

SonicWALL Single Arm Mode Concept and Configuration

*Prepared by SonicWALL, Inc.
6/11/2002*

Introduction:

SonicWALL's 'Single-Arm mode' technology was developed by RedCreek Communications for their Ravlin product line but was integrated into SonicWALL firmware to further expand an already broad VPN feature set. Single-Arm mode allows a SonicWALL to connect its WAN interface onto a subnet and essentially function as a 'router- on a stick,' allowing traffic to come in on the WAN interface, get encrypted according to the appropriate SA, and then get sent out the same interface.

This feature has shown to add a great deal of value for sites, which require VPN, but require that the device be non-intrusive and simply sit on a subnet outside the firewall or on an isolated interface/subnet (as opposed to bridge-between/route-between 2 subnets). This also allows the user to offload VPN functionality to a separate firewall to remove the burden of encryption/decryption from the Internet access firewall.

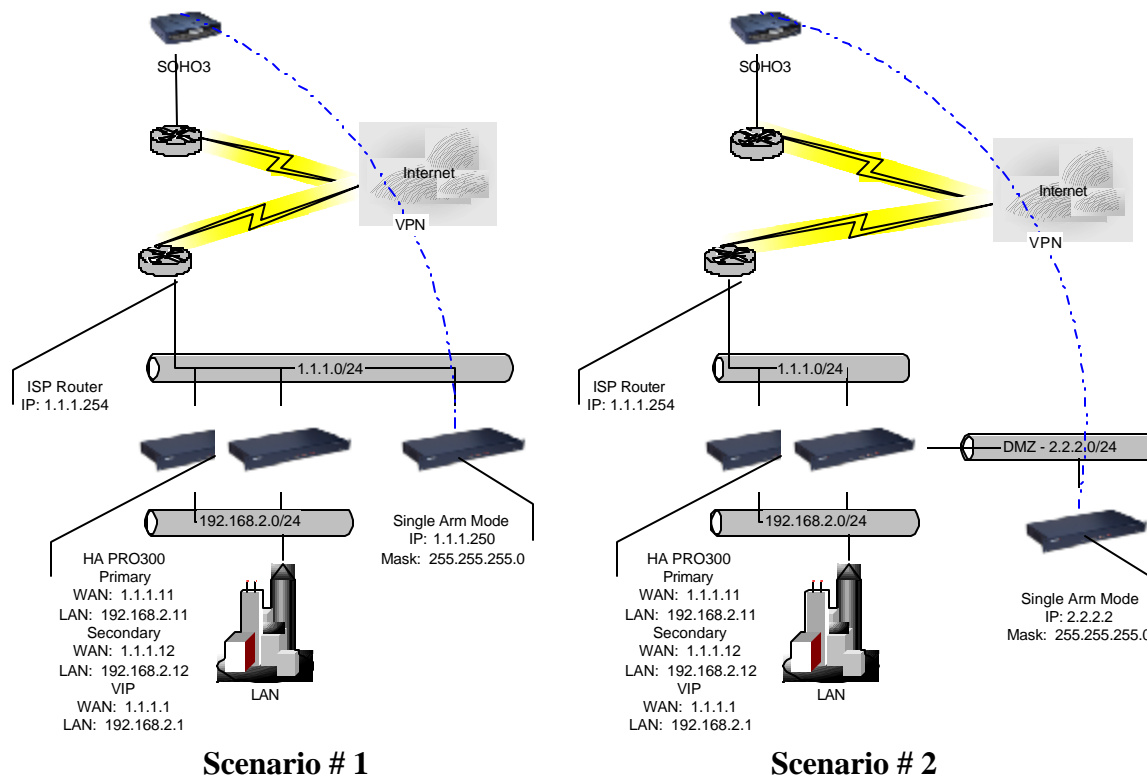
Disclaimer:

This document was written assuming the user has a fundamental understanding of TCP/IP, routing and security concepts, as well as a working familiarity w/SonicWALL configuration. It is meant to assist in understanding the differences in concept and configuration between SonicWALL Single Arm mode and other more commonly used addressing modes. For a more basic configuration guide, please consult the SonicWALL Configuration Guide that shipped with the SonicWALL device.

Conceptual:

To better understand Single Arm mode, it helps to understand some of the typical designs and deployments. Below are two of the more common designs utilizing single arm mode:

SonicWALL Single Arm Mode Concept and Configuration



Above we see 2 typical deployments that can be used, both of which allow the single arm mode firewall to be utilized as a dedicated VPN box (encryptor). The design also allows the box to be isolated and secured from the Corporate LAN by the Internet access firewall.

Scenario #1:

In the first scenario, the single arm mode firewall resides on the WAN subnet in the case where the remote site prefers to not have any device placed within their existing infrastructure. This allows for their main trusted firewall to remain in complete control of what's going in and out of the network, and removes the possibility of unchecked access into the corporate environment.

Scenario #2:

In the second scenario, the single arm mode firewall resides on the firewall's DMZ. This deployment is ideal for 2 main reasons:

1. This allows for VPN connectivity to be created without using the Internet access firewall to encrypt traffic. It allows for a box to be dedicated for Internet access and a box to be dedicated for VPN encryption (so processor/memory intensive VPN encryption/decryption doesn't bog down the Internet access firewall). This can be thought of and sold as 'VPN offloading'.
2. This allows for access rule security to be enforced on traffic once it has gotten through the VPN tunnel before it is allowed to drop into the corporate network. This also provides security for transmissions between the single arm mode firewall and the Internet access firewall.

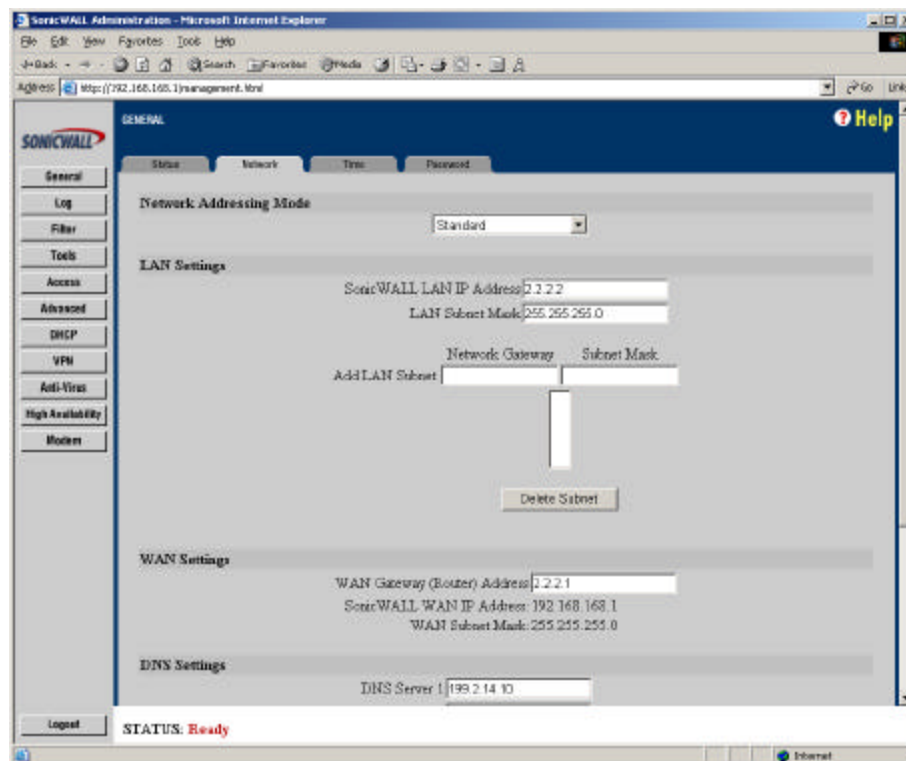
SonicWALL Single Arm Mode Concept and Configuration

Configuration:

Placing a SonicWALL into Single-Arm mode is a very simple task, however, understanding the necessary routing and access rules that must be configured is key to a successful rollout.

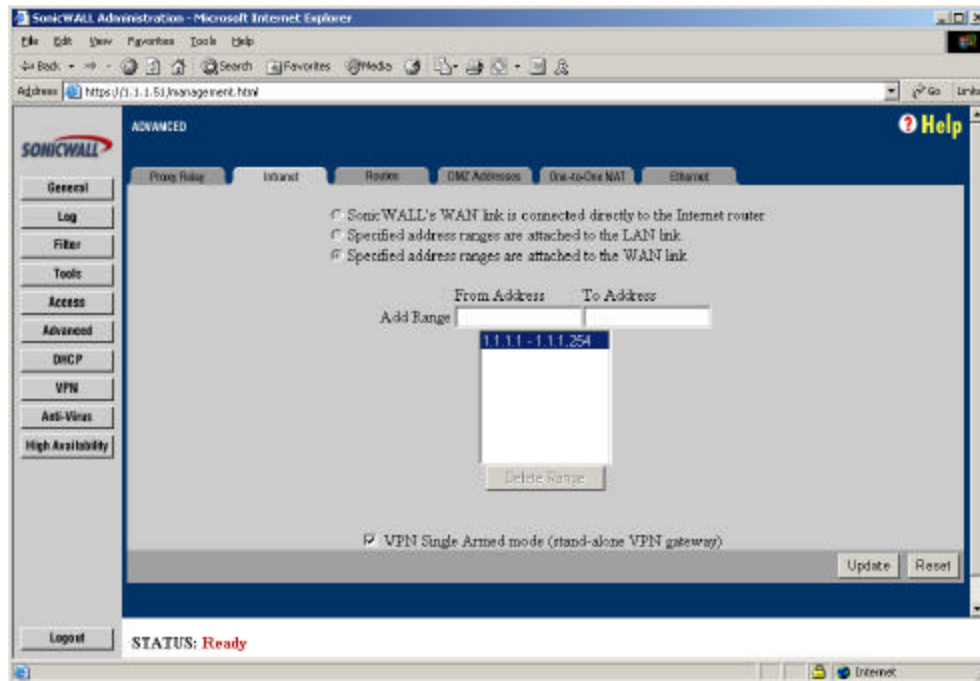
Terminating tunnels to a single arm firewall requires only that remote sites have IKE and IPSec access to the 1 arm firewall, this can be done through a one to one NAT, or through SonicWALL's port forwarding (public LAN server) feature, thus conserving an IP address.

To use Single-Arm mode, the firewall must be placed into 'Standard' or transparent mode (Click on the **General** button, click on the **Network** tab). It should be given the IP address and default gateway appropriate for the subnet that it is being placed on.

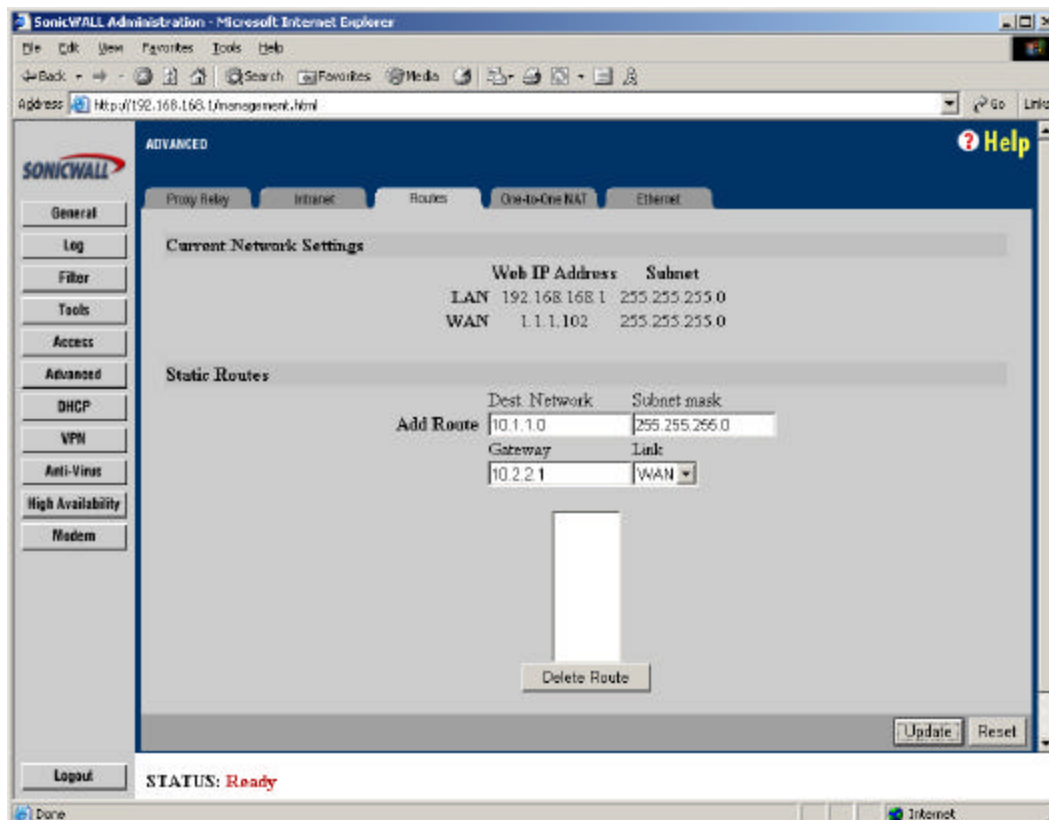


Next, click on the **Advanced** button, and go to the **Intranet** tab. Check the box that says **VPN Single Armed mode (stand-alone VPN gateway)**. Click **Update**.

SonicWALL Single Arm Mode Concept and Configuration



Next, define static routes for all subnets that reside on any of the interfaces of the Internet access firewall, and point the static route to the interface of the Firewall that is on the Single Arm mode Sonicwall's subnet.

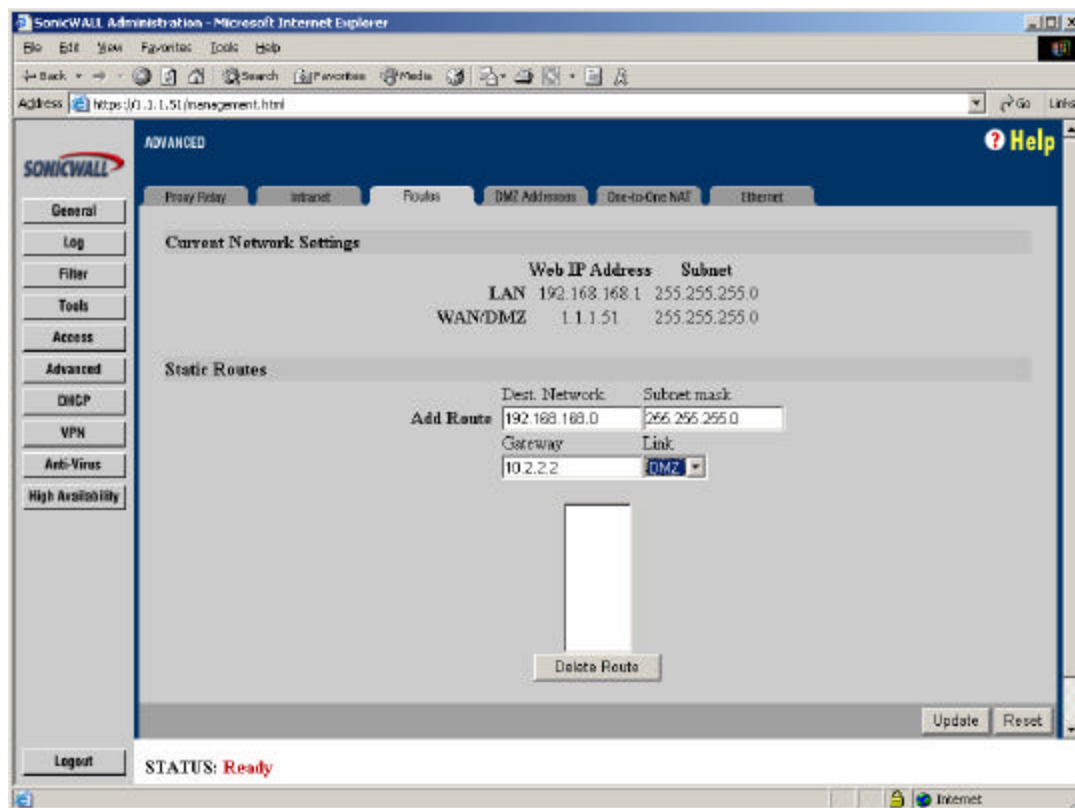


SonicWALL Single Arm Mode Concept and Configuration

The main reasons for the static route are as follows:

1. Traffic bound for other interfaces of the Internet access firewall can be routed appropriately to that firewall. If the Single Arm firewall resides in front of the Internet Access firewall, it will need to have a default gateway of the Internet access router, and will then require static routes to be defined to route traffic into the network through the firewall.
2. SAs can be established to the appropriate routed subnets. Since the SonicWALLs create SAs between the remote firewalls subnets and it's own subnets that are either defined as on an interface, multiple LAN subnet or static route, all subnets that need to connect must be defined as one of these, even though a default route may incidentally be redundant for that static route.
3. Static routes are also needed on the Internet access firewall for the firewall to determine where a remote location's subnets are accessed through (how to reach the remote site through the single arm mode firewall), whether the single arm mode firewall is on the WAN subnet or a DMZ.

Also, static routes are required on the Internet access firewall to route all subnets of the remote site(s) to the interface IP address of the single arm mode firewall.



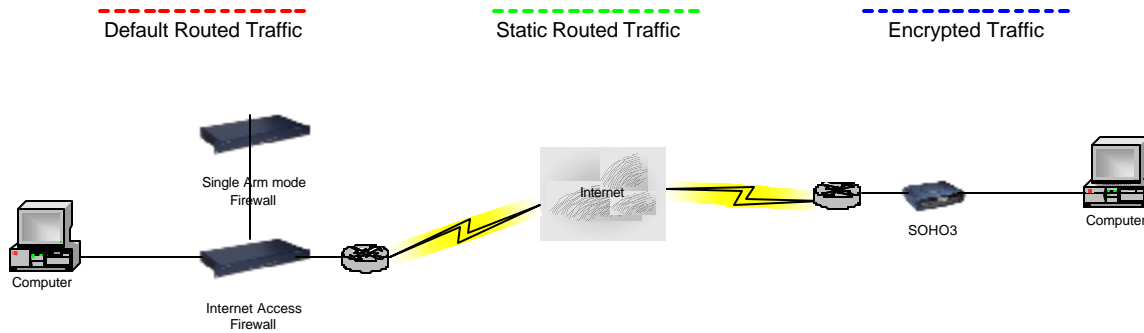
Once this is done, access rules and a one to one NAT must be created to allow IKE and IPSec to pass through from the WAN to the Single Arm firewall on the DMZ (whether through port forwarding or a one to one NAT). Tunnels can then be created from the single arm SonicWALL

Page 5 of 7

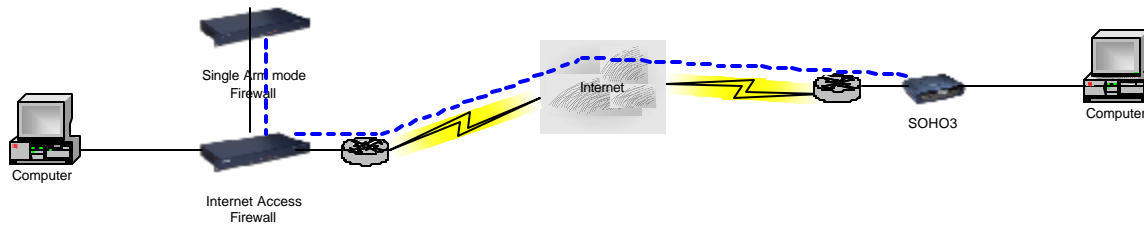
SonicWALL Single Arm Mode Concept and Configuration

to all remote sites, with remote sites defining destination networks that can include the LAN subnet and all subnets defined in the Single Arm firewall's static routes page.

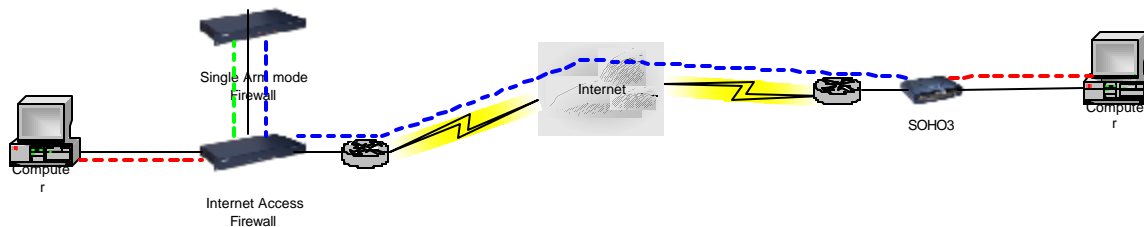
This series of diagrams should more clearly illustrate the traffic/communication that occurs in this configuration.



When an SA is created between the two sites, an IKE negotiation must occur to create an IPsec tunnel between the two encrypting firewalls as shown below:



Once a tunnel is established, traffic can then be sent through the tunnel in either direction as illustrated below:



SonicWALL Single Arm Mode Concept and Configuration

Troubleshooting:

- A good rule of thumb is that any subnets that appear in a static route of the Internet access SonicWALL should have a complimentary static route on the single arm mode firewall routing that subnet back to the Internet access firewall.
- Check to see if the SA is negotiated properly, and if there are 'renegotiate' buttons on the VPN/Status page on both sides. Then try to ping across the tunnel to the opposite end from both sides. Turn on Network Debug in the Log Settings page, and view the logs for any hints as to why it isn't working.
- If the SA is running and both SonicWALLs can ping the opposite sides, make sure the single arm mode SonicWALL has all the needed static routes to route traffic to it's appropriate destination given, that all traffic is otherwise routed to the default router.
- Also make sure that the firewall that the Single arm mode sonicwall is sitting next to, has static routes to route remote network subnets to the single arm mode firewall's IP address.
- Make sure there is sufficient access allowed on the Internet access firewall for traffic both inbound and outbound.
- If the single arm mode sonicwall is on the WAN subnet of the Internet access sonicwall, make sure there is an intranet page entry defining that IP address as being on the WAN link of the Internet access SonicWALL.
- Turn off ARP bridging and be sure to use unique MAC addresses on the .diag page.

Conclusion:

Single Arm mode is yet another way SonicWALL continues to innovate and integrate flexible VPN functionality and value into the product line. Single arm allows for VPN offloading, security policy enforcement through VPN tunnels, and non-intrusive tunnel termination. It is yet another easy to configure and flexible VPN advanced option.