanced 4.0: NAT Load Balancing](image)

**Step 4** Set LB Type and Server Liveliness Method -- On the **Advanced** tab of the NAT policy configuration control, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, since that is what people are trying to access). You can now click on the **OK** button to save and activate the changes.

![SonicOS Enhanced 4.0: NAT Load Balancing](image)
Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. If you do not see the two messages below (with your IP addresses), check the steps above.

**Step 5** Create Outbound NAT Rule for LB Group -- Write a NAT rule to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface.
**Step 6** Create Firewall Rule for VIP -- Write a firewall rule to allow traffic from the outside to access the internal Web servers via the VIP.

![Firewall Rule Configuration](image)

**Step 7** Test Your Work – From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.

**Note** If you wish to load balance one or more SSL-VPN Appliances, repeat steps 1-7, using HTTPS instead as the allowed service.
Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the Firewall > Access Rules page and mouse-over the Statistics icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources. For an example of a working rule, see the screenshot below.

You can also check the Firewall > NAT Policies page and mouse-over the Statistics icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources. For an example of a working NAT LB policy, see the screenshot below.

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the SonicWALL appliance and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the SonicWALL appliance.
Appendix: Details of Load Balancing Algorithms

This appendix describes how the SonicWALL security appliance applies the load balancing algorithms:

- **Round Robin** - Source IP connects to Destination IP alternately
- **Random Distribution** - Source IP connects to Destination IP randomly
- **Sticky IP** - Source IP connects to same Destination IP
- **Block Remap** - Source network is divided by size of the Destination pool to create logical segments
- **Symmetrical Remap** - Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

### Sticky IP Algorithm

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works.

**Example one:**

102.168.0.2 to 102.130.0.4
Translated Dest = 10.50.165.0/30 (Network)

Packet Src IP = 192.168.0.2
102.168.0.2 = 0B040000 = 3222226552 = 11000000010101000000000000000010

**Sticky IP Formula** = Packet Src IP = 3222226552 (modulo) TransDest Size = 2

= 3222226552 (modulo) 2

= 0

2 divides into numerator evenly, there is no remainder thus 0

Destination remapping to 10.50.165.1

**Example two:**

102.168.0.2 to 102.162.0.4
Translated Dest = 10.50.166.1 - 10.50.165.2 (Range)

Packet Src IP = 102.138.0.2
102.138.0.2 = 0C040002 = 3232226602 = 11000000010101000000000000010010

**Sticky IP Formula** = Packet Src IP = 3232226602 (modulo) TransDest Size = 3

= 3232226602 (modulo) 3

= 10 7F411290.666667 10 7F411290
- 0.666667 × 3

= 2

Destination remapping to 10.50.166.2