SonicWall's Firewall RMA Policy

What is an RMA?
An RMA is a Return Material Authorization and is required to return SonicWall equipment.

How long do I have to return SonicWall products if I am getting a replacement part?
Customers must return defective parts in accordance with SonicWall's RMA procedure located at our Support Services site within 30 calendar days of receipt of the replacement parts. If the customer has not returned the defective parts (which must conform in quantity and serial number to the RMA request) within 30 calendar days of receipt of the replacement parts, SonicWall will bill the customer the full retail price of the new unit.

Service Scope
The product must be returned with the applicable tamper seal sticker(s) intact to guarantee that the device has not been altered. If the seal is broken for any reason, your hardware service coverage will be voided, and SonicWall cannot accept responsibility for any subsequent damage.

Customer Actions Before Return

Before returning firewall appliances to SonicWall, customers should ensure that all stored data is removed. To do that, you can reset the equipment back to the factory default settings. Please see the instructions below. **Note: Customers should backup their configuration before resetting the firewall appliance.** Here's how to back up settings:

- Factory Default the SonicWall Firewall from UI
- Factory Default the SonicWall Firewall from Safe Mode

If you cannot reset the appliance to its original settings, all data stored on the firewall/storage is encrypted using strong algorithms to help ensure your data is kept safe.

In addition, for Gen7 firewalls, customers may wipe these appliances from the Safemode GUI, which will remove the firmware, settings, data, and logs from the appliance. Here's how to access Safemode Options on SonicWall Gen7 Devices.

Process Regarding the Removal of Data
All products that are sent back to SonicWall go through a process that includes low-level formatting of all media, verifying any failures present in the product, repairing or scrapping when necessary (scrapping is done by a certified vendor with physical destruction of data media), refurbishing previous customer markings if no fault is found, erasing configs, and resetting to factory defaults.

SonicWall's Hard Disk and Compact Flash Wipe and Destruction Process Regarding Handling of Volatile Memory on SonicWall Hardware Appliances, products that contain hard disks and/or compact flash memories ("Products") when they are returned to SonicWall for service or replacement. All these Products returned to SonicWall are wiped of customer data as described below.

Hard disks that fail to operate: Our operations follow the Department of Defense (DoD) 5220-22-M guidelines to protect your sensitive information. Data-bearing Hard drives (HDD) or flash drives that require physical destruction are either "punched" or shredded. It is the most common level of data destruction, which most often meets or exceeds customer requirements.

Hard disks that are functional upon return to factory: They are wiped using a process that complies with the United States Department of Defense 5220.22-M standard for data sanitization. This includes, but is not necessarily limited to, the following steps:

- Overwrite the entire drive with a defined fixed value.
- Overwrite the entire drive with the complement value of the first overwrite run.
- Overwrite the entire drive with pseudo random values.
- Verify drive operation.
- Hard drives that fail step number (4) are destroyed.

Compact Flash (CF) cards are wiped using the card manufacturer's reset feature, which clears all partition tables and resets all data sectors to a defined fixed value. CF operation is then verified and defective CF cards are destroyed.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 Refer to our website for additional information. **www.sonicwall.com**