SOP-NET-001_SonicWall_Setup_v1.0.0

SOP-NET-001_SonicWall_Setup_v1.0.0

Standard Operating Procedure: Initial SonicWall Firewall Setup

Document ID:	SOP-NET-001
Title:	Initial SonicWall Firewall Setup
Category:	Network Administration
Version:	1.4
Status:	Final
Author:	System
Creation Date:	2025-12-02
Approval Date:	2025-12-02

1.0 Purpose

To establish a standardized, repeatable process for the initial out-of-the-box configuration of a new SonicWall firewall, ensuring all baseline security and system settings are applied before deployment.

2.0 Scope

This SOP applies to all Network Technicians responsible for deploying new SonicWall firewalls for clients. It covers the process from device registration to the final pre-installation configuration step.

3.0 Definitions

- **SOP:** Standard Operating Procedure
- **WAN:** Wide Area Network; the port connecting to the internet.
- **LAN:** Local Area Network; the port for the internal network.
- **MySonicwall Portal:** The official online portal for managing SonicWall device licenses, registration, and firmware.

- **GUI:** Graphical User Interface.
- **DNS:** Domain Name System.
- **IPS:** Intrusion Prevention System.
- **Geo-IP:** IP address filtering based on geographic location.

4.0 Roles & Responsibilities

- **Network Technician/Engineer:** Responsible for executing all steps outlined in this SOP, ensuring the firewall is correctly configured for on-site installation.

5.0 Prerequisites

- A new SonicWall firewall device.
- Access to the MySonicwall portal with valid credentials.
- A computer with an Ethernet port.
- Two Ethernet cables.
- Client's network circuit information sheet (containing static IP, subnet, gateway).

6.0 Procedure

6.1 Initial Connection and Access

1. **Register Device:** Log in to the MySonicwall portal and register the new firewall device if it has not been done already.
2. **Connect Hardware:**
   - Connect the firewall's **WAN (X1)** port to an active internet connection.
   - Connect your computer's Ethernet port to the firewall's **LAN (X0)** port.
3. **Power On:** Power on the SonicWall and wait for the status lights for both WAN and LAN ports to turn solid green.
4. **Configure Static IP:** On your computer, manually configure the IPv4 network adapter settings as follows:
   - **IP address:** `192.168.168.2`
   - **Subnet mask:** `255.255.255.0`
   - **Default gateway:** `192.168.168.168`
   - **DNS Server:** `8.8.8.8` (or any other public DNS)
5. **Log In to Firewall:**
   - Open a web browser in incognito/private mode and navigate to `http://192.168.168.168`.
   - Use the default credentials to log in:
     - **Username:** `admin`
     - **Password:** `password`

- You will be prompted to change the administrator password. Set a new, secure password.
- When prompted for setup type, select **Manual Setup**.

6.2 Device Registration Verification (CRITICAL - Before Firmware)

IMPORTANT: Device registration MUST be fully verified before attempting firmware upload. Firmware upload will fail with "Device not registered" error if this step is incomplete.

1. **Check Registration Status on Firewall:**
   - Navigate to **Device > Settings > MySonicWall** (or **System > Administration > MySonicWall**).
   - If status shows "Not Registered", proceed to step 2.
   - If status shows "Registered", skip to Section 6.3.
2. **Obtain Registration Code from MySonicWall Portal:**
   - Log in to mysonicwall.com.
   - Navigate to **My Products** and click on the registered device.
   - Locate the **Registration Code** in the device details.
   - If device is not yet registered in portal, register it first using the Serial Number and Authentication Code from the firewall.
3. **Enter Registration Code on Firewall:**
   - On the firewall's MySonicWall page, enter the **Registration Code** obtained from the portal.
   - Click **Register** or **Submit**.
   - Wait for confirmation message.
4. **Verify Registration Complete:**
   - Refresh the page and confirm status shows "Registered".
   - Navigate to **Device > Settings > Licenses** and verify licenses are synchronized.
   - **Do NOT proceed to firmware update until registration is confirmed.**
5. **Troubleshooting Registration:**
   - If registration fails, restart the firewall and retry.
   - Ensure firewall has internet access (WAN connected and routing).
   - Verify MySonicWall account has the device under correct tenant.

6.3 System Configuration

1. **Set Firewall Name:** Go to **Device > Settings > Administration**. Set a descriptive name for the firewall (e.g., `Obera-Fairhope`).
2. **Configure Admin Timeout:**
   - On the same page, under **Login/Multiple Administrators**, change **Log out the Admin after inactivity (minutes)** to `60`.
3. **Configure Time Zone and NTP:**
   - Navigate to **Device > Settings > Time**.

- Set **Time Zone** to the client's local time zone (e.g., `America/Chicago` for Central).
- Enable **Use NTP to set time**.
- Set **NTP Server 1** to `time.google.com`.
- Set **NTP Server 2** to `pool.ntp.org`.
- Click **Accept** to save.
- **Note:** Accurate time is critical for logging, certificates, and security event correlation.

4. **Enable Remote Management:** Navigate to **Network > System > Interfaces**. Edit the **X1 (WAN)** interface. Under **Management**, enable **HTTPS** only. Leave HTTP and Ping disabled for security.

6.4 Firmware Update

IMPORTANT: Always check the firmware upgrade path in the Release Notes before upgrading. Direct upgrades across major versions may not be supported.

1. **Check Current Firmware Version:**
   - Note the current version from the Dashboard or **Device > Settings > Firmware & Backups**.
   - Example: `7.0.1-5165`
2. **Download Release Notes and Check Upgrade Path:**
   - Go to the MySonicwall portal and select the firewall.
   - Navigate to the **Downloads** tab.
   - Download the **Release Notes PDF** for the target firmware version.
   - Search for "upgrade path" or "supported upgrade" in the Release Notes.
   - **Key Rule:** If jumping multiple major versions (e.g., 7.0.x to 7.3.x), stepped upgrades may be required.
3. **Determine Upgrade Path:**
   - **Single step OK:** Minor version upgrades within same major version (e.g., 7.0.1 → 7.0.3).
   - **Stepped upgrade required:** Major version jumps - download intermediate firmware versions.
   - Example stepped path: `7.0.1 → 7.3.0 → 7.3.1`
4. **Download Required Firmware:**
   - Download all required `.sig` files from MySonicwall portal.
   - For stepped upgrades, download each intermediate version.
5. **Export Configuration Backup:**
   - Navigate to **Device > Settings > Firmware & Backups**.
   - Click **Export Settings** and save the `.exp` file.
   - **Store backup securely** - see SOP-NET-006.
   - **WARNING:** Once upgraded to newer major version, downgrade may not be supported.
6. **Upload and Apply Firmware:**

- Click **Upload Firmware** and select the `.sig` file.
- If registration error occurs, return to Section 6.2.
- After upload completes, click **Boot Uploaded Firmware**.
- Select "Boot with current configuration".
- The firewall will reboot (3-10 minutes).

7. **Verify Upgrade and Repeat if Stepped:**
   - Log back in after reboot.
   - Confirm new firmware version on Dashboard.
   - Test basic connectivity (internet, management access).
   - **If stepped upgrade:** Repeat steps 5-7 for each intermediate version until target version reached.

6.5 Network DNS Configuration

1. Navigate to **Network > DNS**.
2. Select **Specify DNS Servers Manually**.
3. Configure DNS entries based on the client's environment:
   - **With Domain Controllers:** Set DNS Server 1 and 2 to the client's primary and secondary domain controllers. Set DNS Server 3 to a public DNS (e.g., `8.8.8.8`).
   - **Without Domain Controllers:** Set DNS servers to the ISP-provided DNS or a reliable public DNS service (e.g., `8.8.8.8`, `1.1.1.1`).

6.6 Final WAN Interface Configuration

WARNING: Executing this final step will reconfigure the WAN (X1) interface, and you will lose access to the firewall's management GUI until it is physically installed at the client's site. Ensure all previous configuration steps are completed and verified before proceeding.

1. Navigate to **Network > Interfaces**.
2. Locate the **X1 (WAN)** interface and click the pencil icon to edit it.
3. Refer to the client's circuit sheet for the following information:
   - Set **IP Assignment** to **Static**.
   - Enter the **IP Address** (first usable IP from the client's static block).
   - Enter the **Subnet Mask**.
   - Enter the **Default Gateway**.
   - Set the **DNS Server(s)** to either the client's domain controllers or public DNS (e.g., `8.8.8.8`, `1.1.1.1`).
4. Under the **Management** section for the X1 interface:
   - Enable **HTTPS** for remote management.
   - Leave **Ping** disabled unless required for external monitoring tools.
   - **Security Note:** Enabling Ping on WAN allows ICMP reconnaissance. Only enable if client requires it for monitoring.
5. Click **Accept** to save the changes. Access to the GUI will be lost. The firewall is now ready for on-site installation.

7.0 Verification & Quality Checks

- Confirm the device is registered and all licenses are active in the MySonicwall portal.
- Verify the firmware has been updated to the latest stable release.
- Confirm the WAN interface settings are transcribed correctly from the client circuit sheet before clicking the final 'Accept'.

8.0 Troubleshooting

Issue	Resolution
Cannot access login page at 192.168.168.168.	1. Verify your computer's static IP settings match Section 6.1. 2. Ensure the Ethernet cable is securely connected to the LAN (X0) port. 3. Confirm the firewall's LAN light is green.
Licenses fail to synchronize.	1. Ensure the WAN port is connected to an active internet connection. 2. Verify the MySonicwall portal credentials are correct. 3. Reboot the firewall and try again.
Lost access after WAN configuration.	This is expected behavior. The device must now be installed on-site to be accessed via its new WAN or LAN IP address.
Firmware upload fails with "Device not registered".	1. Complete Section 6.2 registration verification. 2. Get Registration Code from MySonicWall portal. 3. Enter code on firewall's MySonicWall page. 4. Restart firewall if sync fails.
"Serial number registered to another account" error.	Device is registered under different MySonicWall account (e.g., different tenant). Log into correct account or contact SonicWall support for transfer.

Issue	Resolution
Firmware upgrade fails or bricks device.	1. Firewall will auto-rollback to backup firmware. 2. Check release notes for required upgrade path. 3. May need stepped upgrades (e.g., 7.0→7.3.0→7.3.1).

9.0 Related Documents

- Client Network Circuit Information Sheet
- SOP-NET-004: Register Device in MySonicwall
- SOP-NET-006: SonicWall Configuration Backup
- SOP-NET-007: SonicWall Configuration Restore
- SonicOS Release Notes (download from MySonicWall for each firmware version)

10.0 Revision History

Version	Date	Author	Change Description
1.0	2025-12-02	System	Initial document creation from source material.
1.1	2025-12-29	Jeremy Smith	Added Section 6.2 for device registration verification before firmware upload. Expanded Section 6.4 with firmware upgrade path checking, stepped upgrade process, and release notes review. Lessons learned from Jubilee Pool & Spa deployment.

Version	Date	Author	Change Description
1.2	2025-12-29	Jeremy Smith	Removed Security Services Configuration and Network DNS Configuration sections (will be separate SOP). Renumbered Final WAN Interface Configuration to 6.5.
1.3	2025-12-29	Jeremy Smith	Added back Section 6.5 Network DNS Configuration. Renumbered Final WAN Interface Configuration to 6.6.
1.4	2025-12-29	Jeremy Smith	SME Review: Added NTP/Time Zone configuration in Section 6.3. Updated WAN management to disable Ping by default (security hardening). Clarified remote management security notes.

11.0 Approval

Name	Role	Signature	Date
	Network Manager		