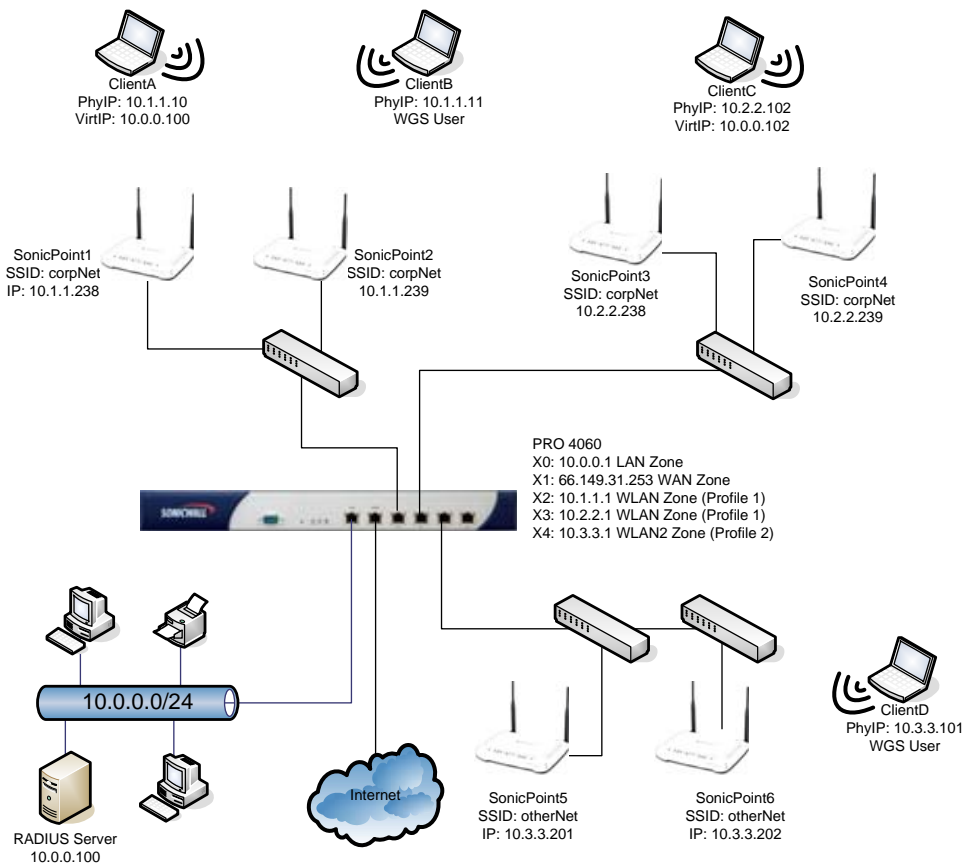


▷ SONICWALL TECH NOTE:

SonicPoint and SonicOS Enhanced 2.5

Distributed Wireless Architecture

As the proliferation of wireless continues in the workplace and within nearly every service industry, it becomes increasingly important to support more diverse, and more geographically expansive wireless network configurations. To accommodate wireless installations larger than those that can be serviced by the high powered SOHO TZW and TZ 170 Wireless, SonicOS Enhanced 2.5 incorporates and builds upon the security and usability innovations of SonicWALL's standalone wireless security products, allowing it to act as the center of a distributed wireless network. To extend the reach and intelligence of the core, up to 128 SonicPoint Access Points can be connected to a SonicWALL appliance (the total number of supported SonicPoints is platform dependent) running SonicOS Enhanced 2.5 or greater.



▷ SONICWALL TECH NOTE:

Table of Contents

DISTRIBUTED WIRELESS ARCHITECTURE	1
SONICPOINT AND SONICOS WLAN ZONE FEATURES.....	3
SONICPOINT MODES OF OPERATION	3
SONICPOINT RADIO CHARACTERISTICS.....	6
802.11D COMPLIANCE	7
WIRELESS ZONES: THE WLAN ZONE	8
SONICPOINT ENFORCEMENT.....	8
WIRELESS FIREWALLING	9
WIFISEC ENFORCEMENT / WPA.....	11
WIRELESS ROAMING	13
GUEST SERVICES.....	15
MAC FILTERING VIA MAC ADDRESS OBJECTS	17
SONICPOINT PROFILES	17
AUTOMATIC PROVISIONING (SDP & SSPP).....	19
SONICPOINT STATES	19
MANAGED MODE AND STAND-ALONE MODE TRANSITIONS.....	20
EVENT AND STATISTICS REPORTING	21
SAFEMODE	23
STAND-ALONE MODE	24
LEDS.....	28
RESET SWITCH	28

▷ SONICWALL TECH NOTE :

SonicPoint and SonicOS WLAN Zone Features

The SonicPoint offers the following capabilities:

- Tri-Mode, Dual-Band, Dual-Radio 802.11a/b/g operation for simultaneous support of 802.11a and 802.11g/b clients
- WPA and WEP Encryption with EAP-PEAP, EAP-TTLS, TKIP and AES Support
- 802.11a/g Turbo modes for data rates up to 108 mbit
- 802.11d compliance
- 802.3af Power over Ethernet
- Managed Mode and Stand-Alone modes of operation
- Rogue Access Point discovery and BSSID/MAC Address Object authorization
- Safemode for recovery

Because of the high throughput capabilities of the SonicPoint, aggregate SonicPoints have the potential to exhaust the capacity of Fast Ethernet interfaces. As such, the following table illustrates—per platform—the maximum number of SonicPoints per interface, and the total recommended number of SonicPoints per appliance:

Managing Security Appliance	Wireless Zone Assignable Interfaces	Maximum # of SonicPoints per WLAN Interface	Recommended # of SonicPoints per Appliance
TZ 170 Series	1 Fast Ethernet	2 SonicPoints	2 SonicPoints
PRO 2040	2 Fast Ethernet	8 SonicPoints	8 SonicPoints
PRO 3060	4 Fast Ethernet	8 SonicPoints	16 SonicPoints
PRO 4060	4 Fast Ethernet	16 SonicPoints	32 SonicPoints
PRO 5060	4 Fast/Gig Ethernet	32 SonicPoints	128 SonicPoints

SonicPoint Modes of Operation

SonicPoint devices can operate in two modes, namely, Stand-Alone Mode and Managed Mode. The mode of operation is automatically selected by the SonicPoint depending on its environment. When the SonicPoint starts up, it will announce itself via SDP (SonicWALL Discovery Protocol) Advertisement broadcasts. If it has a layer 2 attachment to a Wireless Zone interface on a SonicWALL (i.e. connected directly, via a hub, or via a switch) the SonicWALL and the SonicPoint will negotiate a peer-relationship, and the SonicPoint will enter Managed Mode. Once a peer relationship has been established, a SonicPoint will remain wedded to its peered SonicWALL so as to prevent conflicts in the event of multiple SonicWALLs sending SDP on a single segment. The peering can be manually broken from the SonicOS GUI, and peer relationships can also be imposed via manual synchronization from the SonicOS GUI.

▷ SONICWALL TECH NOTE :

If the SonicPoint cannot discover or be discovered by a SonicWALL within 5 seconds of startup, it will reboot into Stand-Alone Mode. When operating in Stand-Alone mode, the SonicPoint will assume a default IP address of **192.168.1.20**, a default username of **admin**, and a default password of **password**. SonicPoints maintain their Stand-Alone and Managed Mode configurations separately so that they do not conflict with, or overwrite one another.

SonicPoints will dynamically transition from one mode to the other in response to environmental changes. For example, if a SonicPoint starts in Stand-Alone mode, but is then plugged into a Wireless Zone, it will respond to SDP Discovery packets from the SonicWALL and will transition to Managed Mode. Alternatively, if the SonicPoint is operating in Managed Mode and it loses its connection with the SonicWALL for 6 minutes, it will transition to Stand-Alone mode. Transitioning from one state to the other requires the SonicPoint to reboot, as do most configuration changes during operation. The reboot process takes approximately 1 minute.

When operating in Stand-Alone Mode, the SonicPoint will function much like a conventional Access Point, configurable via its integrated web-based GUI. The SonicPoint Stand-alone UI has been modeled after the SonicOS UI, but it does not precisely match the SonicPoint configuration interface within SonicOS. Like other generation-four SonicWALL devices, the SonicPoint features SafeMode to facilitate recovery from compromised states of operation. When the SonicPoint is operating in SafeMode, it will be possible to upload a new firmware image via FTP. This is different from SonicOS devices which use an HTTP POST for firmware uploads. Under normal conditions, it will not be necessary to manually update firmware via with FTP on the SonicPoint. SonicPoint firmware is embedded within SonicOS and updates are automatically performed while operating in Managed Mode as part of the auto-provisioning process.

Operating in Managed Mode requires L2 connectivity to a SonicWALL interface assigned to a Wireless Zone. The Wireless Zone type, whose default instance is the 'WLAN Zone', has certain unique characteristics:

- It has additional configuration tabs for 'Wireless' and 'Guest Services'. The 'Wireless' and 'Guest Services' tabs have the following default settings:
 - WiFiSec Enforcement Enabled
 - Require WiFiSec for Site-to-Site VPN Tunnel Traversal
 - Trust WPA traffic as WiFiSec
 - SonicPoint Provisioning Profile set to 'SonicPoint'
 - Wireless Guest Services Disabled
- It enforces that all traffic that enters the zone arrive from a SonicPoint. All other traffic will be dropped (i.e. traffic from wired network systems, or wireless traffic originating from a non-SonicPoint device). You cannot use a third-party wireless Access Point device in a Wireless Zone.
- It is the only Zone type on which SDP and SSPP operate.
- It is the only Zone type on which Guest Services, and WiFiSec enforcement is available.
- The subnet assigned to the Wireless Zone interface must be at least 24 bits (255.255.255.0 or larger).

▷ SONICWALL TECH NOTE :

- A DHCP scope will be activated on Wireless Zones, and based on the platform, the top range of addresses will be reserved for SonicPoints. Refer to the table on page 3 for platform specific numbers.
- The IP Address assigned to the Wireless Zone interface may not conflict with the SonicPoint address reservations described above (for example, for a /24 subnet on a PRO4060, the assigned address must be .238 or below).
- The WLAN GroupVPN (the default Wireless Zone) will NOT be activated by default, due to the fact that an interface must first be added to correctly auto-create Access Rules. The WLAN GroupVPN must be manually activated, and upon activation will employ the following WiFiSec optimized default settings:
 - HTTP and HTTPS Management via this SA Enabled
 - Require authentication of VPN clients via XAUTH
 - User Group for XAUTH Users set to Trusted Users
 - Cache XAUTH User Name and Password on Client set to Single Session
 - Allow Connections to All Secured Gateways
 - Set Default Route as this Gateway

When in Managed Mode, operating parameters for SonicPoint units will be controlled by the peered SonicWALL security appliance. If a SonicWALL discovers a SonicPoint for which it has no stored configuration, it will consider that SonicPoint to be unprovisioned, and it will use the Zone's assigned SonicPoint Profile to auto-provision the SonicPoint. This can occur in the following cases:

- The SonicPoint had never been previously provisioned
- The SonicPoint had been provisioned, but was manually deleted via the SonicOS GUI
- The SonicPoint was provisioned by one SonicWALL, and then moved to a different SonicWALL that contains no stored configuration for that SonicPoint

As part of the provisioning process, the SonicWALL will store the configuration for that SonicPoint, and will push the configuration to the SonicPoint via SSPP (SonicWALL Simple Provisioning Protocol). Upon receiving the configuration, the SonicPoint will update its configuration, will reboot to affect the changes, and will enter an *operational* state. While still peered with the same SonicWALL, changes to that SonicPoint's configuration will only be possible via the SonicOS GUI, and must be performed at the unit (as opposed to the Profile) level.

While in Managed Mode, the SonicPoint will report its state to the SonicWALL via SDP packets. A full description of SonicPoint state information can be found in the 'SonicPoint States' section of this document. Also included in the SDP packets sent by *operational* SonicPoint devices is a checksum value for its configuration. If the SonicWALL determines from the checksum that there is a disagreement between its configuration checksum for that SonicPoint and that SonicPoint's advertised checksum, it will engage an encrypted SSPP channel with that SonicPoint, and will send it the proper configuration. The SonicPoint will then reboot to assume the corrected configuration.

▷ SONICWALL TECH NOTE :

It is important to note that changing a SonicPoint Profile on the SonicWALL will not update operational SonicPoint units. This is by design, so as to allow Profiles to be added, deleted, and modified with interrupting network operation. SonicPoint Profiles will only affect an unprovisioned SonicPoint device, that is, a SonicPoint for which SonicWALL has no stored configuration. Changing the configuration on an operational SonicPoint requires modification to that SonicPoint's settings (under *Wireless > SonicPoints > SonicPoint Settings*). Alternatively, it is possible to delete the SonicPoint peering from the SonicOS GUI, thus forcing a new auto-provisioning process using the appropriate SonicPoint Profile.

SonicPoint Radio Characteristics

Each SonicPoint contains two separate radios, a 2.4GHz radio for 802.11b and 802.11g, and 5GHz radio for 802.11a. Since the radios are fully distinct, each SonicPoint can simultaneously host 802.11g/b and 802.11a clients, providing the highest level of wireless client compatibility.

SonicPoints support data rates of 6 to 54 Mbps in 802.11a and 802.11g modes, and up to 11 Mbps in 802.11b mode. Turbo Modes are also available in 802.11a and 802.11g modes, providing data rates of up to 108 Mbps.

Depending on the regulatory domain, the 5GHz 802.11a radio supports a maximum of 47 channels, with channel frequencies from 5130MHz to 5825MHz, non-contiguously. In 802.11a Static Turbo Mode, available only within the FCC regulatory domain, it supports 5 channels, with channels frequencies of 5210, 5250, 5290, 5760, and 5800MHz. In 802.11a Dynamic Turbo Mode, also available only within the FCC regulatory domain, it supports and additional 5 channels, with channel frequencies of 5200, 5240, 5280, 5765, and 5805Mhz.

The 2.4Ghz 802.11g/b radio supports a maximum of 14 channels, depending on the regulatory domain, with a frequency range of 2412MHz to 2484MHz. The FCC regulatory domain also allows the channel frequency of 2437MHz to be used for either Static or Dynamic Mode Turbo 802.11g operation.

Note: Regulatory domain information is configured on the SonicPoint during the manufacturing process. When a SonicPoint operated in Stand-alone mode, radio configuration options will be limited to those allowed by the programmed regulatory domain. While operating in Managed Mode, the SonicPoint will advertise its regulatory domain to the managing SonicWALL security appliance via SDP, and the SonicWALL will only allow for radio configuration options appropriate to the advertised regulatory domain.

Frequency Band	802.11a: 5.15~5.25GHz, 5.25~5.35GHz, 5.725~5.825GHz 802.11b/g: 2.412~2.462GHz(US) 2.412~2.484GHz(Japan) 2.412~2.472GHz(Europe ETSI) 2.457~2.462GHz(Spain) 2.457~2.472GHz(France)
Modulation Technology	802.11a/g:

▷ SONICWALL TECH NOTE :

	OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b: DSSS (DBPK, DQPSK, CCK)
Operating Channels	802.11a: 12 for FCC 11 for Europe 4 for Japan 4 for Singapore 4 for Taiwan 802.11b/g: 11 for FCC 14 for Japan 13 for Europe 2 for Spain 4 for France
Receive Sensitivity (typical)	802.11a: -82dBm @ 6Mbps -81dBm @ 9Mbps -79dBm @ 12Mbps -78dBm @ 18Mbps -75dBm @ 24Mbps -72dBm @ 36Mbps -70dBm @ 48Mbps -68dBm @ 54Mbps 802.11b/g: -91dBm @ 1Mbps -90dBm @ 2Mbps -89dBm @ 5.5Mbps -84dBm @ 6Mbps -82dBm @ 9Mbps -87dBm @ 11Mbps -79dBm @ 12Mbps -77dBm @ 18Mbps -75dBm @ 24Mbps -73dBm @ 36Mbps -70dBm @ 48Mbps -68dBm @ 54Mbps
Transmit Output Power (Typical)	802.11a: Up to 20dBm = Up to 100mw 802.11g: Up to 21dBm = Up to 126mw 802.11b: Up to 23dBm = Up to 200mw

802.11d Compliance

802.11d compliance is a regulatory domain update wherein physical and MAC layer signaling automatically behaves in accordance with geographic requirements for such settings as channels of operation and power. Access Points and wireless clients implement 802.11d differently; the Access Point can be thought of as the 802.11d provider, wherein it either provides the 802.11d capability or not - the Access Point remains agnostic to the 802.11d capabilities of associated clients. The wireless client is in turn the 802.11d consumer - if the

▷ SONICWALL TECH NOTE :

client is not 802.11d capable, it can associate with an Access Point regardless of its 802.11d capabilities. If the client is 802.11d capable, it can generally operate in one of 3 802.11d modes:

- **None** - The wireless device will communicate with any other available wireless device, regardless of 802.11d compliance. This is useful for peer-to-peer (IBSS) networking which currently is not supported by the 802.11d standard.
- **Flexible** - The wireless device will communicate with any other available wireless device, and will abide by 802.11d information if it is presented.
- **Strict** - The wireless device will only communicate with devices that support the 802.11d standard.

Wireless Zones: The WLAN Zone

The Wireless Zone type has been added to existing Zone types (Trusted, Untrusted, Public, Encrypted, Multicast) to provide support to SonicPoint Access Points. The default Wireless Zone instance will be the "WLAN Zone".

Interfaces assigned to a Wireless Zone will have the following important and unique characteristics:

- **SonicPoint Enforcement** - As traffic passes from wireless clients through a SonicPoint, the SonicPoint will tag the traffic so that it will be identifiable by a Wireless Zone interface. If the Wireless Zone interface receives traffic that has not been appropriately tagged, it will discard the traffic.
- **Wireless Firewalling** - The next-generation of the Inter-client Communications. The ability to apply firewall Access Rules and Security Services to all wireless client traffic, even client-to-client traffic through a single or multiple SonicPoints.
- **WiFiSec Enforcement** - The ability to require that all traffic that enters into a Wireless Zone interface be either IPsec traffic, WPA traffic, or both.
- **Guest Services** - Guest Services will only be available on interfaces belonging to a Wireless Zone. Recent Guest Services enhancements include Profiles for automated account generation, customizable post-authentication landing page, SMTP Redirection, and the integration of Guest Services accounts and local user accounts and groups.
- **SonicPoint Profiles** - The ability to define profiles containing the complete set of SonicPoint parameters that can be assigned to a Wireless Zone, and inherited by any connected SonicPoint.
- **Automatic SonicPoint Provisioning** - Utilizing the newly developed SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP) SonicPoints will be automatically updated with the latest firmware and configurations by their managing SonicWALL appliance.

SonicPoint Enforcement

SonicPoint Enforcement is automatically enabled on all Wireless Zones, and is undefeatable. This feature requires that any traffic that enters into a Wireless Zone be delivered via a SonicPoint. It will not be possible to pass traffic from an OTS Access Point, or even from a

▷ SONICWALL TECH NOTE:

wired host through a Wireless Zone. Therefore, only SonicPoints should be connected to Wireless Zone interfaces, either directly or through a switch or hub. Layer 2 connectivity between SonicPoints and the managing SonicWALL appliance will be required; routed connections are not supported.

Wireless Zone interfaces will automatically recognize when a SonicPoint has been connected using the SonicWALL Discovery Protocol (SDP). SDP will then conjoin the SonicPoint to the PRO that first discovered it, making it its peer (to protect against the event of a SonicPoint being on an L2 segment with more than one PRO). Once peered, SDP will negotiate encryption parameters and will determine the configuration state of the SonicPoint. If the configuration state is validated by the PRO, the SonicPoint will immediately enter into an operational state. If, however, the PRO determines that the configuration requires some kind of update, it will then engage provisioning mode using the SonicWALL Simple Provisioning Protocol (SSPP) and will reconfigure the SonicPoint as needed.

Wireless Firewalling

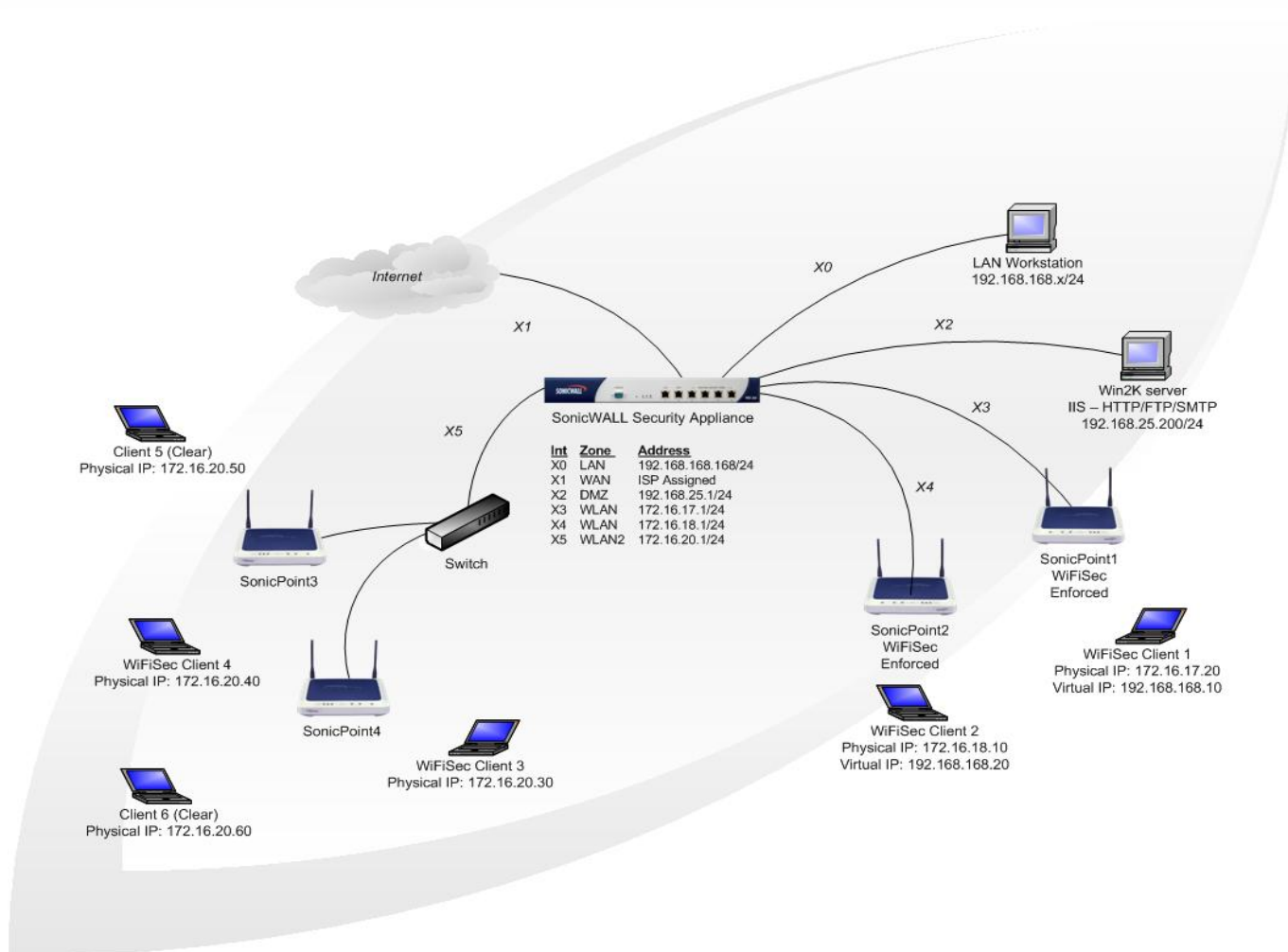
Some high-end wireless Access Points provide the ability to control wireless Inter-client Communications, meaning they can allow or disallow wireless clients connected to that particular Access Point from communicating with each other. These Access Points, however, generally cannot directly control a wireless client's communication with a remote host, such as a wired client, an internet host, or even a wireless client associated with another Access Point.

The Inter-client communication control feature on the SOHO TZW took this control a step further by consolidating the Access Point, Secure Wireless Gateway and the Firewall into a single unit - providing full firewall Access Rule applicability to all wireless traffic on that individual unit.

Wireless Firewalling within the Distributed Wireless Architecture provides this same level of granular control, only in a highly scalable, distributed fashion. It is a function of a design innovation wherein all traffic that enters the wireless interfaces on a SonicPoint is forwarded back to the managing SonicWALL security appliance where it can be processed by firewall Access Rules, NAT Policies, and Security Services. While in Managed mode, Wireless Firewalling allows no direct communication an affected wireless client and any other host, whether connected to the same or a different SonicPoint, or whether wireless or wired; all traffic must traverse the firewall. This can be used, for example, for the following application:

- To control access for all wireless inter-client communications
- To control access for certain wireless client communications with other wireless clients
- To control access for wireless client communications with wired hosts, or Internet hosts
- To control access using Service Objects

▷ SONICWALL TECH NOTE:



Access Rules for Wireless clients are controlled using Zone based intersections and applicable Address Objects. Consider the following examples from the illustration above (Address Objects used are generalized by subnet, and can be made more specific):

Address Object	Type	Address	Netmask	Bound to Zone
192.168.168.0	Network	192.168.168.0	255.255.255.0	VPN
172.16.17.0	Network	172.16.17.0	255.255.255.0	VPN
172.16.18.0	Network	172.16.18.0	255.255.255.0	VPN
172.16.20.0	Network	172.16.20.0	255.255.255.0	VPN

From Host	To Host	From Zone	To Zone	Source Address Object	Destination Address Object
Client 1	Client 2	VPN	VPN	192.168.168.0	192.168.168.0
Client 3	Client 4	VPN	VPN	172.16.20.0	172.16.20.0
Client 2	Client 3	VPN	VPN	192.168.168.10	172.16.20.0
Client 5	Client 6	WLAN2	WLAN2	WLAN2 Subnets	WLAN2 Subnets
Client 6	LAN Workstation	WLAN2	LAN	WLAN2 Subnets	LAN Subnets

Default levels of trust for Wireless Zones are as follows:

▷ SONICWALL TECH NOTE :

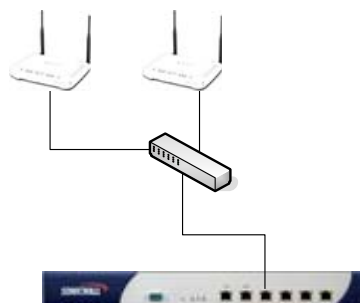
From Zone	To Zone Type	Action
Trusted	Wireless	Allow
Untrusted	Wireless	Deny
Public	Wireless	Deny
Wireless	Trusted	Deny
Wireless	Untrusted	Allow
Wireless	Public	Allow
Wireless	Wireless	Interface Trust
Wireless (custom)	Wireless	Deny
Encrypted (WiFiSec)	Trusted	Allow
Encrypted (WiFiSec)	Untrusted	Allow
Encrypted (WiFiSec)	Public	Allow
Encrypted (WiFiSec)	Wireless	Allow

WiFiSec clients are terminated at the 'WLAN GroupVPN' (or custom Wireless Zone GroupVPN) are associated with the VPN (Encrypted) Zone. By default, the 'WLAN GroupVPN' enables the 'Set Default Route as this Gateway' option (see page 5 for default settings), but VPN Access must still be assigned at the User or Group level (e.g. to 'WLAN RemoteAccessNetworks', which is effectively '0.0.0.0' or 'Any') for access to the Internet and trusted resources.

Access types not covered by the default levels of trust (e.g. WiFiSec to WiFiSec) will require custom Access Rules, and changes to the above default behaviors can be made more or less restrictive by modifying the default rules.

WiFiSec Enforcement / WPA

As introduced on the SOHO TZW, WiFiSec Enforcement is the ability to require that all traffic that traverse the wireless network be IPsec (VPN) traffic. We will be able to enforce the same level of security with the Distributed Wireless Architecture by providing WiFiSec Enforcement at the Zone level; all non-guest wireless clients connected to SonicPoints attached to an interface belonging to a Zone on which WiFiSec is enforced will be required to use the strong security of IPsec. The VPN connection will terminate at the "WLAN GroupVPN", which can be configured independently of "WAN GroupVPN" or other Zone GroupVPN instances.



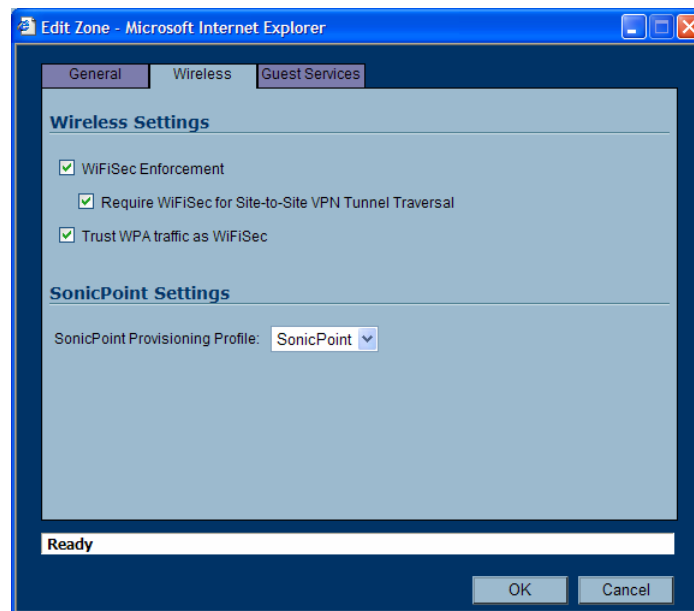
Sensitive to the fact that WPA (WiFi Protected Access) provides security rivaling that of WiFiSec, albeit in a more complicated and less versatile fashion, administrators enabling WiFiSec Enforcement on a Wireless Zone will have the option to accept WPA as an allowable

▷ SONICWALL TECH NOTE :

alternative to IPSec. Both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server) will be supported on SonicPoints.

Consider the above example where there are two SonicPoints connected to the WLAN Zone where WiFiSec is enforced. SonicPoint1 does not have WPA enabled, but WPA is enabled and is 'Trusted as WiFiSec' (meaning it has been allowed as an acceptable alternative to WiFiSec) on SonicPoint2. Non-Guest clients that are connected to SonicPoint1 will have to use IPSec to communicate through the X2 interface on the PRO, or the traffic will be dropped at the interface. Guest clients will be able to associate with SonicPoint1, and use Guest Services. Because WPA is enabled on SonicPoint2, clients connecting to SonicPoint2 *must use* WPA, since WPA is an all-or-nothing technology. This means that Guest clients will either have to have WPA credentials, or they will not be able to associate with SonicPoint2. Once a client provides WPA credentials and successfully associates with SonicPoint2, as traffic passes from SonicPoint2 to the X2 interface, SonicPoint2 will tag the packets as having been transmitted using WPA. The X2 interface will recognize these tags, and will accept the traffic, even if it is not IPSec.

The all-or-nothing restriction of WPA, along with the added complexity of having to maintain an external EAP capable directory service, is perhaps the greatest drawbacks of WPA as compared to WiFiSec. Take, for example, a wireless network wishing to simultaneously offer Guest Services to visiting users and encryption enforcement for access to trusted resources. This combination of differentiated access could easily be afforded by SonicPoint1 using WiFiSec, but Guest users connecting to SonicPoint2 would require the WPA pre-shared key or a previously created EAP account, effectively defeating the extemporaneous and dynamic nature of Guest Services.



“WiFiSec Enforcement” and the “Trust WPA Traffic as WiFiSec” settings are only available on Wireless Zones (i.e. the default WLAN Zone, or user-created Wireless Zone instances).

▷ SONICWALL TECH NOTE:

Because Wireless Zones only accept SonicPoint traffic, only SonicPoints can provide this feature; it will not be possible to provide this security feature with any other WPA-capable OTS Access Point.

Wireless Roaming

As wireless clients move through a distributed wireless network, it is necessary to support roaming from one SonicPoint to another in as non-interruptive a manner as possible. The SonicWALL Distributed Wireless Architecture was designed such that client connections, even across multiple SonicPoint Access Points, traverse a single point - whether it is the physical interface on the SonicOS device, or a Virtualized Adapter via the Global VPN Client (GVC). This method helps to ensure that even as a client moves through the wireless network in nomadic fashion that applications will experience minimal if any interruption, providing a virtually seamless wireless client experience.

Roaming decisions are made by the wireless client, and are done so in a non-prescribed fashion, meaning that different wireless client card vendors can implement different types of roaming decision algorithms. Generally, the roaming process involves the following components:

- The client decides to roam - based on an undefined set of factors, which can include such elements as signal strength, missed beacons, or acknowledgements, the client will enter into a roaming state.
- The client determines where to roam - Once the client has decided to roam, it must then decide where to roam to. Finding an eligible Access Point to roam to is accomplished using some sort of scanning technique, either active or passive, and the scan may be performed either preemptively (before the decision to roam) or reactively (after the decision to roam). The scanning technique employed may or may not affect the client's ability to send and receive data during the scanning process. This varies from vendor to vendor. Some clients cleverly employ power-saving to make this process more seamless - they signal the Access Point to which they're attached that they are entering a power-save mode before starting the scanning process. The client and Access Point then attempt to queue data for the "sleeping" client. During this respite, the client performs its scan. When the client finds a new Access Point, it wakes up, and exchanges queued data with the Access Point.
- The client roams - by de-associating with the old access point, and re-associating with the new access point. Layer 2 connectivity is severed and re-established during this process.
- The client's applications resume - Layer 3 (and higher) communications can resume after layer 2 connectivity is restored. The effect this has on the continuity of the application depends on whether the application is connection-oriented (such as a telnet or SSH session), or connectionless (such as web-browsing). Connection-oriented applications will generally be interrupted by roaming while connectionless applications will exhibit no ill-effects. Many client-server applications, such as a Microsoft Outlook client connection to an Exchange Server, use higher layer logic to automatically re-establish the client-server connection after layer 2/3 connectivity is restored, and these will operate with relative seamlessness.

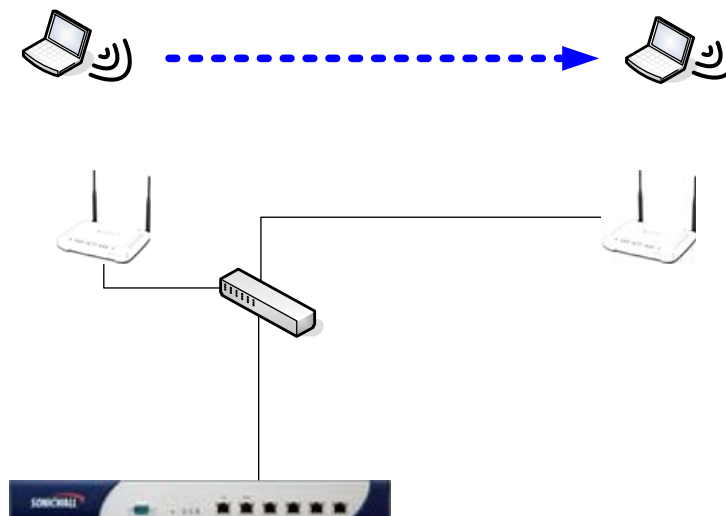
▷ SONICWALL TECH NOTE :

There are many factors that can affect the roaming process, and the effect it will have on the user application. For example, using WPA introduces additional latency as a result of the 4-way handshake that must occur during association or re-association with the new Access Point. Latency can introduce a significant amount of interruption, especially to connection-oriented or streaming/multimedia applications.

Roaming from one Access Point to another can occur across different boundaries, within the same L2 segment, across L2 segments, and across L3 segments. Generally, remaining within the same L2 segment while roaming presents the least potential for interruption, crossing L2 segments presents more, and crossing L3 segments presents the most.

Roaming Within L3 Boundaries

In configurations where a single SonicPoint or multiple SonicPoints are connected to a single interface on a SonicWALL security appliance, roaming (under most circumstances) will be seamless to the user since the client connection is terminated at the SonicWALL's interface rather than at the individual SonicPoint. Consider the following configuration:

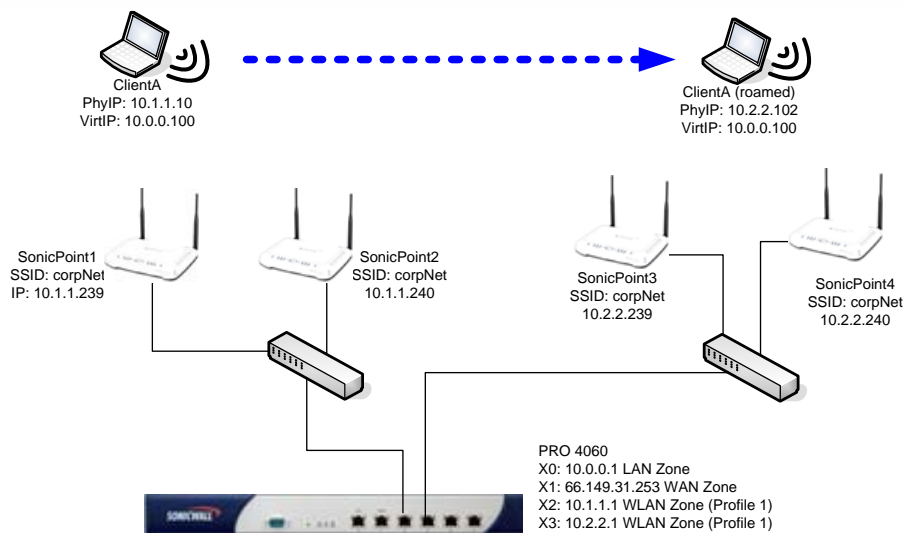


In the above configuration, the WLAN Zone has WiFiSec enforced, but the 'WLAN GroupVPN' does not have 'Use DHCP to obtain Virtual IP for this Connection' enabled. ClientA associates with SonicPoint1, and received a DHCP lease of 10.1.1.10. All wireless traffic entering SonicPoint1 traverses the X2 interface. As ClientA moves through the network, the wireless client adapter will at some point make a decision to roam to SonicPoint2. Upon doing so, the wireless client adapter will preserve the same DHCP lease (10.1.1.10) and in most cases, there should be no perceptible interruption to traffic.

Roaming Across Multiple SonicWALL Interfaces

If it becomes necessary or desirable to span a contiguous network of SonicPoints across multiple interfaces on a SonicWALL security appliance, the effects of roaming across L3 boundaries can be mitigated by using the GVC with the Virtual Adapter option:

▷ SONICWALL TECH NOTE :



The illustration above depicts a wireless client (ClientA) associated with SonicPoint1. SonicPoint1 is attached to PRO port X2 occupying address space 10.1.1.x/24. A DHCP Server is active on X2, and has provided a lease of 10.1.1.10 to ClientA. ClientA has a WiFiSec connection to the PRO, and a Virtual Adapter lease of 10.0.0.100 from the X0 (LAN) scope.

As ClientA moves from SonicPoint1 to SonicPoint2, both of which use the same SSID (corpNet), roaming occurs within the same L2 segment. When ClientA re-associates, the physical adapter IP address (10.1.1.10) will remain the same, as will the Virtual Adapter address (10.0.0.100). The GVC client will automatically re-establish the WiFiSec connection, and all but the most sensitive connection-oriented applications will continue without perceptible interruption.

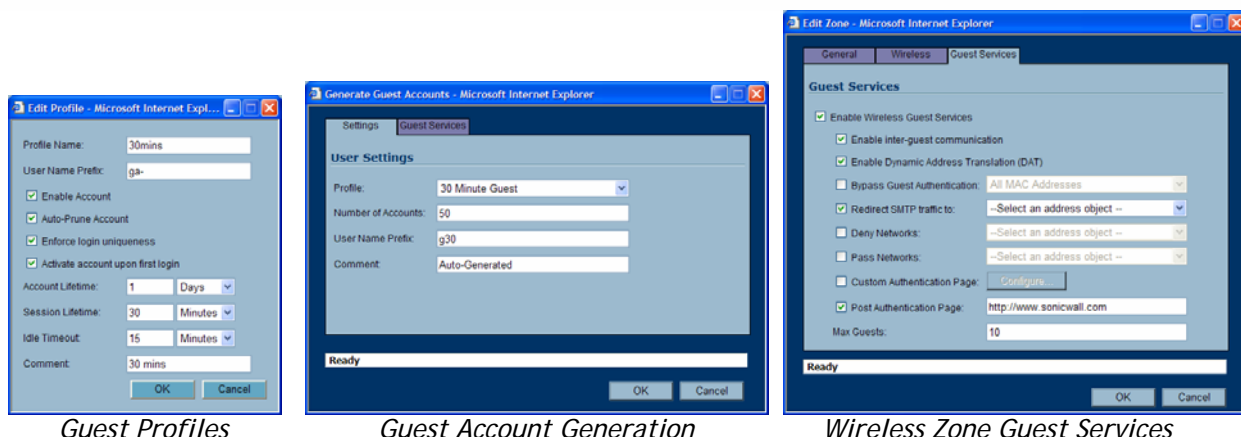
If ClientA continues to move through the distributed wireless network, roaming from SonicPoint2 to SonicPoint3, roaming will cross both L2 and L3 boundaries. When ClientA associates with SonicPoint3, the physical adapter IP address will change to a lease from the scope on the X3 interface (for example, 10.2.2.102), but the Virtual Adapter address will remain the same (10.0.0.100). Through the use of the GVC with the Virtual Adapter, the roaming process can be made significantly less interruptive.

Guest Services

Guest Services are designed to provide guest users with wireless access to public resources, such as the Internet, or a number of “walled-garden” (explicitly allowed) sites. Adding to the capabilities of WGS on the SOHO TZW, Guest Services on the SonicOS Enhanced offers:

- Profiles to allow for template based account generation
- Bulk Account generation to create multiple accounts at once
- Limited Admin access to Guest Services management pages
- Integration of Guest Services user accounts into the Local User/Group account structure

▷ SONICWALL TECH NOTE:



Guest Profiles

Guest Account Generation

Wireless Zone Guest Services

Guest Services controls on SonicOS Enhanced 2.5 will be integrated into the Zone configuration pages, and will be uniquely configurable on every Wireless Zone instance. In other words, it will be possible to provide WGS on a user created “PublicWLAN Zone” while not providing guest access on the default “WLAN Zone”, or to provide one set of Guest Services options on one Wireless Zone, and a completely different set of options on another.

Inter-guest Communications

The option to enable inter-guest communications allows for Guest Services users to communicate with each other for the purpose of peer-to-peer networking, WiFi VoIP communications, gaming, etc. Inter-guest communications controls occur at the Wireless Gateway layer, below the Firewall Access Rules, and will not manifest itself in the Access Rule table. If IP addresses are known or predictable, it will still be possible to create Access Rules to further control Guest user traffic. DAT (Dynamic Address Translation) Guest users will not be able to communicate with each other, regardless of Inter-guest Communication settings.

Dynamic Address Translation

Dynamic Address Translation allows for Guest clients to use any IP addressing scheme and DNS settings rather than requiring them to reside on a pre-scribed L3 subnet. This allows for statically addressed guests to use Guest Services without having to reconfigure their client settings.

Bypass Guest Authentication

Bypass Guest Authentication can be enabled for the “All MAC Addresses” address object, providing un-authenticated Guest Services access to all users, or MAC Addresses can be specified (individually as a group) to provide unauthenticated Internet access to certain Stations. This is useful in providing Internet access to pre-defined users, or to devices that lack the ability to authenticate (e.g. WiFi-SIP VoIP phones, or other browser-less wireless networking devices).

Customizable Authentication Pages

It is possible to define either an external URL, or text/html-based header and footer information the authentication page for users authenticating on a Wireless Zone interface

▷ SONICWALL TECH NOTE :

rather than presenting the default SonicWALL auth.html authentication page. This allows for the sort of customizability required for hotspot, business, or hospitality environments.

It is also now possible to define a post-authentication page, that is, a page to which the user will be automatically redirected after successful authentication. This can be used to present such things as usage policy information or custom portal pages.

SMTP Redirection

In a hotspot or hospitality environment, users with variously configured SMTP settings will visit, and will expect the same network experience as they have at home or at work. An obstacle to this sort of transparency is the fact that many ISP's only allow connections to their SMTP servers from source IP addresses that fall into their own ranges of IP addresses. This security mechanism, or the much more prevalent (although unfortunately not yet ubiquitous) prevention of SMTP relaying will prevent hotspot users from sending e-mail via SMTP when connecting from the IP address of the hotspot provider.

To solve this problem, SMTP Redirection intercepts and translates all outbound SMTP (TCP port 25) traffic to a server that can be defined by the hotspot operator. This server is then be used to send outbound e-mail for all hotspot visitors, regardless of their client software configurations.

Note: The potential for using this sort of arrangement for spamming must be mitigated by anti-spam software running on the mail server, or on some security (anti-spam) gateway or appliance.

MAC Filtering via MAC Address Objects

MAC filtering has long been used by wireless Access Points as a rudimentary form of security. Although easily thwarted, MAC filters still provide a fair first layer of defense in the area of wireless security. To make the application of MAC filters fit better within the framework of SonicOS Enhanced and the Distributed Wireless Architecture, MAC Address Objects and Groups will be introduced in SonicOS Enhanced 2.5, allowing for MAC Addresses, or Groups of MAC Addresses to be defined and applied to SonicPoints. MAC Filters can be applied in either an "Allow" or a "Deny" fashion, wherein Allowed MAC Filters will define the list of MAC addresses that can connect (denying all others), and Deny MAC Filters will define the list of MAC addresses that cannot connect (allowing all others). Changes to MAC Filter settings, or the MAC Filter Objects or Groups themselves will take effect immediately on all affected SonicPoints.

SonicPoint Profiles

SonicPoint Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions will include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, including SSID's, encryption settings, MAC filters, channels of operation, etc. Once defined, profiles can be applied at the Zone level in a fully flexible fashion, meaning that one Wireless Zone can use one profile, while a different Wireless Zone uses another.

▷ SONICWALL TECH NOTE:

Wireless > SonicPoints [Synchronize SonicPoints] [Apply] [Cancel] [?]

SonicPoint Provisioning Profiles

Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
<input type="checkbox"/> SonicPoint	WLAN	SSID: spA Channel: AutoChannel	SSID: spG Channel: AutoChannel	[Edit] [Delete]

[Add...] [Delete] [Delete All]

SonicPoint Settings

Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
<input type="checkbox"/> SonicPoint e0009b	X3 (WLAN)	IP: 172.16.17.239 MAC: 00:02:6f:e0:00:9b	Operational	SSID: spA Channel: AutoChannel	SSID: spG Channel: AutoChannel	<input checked="" type="checkbox"/>	[Edit] [Delete]

[Delete] [Delete All]

Note: All Operational SonicPoints are upgraded to SonicPoint Firmware Version 2.5.0.0. Download: [icon]

Status: Ready

SonicPoint Profile: 'SonicPoint' Settings

Enable SonicPoint

Name Prefix: SonicPoint

Country Code: United States

Ready [OK] [Cancel] [Help]

802.11a Radio Settings

Enable 802.11a Radio

SSID: spA

Radio Mode: 54Mbps - 802.11a

Channel: AutoChannel

ACL Enforcement: Disabled

WEP/WPA Encryption

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Key Mode: None

Default Key: Key 1

Key Entry: Alphanumeric

Key 1: []

Key 2: []

Key 3: []

Key 4: []

Ready [OK] [Cancel] [Help]

802.11g Advanced Radio Settings

Hide SSID in Beacon

Data Rate: Best

Transmit Power: Full Power

Antenna Diversity: Best

Beacon Interval (milliseconds): 100

DTIM Interval: 1

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

Maximum Client Associations: 32

Preamble Length: Long

Protection Mode: None

Protection Rate: 1 Mbps

Protection Type: CTS-only

Enable Short Slot Time

Allow Only 802.11g Clients to Connect

Ready [OK] [Cancel] [Help]

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.

Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- Via manual configuration changes - Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.

▷ SONICWALL TECH NOTE :

- Via un-provisioning - Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Automatic Provisioning (SDP & SSPP)

The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS Enhanced 2.5 and higher. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- Advertisement - SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- Discovery - SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- Configure Directive - A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.
- Configure Acknowledgement - A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- Keepalive - A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (e.g. on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

SonicPoint States

SonicPoint devices can function in and report the following states:

- **Initializing** - The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational mode.
- **Unprovisioned** - The SonicPoint has not yet received provisioning information from the managing SonicOS peer device.

▷ SONICWALL TECH NOTE :

- **Operational** - Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into an operational state, and will be ready for clients.
- **Provisioning** - If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safemode** - Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, and disables the radios. The SonicPoint must then be rebooted to enter either a Stand-alone, or some other functional state.
- **Non-Responsive** - If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware** - If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Over-Limit** - Based upon the SonicWALL security appliance, anywhere from 2 to 32 SonicPoint devices can be attached to each Wireless Zone interface. If more than the maximum number of units is detected, the over-limit devices will report an over-limit state, and will not enter an operational mode.
- **Rebooting** - After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware Update Failed** - If a firmware update fails, the SonicPoint will report the failure, and will then reboot.
- **Scanning** - When the SonicPoint first starts up, it will enter an active scanning mode to detect Access Points in its area. The scanning process takes no more than 15 seconds, and the results will be reported to the managing SonicWALL security appliance.
- **Provision Failed** - In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Disabled** - The radios on the SonicPoint have been manually disabled. Re-enabling will cause the SonicPoint to reboot into a fully operational and enabled mode.
- **Stand-alone Mode (not reported)** - If a SonicPoint device cannot find or be found by a SonicOS device to peer with, it will enter a stand-alone mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS device that is sending Discovery packets, it will leave stand-alone mode, and will enter into a managed mode. The stand-alone configuration will be retained.

Managed Mode and Stand-Alone Mode Transitions

Managed Mode requires that the SonicPoint be connected to a Wireless Interface of a SonicWALL appliance running SonicOS Enhanced 2.5 or greater. When a SonicPoint is in Managed Mode, it senses if a SonicWALL is present using the SonicWALL Discovery Protocol

▷ SONICWALL TECH NOTE :

(SDP). Immediately after a boot, if a SonicWALL is not detected, the SonicPoint will reboot after a short time interval (~5 seconds) into Stand-alone Mode. If a SonicWALL is initially detected (resulting in Managed Mode) but then becomes unavailable (e.g. it is powered off, or physically disconnected from the SonicPoint), the SonicPoint will poll at a longer interval (~6 minutes), and then revert into Stand-alone Mode.

If for any reason a SonicPoint unexpectedly reboots while in Managed Mode, it will reboot into Managed Mode, unless the unexpected reboot occurred while attempting to upload firmware; in this case it will reboot into SafeMode. This failsafe measure is achieved by setting the flash boot ROM pointer to the SafeMode image at the start of every firmware upgrade process, and setting it back to the Firmware image only after verifying that the image update completed successfully. Once entering into SafeMode via this course, if the SonicPoint is still connected to the SonicWALL, it will automatically attempt to upgrade firmware again.

Failing to sense a SonicWALL via SDP for a time interval greater than 6 minutes, a SonicPoint in Managed Mode will reboot into Stand-alone Mode. In Stand-alone mode, the SonicPoint acts like a normal off-the-shelf access point. The SDP protocol continues to run while in Stand-alone Mode, so if a PRO is ever sensed, the SonicPoint will automatically reboot into Managed Mode.

- The SonicPoint maintains separate Managed Mode and Stand-alone mode configurations so that neither conflicts with nor overwrites the other.
- When SafeMode is engaged, either manually or automatically, both Managed Mode and Stand-alone Mode configurations are restored to Factory Defaults.
- Restoring factory defaults via the Reset Switch (see 'Reset Switch' section below) only restores Factory Defaults for that mode of operation, e.g. depressing the Reset Switch for 5 seconds while in Managed mode will only reset the Managed Mode configuration, but the Stand-alone configuration will be left intact.

Event and Statistics Reporting

SonicPoint Statistics

SonicPoint Information	
Name:	SonicPoint e0009b
Mac Address:	00:02:6f:e0:00:9b
IP Address:	172.16.17.239
Interface:	X3
Zone:	WLAN
Status:	Operational

Radio Statistics		
Description	802.11a	802.11g
BSSID:	00:02:6f:00:03:7c	00:02:6f:00:03:7d
SSID:	spA	spG
Channel:	AutoChannel	AutoChannel
Connected Stations:	1	1
Associations:	2	1
Disassociations:	1	0
Reassociations:	0	0
Authentications:	2	1
Deauthentications:	2	1
Discards Packets:	0	535

Traffic Statistics				
Description	802.11a Radio (5GHz)		802.11g Radio (2.4GHz)	
	Rx	Ix	Rx	Ix
Good Packets:	21556	24314	17191	22987
Bad Packets:	8916	143	43301077	702
Good Bytes:	4852974	13470451	3231909	7178138
Management Packets:	733	769	8033	4470
Control Packets:	0	0	364	0
Data Packets:	58311	23545	17724	18819

Refresh OK

SonicPoint Statistics

Station Statistics

Station Information	
Name:	
Mac Address:	00:02:6f:00:02:a6
IP Address:	
SonicPoint:	SonicPoint e0009b
AID:	1
Status:	Connected
Connect Rate:	54 Mbps
Tx Rate:	48 Mbps
Signal Strength:	39% - Fair

Radio Statistics	
Description	Value
Radio:	802.11a Radio (5GHz)
SSID:	spA
Channel:	AutoChannel
Associations:	4
Disassociations:	1
Reassociations:	0
Authentications:	2
Deauthentications:	2
Discards Packets:	0

Traffic Statistics		
Description	Rx	Ix
Good Packets:	21772	23178
Bad Packets:	0	143
Good Bytes:	4864066	13538203
Management Packets:	4	4
Control Packets:	0	0
Data Packets:	58637	23174

Refresh OK

Station Statistics

▷ SONICWALL TECH NOTE:

On the 'Wireless > Station Status' page, each SonicPoint device will report for both radios, and for each station, the following information to its SonicOS peer:

- MAC Address - The client's (Station's) hardware address
- Station State - The state of the station. States can include:
 - None - No state information yet exists for the station
 - Authenticated - The station has successfully authenticated.
 - Associated - The station is associated.
 - Joined - The station has joined the ESSID.
 - Connected - The station is connected (joined, authenticated or associated).
 - Up - An Access Point state, indicating that the Access Point is up and running.
 - Down - An Access Point state, indicating that the Access Point is not running.
- Associations - Total number of Associations since power up.
- Dis-Associations - Total number of Dis-Associations.
- Re-Associations - Total number of Re-Associations.
- Authentications - Number of Authentications.
- De-Authentications - Number of De-Authentications.
- Good Frames Received - Total number of good frames received.
- Good Frames Transmitted - Total number of good frames transmitted.
- Error in Receive Frames - Total number of error frames received.
- Error in Transmit Frames - Total number of error frames transmitted.
- Discarded Frames - Total number of frames discarded. Discarded frames are generally a sign of network congestion.
- Total Bytes received - Total number of bytes received.
- Total Bytes Transmitted - Total number of bytes transmitted.
- Management Frames Received - Total number of Management frames received.
Management Frames include:
 - Association request
 - Association response
 - Re-association request
 - Re-association response
 - Probe request
 - Probe response
 - Beacon frame
 - ATIM message
 - Disassociation
 - Authentication
 - De-authentication
- Management Frames Transmitted - Total number of Management frames transmitted.
- Control Frames Received - Total number of Control frames received. Control frames include:
 - RTS - Request to Send
 - CTS - Clear to Send
 - ACK - Positive Acknowledgement

▷ SONICWALL TECH NOTE:

- Control Frames Transmitted - Total number of Control frames transmitted.
- Data Frames Received - Total number of Data frames received.
- Data Frames Transmitted - Total number of Data frames transmitted.

SafeMode

SonicPoint SafeMode

Your SonicPoint is now running in SafeMode.

SafeMode will allow you to view your basic SonicPoint settings and upload a new firmware image.

System Information

Product Name:	SonicPoint
Regulatory Domain:	Domestic
Serial Number:	00026FE0009B
ROM Version:	SonicROM 2.5.0.0
SafeMode Firmware Version:	SonicOS 2.5.0.6
LAN MAC Address:	00:02:6F:E0:00:9B
IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
802.11a Radio MAC (BSSID):	00:02:6F:00:03:7C
802.11g Radio MAC (BSSID):	00:02:6F:00:03:7D
SonicWall Discovery Protocol (SDP):	Enabled
SonicWall Simple Provision Protocol (SSPP):	Enabled

Firmware Management

FTP Server IP Address:


User Name:

Password:

Firmware Image Filename:

Status: Ready.

The SafeMode image provides a failsafe mechanism for the firmware upload process as performed from either the stand-alone GUI using FTP, or via automatic updates performed by a SonicOS device using SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP). In the event of firmware image corruption, the SonicPoint will automatically enter into SafeMode, the configuration (both Stand-alone and Managed) will be restored to factory defaults, and a new firmware image can be uploaded via FTP.

Note: An FTP server hosting the SonicPoint firmware image is required for this process. The SonicPoint firmware is embedded in SonicOS Enhanced version 2.5 and later, and can be retrieved from the SonicOS GUI using the download  link at bottom of the **Wireless > SonicPoints** page. After successfully uploading the new firmware image to the SonicPoint via FTP, the ROM pointer will be updated, and the SonicPoint will reboot using the new firmware image. The default IP address of the Safemode (and Stand-alone) GUI is 192.168.1.20. Safemode does not require a login, while Stand-alone mode employs a default username of 'admin' and a password of 'password'.

▷ SONICWALL TECH NOTE:

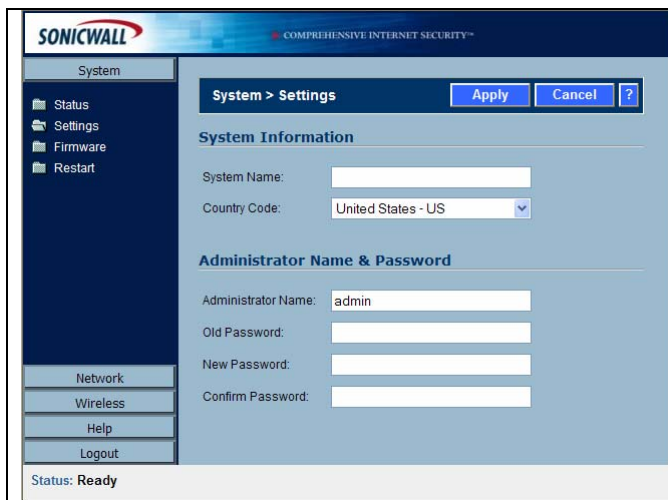
Stand-Alone Mode

The Stand-Alone mode of operation allows a SonicPoint to behave like a standard Access Point. While in Stand-Alone mode, data exiting the SonicPoint is not tagged, nor is it hauled to an aggregation point via the LAN interface. The Stand-Alone GUI is modeled after the SonicOS UI, and provides a nearly complete subset of the functionality available through Managed Mode.



System > Status

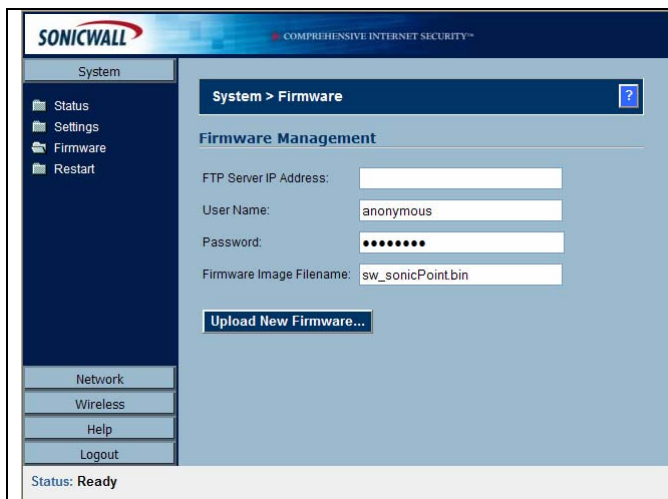
Provides a view of operating parameters on the SonicPoint, and provides quick links to the Network Interface settings.



System > Settings

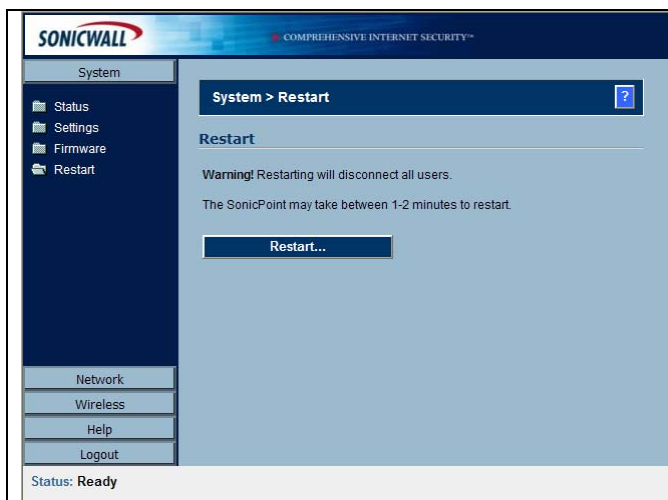
Allows for the System Name, Country Code, and administrative information to be configured.

▷ SONICWALL TECH NOTE :



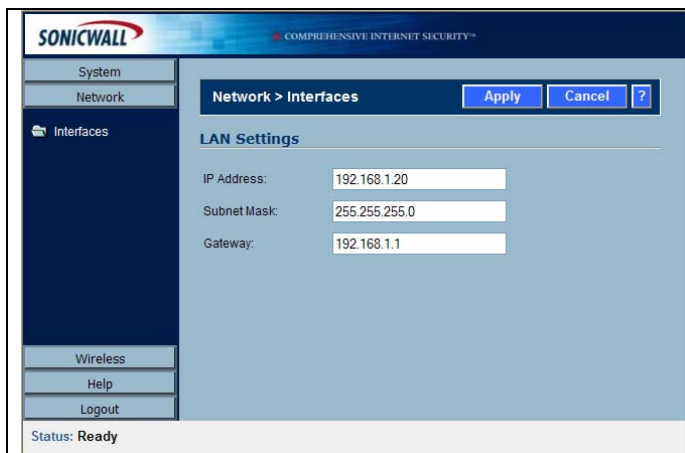
System > Firmware

Provides an interface to upload new firmware via FTP. Requires access to an external FTP server hosting a SonicPoint Firmware image. SonicPoint firmware can be downloaded from a SonicOS Enhanced 2.5 or greater device from the 'Wireless > SonicPoints' page, or from www.mysonicwall.com



System > Restart

UI based restarting of the SonicPoint.



Network > Interfaces

Configuration of LAN IP, netmask, and default gateway.

▷ SONICWALL TECH NOTE:

WLAN Radio Settings

Setting	802.11a Radio	802.11g Radio
Radio:	Enabled	Enabled
SSID:	sonicwall	sonicwall
Radio Mode:	5GHz 54 Mbps - 802.11a	2.4GHz 54 Mbps - 802.11g
Channel:	AutoChannel	AutoChannel
Authentication:	WEP - Open System	WEP - Open System
Data Rate:	Best	Best
Transmit Power:	Full Power	Full Power
Antenna Diversity:	Best	Best
Beacon Interval:	100	100
DTIM Interval:	1	1
Fragment Threshold:	2346	2346
RTS Threshold:	2346	2346
Maximum Clients:	128	128

WLAN Radio Statistics

Statistic	802.11a Radio		802.11g Radio	
	Rx	Tx	Rx	Tx
Good Frames:	0	231	0	273
Bad Frames:	142	0	92739	60
Good Bytes:	439	18411	56354	21926
Management Frames:	11	26	985	128
Control Frames:	0	0	0	0
Data Frames:	0	205	0	205

Station Status

#	MAC Address	Radio	Authenticated	Associated	Association Id
1	00:02:8f:00:02:a6	802.11a	Authenticated	Associated	1

Wireless > Status

View statistics for both radios, and associated Station status.

802.11a Radio Settings

Enable 802.11a Radio

SSID:

Radio Mode:

Channel:

WEP/WPA Encryption

Authentication Type:

WEP Key Mode:

Default Key:

Key Entry:

Key 1:

Key 2:

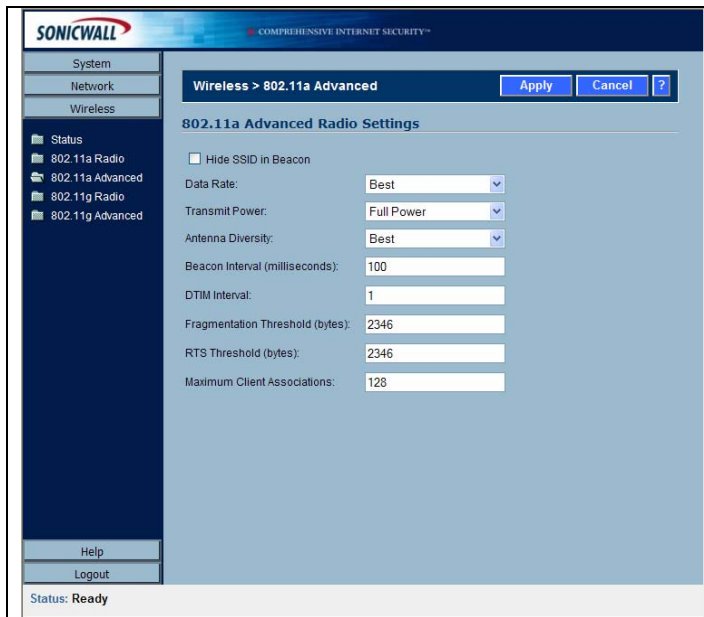
Key 3:

Key 4:

Wireless > 802.11a Radio

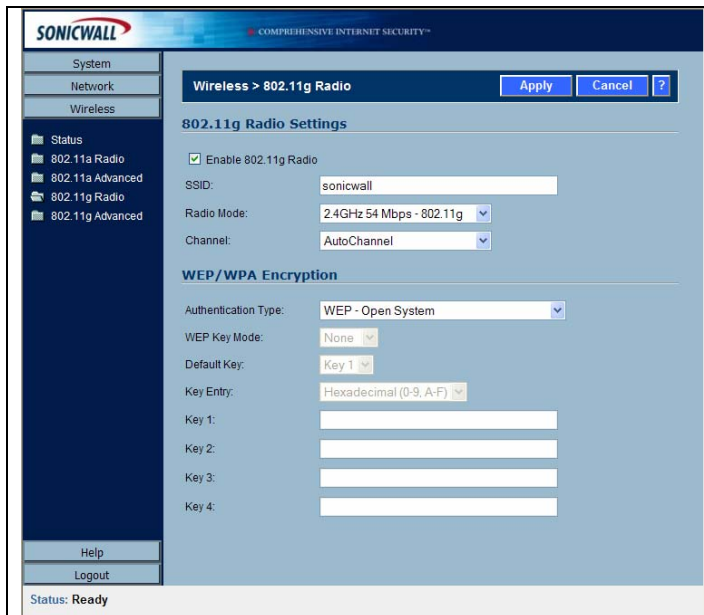
802.11a (5GHz) Radio settings

▷ SONICWALL TECH NOTE:



Wireless > 802.11a Advanced

Advanced 802.11a (5GHz) Radio settings



Wireless > 802.11g Radio

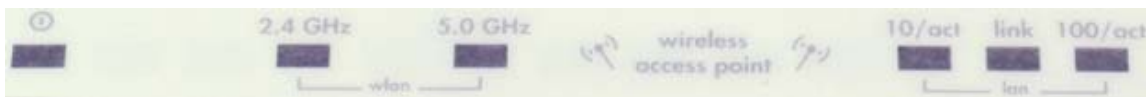
802.11g/b (2.4GHz) Radio settings

▷ SONICWALL TECH NOTE :

	<p>Wireless > 802.11g Advanced</p> <p>Advanced 802.11g/b (2.4GHz) Radio settings</p>
--	--

LEDs

A SonicPoint has the following six LEDs (from left to right):



1. **Power** - The Power LED is controlled directly by Vcc, +12.0 Volt DC power via power supply connector (power port) or 802.3af Power over Ethernet (PoE) through the LAN connector.
2. **WLAN 2.4 GHz Radio** - The 2.4 GHz Radio LED is controlled via the wireless radio and is governed by the hardware state. The LED will blink at a constant rate when ready to receive traffic, and will blink at a variable rate while transferring data with connected 802.11g/b stations.
3. **WLAN 5.0 GHz Radio** - The 5 GHz Radio LED is controlled via the wireless radio and is governed by the hardware state. The LED will blink at a constant rate when ready to receive traffic, and will blink at a variable rate while transferring data with connected 802.11a stations.
4. **LAN 10/act** - The LAN 10/act LED is controlled via the network interface and is governed by the hardware state. It will blink to indicate 10mbit LAN activity.
5. **LAN Link** - The LAN 10/act LED is controlled via the network interface and is governed by the hardware state. It illuminates to indicate physical layer connectivity.
6. **LAN 100/act** - The LAN 100/act LED is controlled via the network interface and is governed by the hardware state. It will blink to indicate 100mbit LAN activity.

Reset Switch

A SonicPoint also has a single reset switch located on the rear panel of the unit. The following table details all possible behaviors of the reset switch based upon the operating image, along with the expected response and the corresponding Power LED behavior.

▷ SONICWALL TECH NOTE :

Image	Action/State	Response	Power LED
Any	Power Off.	N/A	Off
Any	Power On.	N/A	On
ROM	Booting.	N/A	Blinking
ROM	Reset Switch Depressed.	Temporally dependent. See below.	On
ROM	Reset Switch sensed for 3 seconds, but less than 8 seconds.	Config restored to factory defaults. SonicPoint reboots.	Flash three times
ROM	Reset Switch sensed for 8 seconds or more.	Boot target set to SafeMode image. SonicPoint reboots into SafeMode.	Blink three times
ROM	Bootrom CLI.	N/A	On
SafeMode	Booting.	N/A	Blinking
SafeMode	Boot to SafeMode complete.	N/A	Blinking
Firmware	Booting.	N/A	Blinking
Firmware	Reset Switch sensed for 3 seconds, but less than 8 seconds.	Config restored to factory defaults. SonicPoint reboots.	Flash three times
Firmware	Reset Switch sensed for 8 seconds or more.	Boot target set to SafeMode image. SonicPoint reboots into SafeMode.	Blink three times
Firmware	Boot to operating Firmware complete.	Radios initialize. Device enters operational state.	On

Flash is defined as .25 seconds on followed by .25 seconds off.

Blink is defined as .5 seconds on followed by .5 seconds off.