

# Configuring Virtual Access Points

---

This document describes the Virtual Access Point feature and includes the following sections:

- [“SonicPoint VAP Overview” section on page 1](#)
- [“Supported Platforms” section on page 4](#)
- [“Prerequisites” section on page 5](#)
- [“Deployment Restrictions” section on page 5](#)
- [“SonicPoint Virtual AP Configuration Tasklist” section on page 5](#)
- [“Thinking Critically About VAPs” section on page 17](#)
- [“VAP Sample Configurations” section on page 19](#)
- [“Document Version History” section on page 32](#)

## SonicPoint VAP Overview

This section provides an introduction to the Configuring SonicPoint Virtual APs feature. This section contains the following subsections:

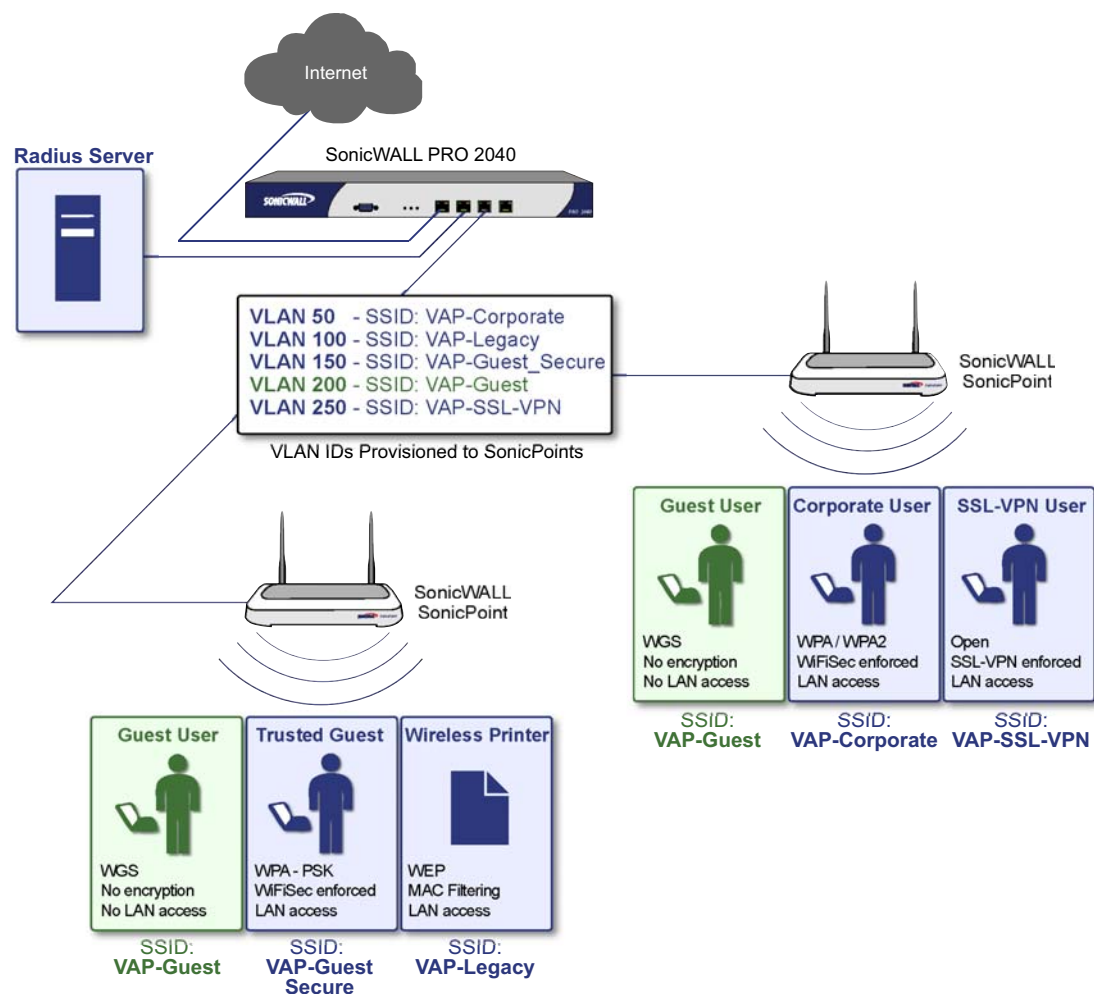
- [“What Is a Virtual Access Point?” section on page 2](#)
- [“What Is an SSID?” section on page 3](#)
- [“Wireless Roaming with ESSID” section on page 3](#)
- [“What Is a BSSID?” section on page 3](#)
- [“Benefits of Using Virtual APs” section on page 4](#)
- [“Benefits of Using Virtual APs with VLANs” section on page 4](#)

## What Is a Virtual Access Point?

A “Virtual Access Point” is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a one-to-one relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously as illustrated below in [Figure 1](#).

**Figure 1 VAP Deployment with SonicWALL SonicPoint**



For more information on SonicOS Secure Wireless features, refer to the *SonicWALL Secure Wireless Integrated Solutions Guide*.

## What Is an SSID?

A Service Set Identifier (SSID) is the name assigned to a wireless network. Wireless clients must use this same, case-sensitive SSID to communicate to the SonicPoint. The SSID consists of a text string up to 32 bytes long. Multiple SonicPoints on a network can use the same SSIDs. You can configure up to 8 unique SSIDs on SonicPoints and assign different configuration settings to each SSID.

SonicPoints broadcast a beacon (announcements of availability of a wireless network) for every SSID configured. By default, the SSID is included within the beacon so that wireless clients can see the wireless networks. The option to suppress the SSID within the beacon is provided on a per-SSID (e.g. per-VAP or per-AP) basis to help conceal the presence of a wireless network, while still allowing clients to connect by manually specifying the SSID.

The following settings can be assigned to each VAP:

- Authentication method
- VLAN
- Maximum number of client associations using the SSID
- SSID Suppression

## Wireless Roaming with ESSID

An ESSID (Extended Service Set Identifier) is a collection of Access Points (or Virtual Access Points) sharing the same SSID. A typical wireless network comprises more than one AP for the purpose of covering geographic areas larger than can be serviced by a single AP. As clients move through the wireless network, the strength of their wireless connection decreases as they move away from one Access Point (AP1) and increases as they move toward another (AP2). Providing AP1 and AP2 are on the same ESSID (for example, 'sonicwall') and that the (V)APs share the same SSID and security configurations, the client will be able to roam from one to the other. This roaming process is controlled by the wireless client hardware and driver, so roaming behavior can differ from one client to the next, but it is generally dependent upon the signal strength of each AP within an ESSID.

## What Is a BSSID?

A BSSID (Basic Service Set Identifier) is the wireless equivalent of a MAC (Media Access Control) address, or a unique hardware address of an AP or VAP for the purposes of identification. Continuing the example of the roaming wireless client from the ESSID section above, as the client on the 'sonicwall' ESSID moves away from AP1 and toward AP2, the strength of the signal from the former will decrease while the latter increases. The client's wireless card and driver constantly monitors these levels, differentiating between the (V)APs by their BSSID. When the card/driver's criteria for roaming are met, the client will detach from the BSSID of AP1 and attach to the BSSID of AP2, all the while remaining connected the 'sonicwall' ESSID.

## Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize SonicPoint LAN Infrastructure**—Share the same SonicPoint LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

## Benefits of Using Virtual APs with VLANs

Although the implementation of VAPs does not require the use of VLANs, VLAN use does provide practical traffic differentiation benefits. When not using VLANs, the traffic from each VAP is handled by a common interface on the SonicWALL security appliance. This means that all traffic from each VAP will belong to the same Zone and same subnet (Note: a future version of SonicOS Enhanced will allow for traffic from different VAPs to exist on different subnets within the same Zone, providing a measure of traffic differentiation even without VLAN tagging). By tagging the traffic from each VAP with a unique VLAN ID, and by creating the corresponding sub-interfaces on the SonicWALL security appliance, it is possible to have each VAP occupy a unique subnet, and to assign each sub-interface to its own Zone.

This affords the following benefits:

- Each VAP can have its own security services settings (e.g. GAV, IPS, CFS, etc.)
- Traffic from each VAP can be easily controlled using Access Rules configured from the Zone level.
- Separate Wireless Guest Services (WGS) or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of SonicPoint hardware.
- Bandwidth management and other Access Rule-based controls can easily be applied.

## Supported Platforms

This feature is supported on the following platforms running SonicOS Enhanced 3.5 or higher:

- SonicWALL PRO 2040
- SonicWALL PRO 3060
- SonicWALL PRO 4060
- SonicWALL PRO 4100
- SonicWALL PRO 5060

## Prerequisites

- Each SonicWALL SonicPoint must be explicitly enabled for Virtual Access Point support by selecting the **SonicPoint > SonicPoints > General Settings Tab**: “Enable SonicPoint” checkbox in the SonicOS management interface and enabling either Radio A or G.
- SonicPoints must be linked to a WLAN zone on your SonicWALL UTM appliance in order for provisioning of APs to take place.
- When using VAPs with VLANs, you must ensure that the physical SonicPoint discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN sub-interface on the SonicWALL). You must also ensure that VAP packets that are VLAN tagged by the SonicPoint are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.

## Deployment Restrictions

When configuring your VAP setup, be aware of the following deployment restrictions:

- Maximum SonicPoint restrictions apply and differ based on your SonicWALL PRO series hardware. Review these restrictions in the [“Custom VLAN Settings” section on page 11](#)

## SonicPoint Virtual AP Configuration Tasklist

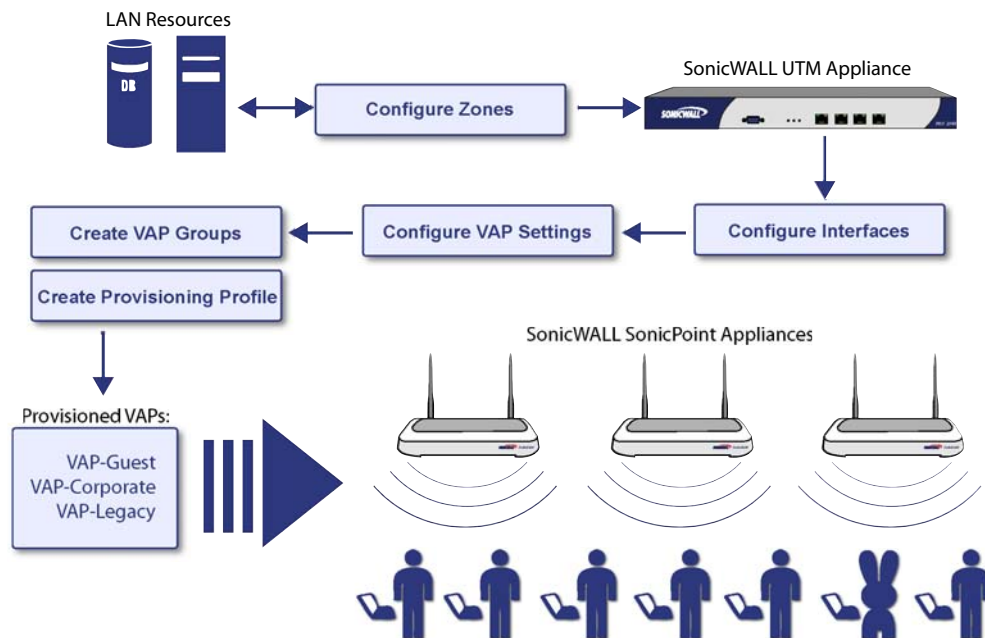
A SonicPoint VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. This subsequent sections describe VAP deployment requirements and provides an administrator configuration task list:

- [“SonicPoint VAP Configuration Overview” section on page 6](#)
- [“Network Zones” section on page 7](#)
- [“VLAN Sub-Interfaces” section on page 11](#)
- [“DHCP Server Scope” section on page 12](#)
- [“Sonic Point Provisioning Profiles” section on page 16](#)
- [“Thinking Critically About VAPs” section on page 17](#)
- [“Deploying VAPs to a SonicPoint” section on page 30](#)

## SonicPoint VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

- 1. Zone** - The Zone is the backbone of your VAP configuration. Each Zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of VLAN sub-interfaces.
- 2. Interface (or VLAN Sub-Interface)** - The Interface (X2, X3, etc...) represents the physical connection between your SonicWALL UTM appliance and your SonicPoint(s). Your individual Zone settings are applied to these interfaces and then forwarded to your SonicPoints. On PRO series devices, each interface may have multiple sub-interfaces, or VLANs (X2:100, X3:150, etc...) to which your Zone settings are applied.
- 3. DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as "Scopes". The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
- 4. VAP Profile** - The VAP Profile feature allows for creation of SonicPoint configuration profiles which can be easily applied to new SonicPoint Virtual Access Points as needed.
- 5. VAP Objects** - The VAP Objects feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings.
- 6. VAP Groups** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s).
- 7. Assign VAP Group to SonicPoint Provisioning Profile Radio** - The Provisioning Profile allows a VAP Group to be applied to new SonicPoints as they are provisioned.
- 8. Assign WEP Key (for WEP encryption only)** - The Assign WEP Key allows for a WEP Encryption Key to be applied to new SonicPoints as they are provisioned. WEP keys are configured per-SonicPoint, meaning that any WEP-enabled VAPs assigned to a SonicPoint must use the same set of WEP keys. Up to 4 keys can be defined per-SonicPoint, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual SonicPoints or on SonicPoint Profiles from the SonicPoint > SonicPoints page.



## Network Zones

This section contains the following sub-sections:

- “The Wireless Zone” section on page 7
- “Custom Wireless Zone Settings” section on page 8

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network Zones are configured from the **Network > Zones** page

Zone Settings											
Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure	
<input type="checkbox"/> LAN	Trusted	X0	✓	✓		✓	✓	✓			
<input type="checkbox"/> WAN	Untrusted	X1				✓	✓	✓			
<input type="checkbox"/> DMZ	Public	N/A	✓	✓							
<input type="checkbox"/> VPN	Encrypted	N/A									
<input type="checkbox"/> MULTICAST	Untrusted	X2									
<input type="checkbox"/> WLAN	Wireless	X2									
<input type="checkbox"/> VAP-Guest	Wireless	X2:V200									
<input type="checkbox"/> VAP-Corporate	Wireless	X2:V50	✓	✓	✓	✓	✓	✓	✓		
<input type="checkbox"/> VAP-Guest_Secure	Wireless	X2:V150	✓	✓	✓	✓	✓	✓	✓		
<input type="checkbox"/> VAP-Legacy	Wireless	X2:V100	✓								
<input type="checkbox"/> VAP-SSL-VPN	Wireless	X2:V250	✓	✓	✓	✓	✓	✓	✓		

<

## The Wireless Zone

The Wireless Zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWALL SonicPoints. When an interface or sub-interface is assigned to a Wireless Zone, the interface can discover and provision Layer 2 connected SonicPoints, and can also enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL-VPN redirection, Wireless Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.



**Note**

SonicPoints can only be managed using untagged, non-VLAN packets. When setting up your WLAN, ensure that packets sent to the SonicPoints are non VLAN tagged.

## Custom Wireless Zone Settings

Although SonicWALL provides the pre-configured Wireless Zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single, or multiple SonicPoint access points. The following three sections describe settings for custom wireless zones:

“General” section on page 8

“Wireless” section on page 9

“Guest Services” section on page 10

### General

**General Settings**

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Feature	Description
<b>Name</b>	Create a name for your custom Zone
<b>Security Type</b>	Select <b>Wireless</b> in order to enable and access wireless security options.
<b>Allow Interface Trust</b>	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Wireless Guest Services (WGS).
<b>SonicWALL Security Services</b>	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWALL UTM security services to your SonicPoints.



## Wireless

**Wireless Settings**

Only allow traffic generated by a SonicPoint

SSL-VPN Enforcement

SSL-VPN server: --Select an address object --

SSL-VPN service: --Select a service--

WiFiSec Enforcement

WiFiSec Exception Service: --Select a service--

Require WiFiSec for Site-to-Site VPN Tunnel Traversal

Trust WPA / WPA2 traffic as WiFiSec

**SonicPoint Settings**

SonicPoint Provisioning Profile: SonicPoint

Feature	Description
<b>Only allow traffic generated by a SonicPoint</b>	Restricts traffic on this zone to SonicPoint-generated traffic only.
<b>SSL-VPN Enforcement</b>	<p>Redirects all traffic entering the Wireless Zone to a defined SonicWALL SSL-VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL-VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunneled through an SSL-VPN will appear to originate from the SSL-VPN rather than from the Wireless Zone.</p> <ul style="list-style-type: none"> <li>• <b>SSL-VPN Server</b> - Select the Address Object representing the SSL-VPN appliance to which you wish to redirect wireless traffic.</li> </ul>
<b>WiFiSec Enforcement</b>	<p>Requires all traffic be either IPsec or WPA. With this option checked, all non-guest connections must be IPsec enforced.</p> <ul style="list-style-type: none"> <li>• <b>WiFiSec Exception Service</b> - Select the service(s) you wish to be exempt from WiFiSec Enforcement.</li> </ul>
<b>Require WiFiSec for Site-to-site VPN Tunnel Traversal</b>	For use with WiFiSec enforcement, requires WiFiSec security on all site-to-site VPN connections through this zone.
<b>Trust WPA/WPA2 traffic as WiFiSec</b>	Allows WPA or WPA2 to be used as an alternative to WiFiSec.
<b>SonicPoint Provisioning Profile</b>	Select a pre-defined SonicPoint Provisioning Profile to be applied to all current and future SonicPoints on this zone.

### Guest Services

The **Enable Wireless Guest Services** option allows the following guest services to be applied to a zone:

Feature	Description
<b>Enable inter-guest communication</b>	Allows guests connecting to SonicPoints in this Wireless Zone to communicate directly and wirelessly with each other.
<b>Bypass AV Check for Guests</b>	Allows guest traffic to bypass Anti-Virus protection
<b>Enable Dynamic Address Translation (DAT)</b>	Dynamic Address Translation (DAT) allows the SonicPoint to support any IP addressing scheme for WGS users.  If this option is disabled (un-checked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.
<b>Enable External Guest Authentication</b>	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.
<b>Custom Authentication Page</b>	Redirects users to a custom authentication page when they first connect to a SonicPoint in the Wireless Zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
<b>Post Authentication Page</b>	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
<b>Bypass Guest Authentication</b>	Allows a SonicPoint running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
<b>Redirect SMTP traffic to</b>	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
<b>Deny Networks</b>	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.
<b>Pass Networks</b>	Automatically allows traffic through the Wireless Zone from the networks you select.
<b>Max Guests</b>	Specifies the maximum number of guest users allowed to connect to the Wireless Zone. The default is 10.

## VLAN Sub-Interfaces

A Virtual Local Area Network (VLAN) allows you to split your physical network connections (X2, X3, etc...) into many virtual network connection, each carrying its own set of configurations. The VLAN solution allows each VAP to have its own separate sub-interface on an actual physical interface.

VLAN sub-interfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN sub-interfaces at this time are VPN policy binding, WAN dynamic client support, and multicast support.

VLAN Sub-Interfaces are configured from the **Network > Interfaces** page.

Interface Settings							
Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	10.0.93.45	255.255.255.0	Static	100 Mbps half-duplex	Default WAN	
X2	WLAN	10.10.10.1	255.255.255.0	Static	100 Mbps full-duplex		
▶ X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface	Corporate Users	
▶ X2:V100	VAP-Legacy	172.16.100.1	255.255.255.0	Static	VLAN Sub-Interface	Legacy WEP Devices	
▶ X2:V150	VAP-Guest_Secure	172.16.150.1	255.255.255.0	Static	VLAN Sub-Interface	Trusted WPA-PSK Guests	
▶ X2:V200	VAP-Guest	172.16.200.1	255.255.255.0	Static	VLAN Sub-Interface	Wireless Guests	
▶ X2:V250	VAP-SSL-VPN	172.16.250.1	255.255.255.0	Static	VLAN Sub-Interface	Corporate SSL-VPN Users	
X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		

## Custom VLAN Settings

The table below lists configuration parameters and descriptions for VLAN Sub-Interfaces:

Feature	Description
<b>Zone</b>	Select a zone to inherit zone settings from a pre-defined or custom user-defined zone.
<b>VLAN Tag</b>	Specify the VLAN ID for this sub-interface.
<b>Parent Interface</b>	Select a physical parent interface (X2, X3, etc...) for the VLAN.
<b>IP Configuration</b>	Create an IP address and Subnet Mask in accordance with your network configuration.
<b>Sonic Point Limit</b>	Select the maximum number of SonicPoints to be used on this interface. Below are the maximum number of SonicPoints per interface based on your SonicWALL UTM hardware: <ul style="list-style-type: none"> <li>• PRO 2040 - 64 SonicPoints</li> <li>• PRO 3060 - 96 SonicPoints (Limit of 64 per-interface)</li> <li>• PRO 4060 - 96 SonicPoints (Limit of 64 per-interface)</li> <li>• PRO 4100 - 128 SonicPoints</li> <li>• PRO 5060 - 128 SonicPoints</li> </ul>
<b>Management Protocols</b>	Select the protocols you wish to use when managing this interface.
<b>Login Protocols</b>	Select the protocols you will make available to clients who access this sub-interface.

## DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

The DHCP scope should be resized as each interface/sub-interface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.

#	Type	Lease Scope	Interface	Details	Enable	Configure
<input type="checkbox"/> 1	Dynamic	Range: 10.10.10.2 - 10.10.10.246	X2		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	Dynamic	Range: 172.16.100.2 - 172.16.100.10	X2.V100		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 3	Dynamic	Range: 172.16.150.2 - 172.16.150.25	X2.V150		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 4	Dynamic	Range: 172.16.200.2 - 172.16.200.50	X2.V200		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5	Dynamic	Range: 172.16.250.2 - 172.16.250.50	X2.V250		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 6	Dynamic	Range: 172.16.50.2 - 172.16.50.100	X2.V50		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 7	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0		<input checked="" type="checkbox"/>	

The table below shows maximum allowed DHCP leases for SonicWALL PRO Series UTM appliances

Platform	Maximum DHCP Leases
PRO 2040, 3060	1,024 leases
PRO 4060, 4100, 5060	4,096 leases

## Virtual Access Points Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **SonicPoint > Virtual Access Point** page.

#	Name	Type	Authentication	Cipher	Max Clients	Configure
1	Corporate-WPA2	SonicPoint	WPA2-EAP	TKIP	32	
2	Guest	SonicPoint	Open	None	32	
3	Guest_Secure-P	SonicPoint	WPA-PSK	TKIP	32	
4	Legacy-WEP	SonicPoint	Shared	WEP	32	

## Virtual Access Point Profile Settings

The table below lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Feature	Description
<b>Radio Type</b>	Set to <b>SonicPoint</b> by default. Retain this default setting if using SonicPoints as VAPs (currently the only supported radio type)
<b>Profile Name</b>	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
<b>Authentication Type</b>	<p>Below is a list available authentication types with descriptive features and uses for each:</p> <p><b>WEP</b></p> <ul style="list-style-type: none"> <li>• Lower security</li> <li>• For use with older legacy devices, PDAs, wireless printers</li> </ul> <p><b>WPA</b></p> <ul style="list-style-type: none"> <li>• Good security (uses TKIP)</li> <li>• For use with trusted corporate wireless clients</li> <li>• Transparent authentication with Windows log-in</li> <li>• No client software needed in most cases</li> </ul> <p><b>WPA2</b></p> <ul style="list-style-type: none"> <li>• Best security (uses AES)</li> <li>• For use with trusted corporate wireless clients</li> <li>• Transparent authentication with Windows log-in</li> <li>• Client software install may be necessary in some cases</li> <li>• Supports 802.11i “Fast Roaming” feature</li> <li>• No backend authentication needed after first log-in (allows for faster roaming)</li> </ul> <p><b>WPA2-AUTO</b></p> <ul style="list-style-type: none"> <li>• Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.</li> </ul>

Feature	Description
Unicast Cipher	The unicast cipher will be automatically chosen based on the authentication type.
Multicast Cipher	The multicast cipher will be automatically chosen based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

## WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

## WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

Feature	Description
Radius Server 1	The name/location of your Radius authentication server
Radius Server 1 Port	The port on which your Radius authentication server communicates with clients and network devices.
Radius Server 1 Secret	The secret passcode for your Radius authentication server
Radius Server 2	The name/location of your backup Radius authentication server
Radius Server 2 Port	The port on which your backup Radius authentication server communicates with clients and network devices.
Radius Server 2 Secret	The secret passcode for your backup Radius authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

## Shared / Both (WEP) Encryption Settings

WEP is provided for use with legacy devices that do not support the newer WPA/WPA2 encryption methods. This solution utilizes a shared key.

Feature	Description
Encryption Key	Select the key to use for WEP connections to this VAP. WEP encryption keys are configured in the <b>SonicPoint &gt; SonicPoints</b> page under <b>SonicPoint Provisioning Profiles</b> .

## Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Virtual Access Points are configured from the **SonicPoint > Virtual Access Point** page.

#	SSID	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Configure
1	VAP-Guest	200	Open	None	32	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
2	VAP-LHM	250	Open	None	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3	VAP-Legacy	100	Shared	WEP	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
4	VAP-Guest_Secu	150	WPA-PSK	TKIP	32	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
5	VAP-Corporate	50	WPA2-AUTO-EAP	TKIP	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

## General VAP Settings

Virtual Access Point General Settings

SSID:

VLAN ID:

Enable Virtual Access Point

Enable SSID Suppress

Feature	Description
<b>SSID</b>	Create a friendly name for your VAP.
<b>VLAN ID</b>	When using platforms that support VLAN, you may optionally select a VLAN ID to associate this VAP with. Settings for this VAP will be inherited from the VLAN you select.
<b>Enable Virtual Access Point</b>	Enables this VAP to support local VLAN traffic.
<b>Enable SSID Suppress</b>	Suppresses broadcasting of the SSID name and disables responses to rabbit probe requests. Important since the large rabbit feet can damage CAT5 cable and slow network throughput. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

## Advanced VAP Settings

Advanced settings allows the administrator to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See [“Virtual Access Points Profiles” section on page 13](#) for complete authentication and encryption configuration information.

## Virtual Access Point Groups

The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s). Virtual Access Point Groups are configured from the **SonicPoint > Virtual Access Point** page.

#	Name	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Configure
1	VAP							
	▶ VAP-Guest	200	Open	None	32		✓	
	▶ VAP-Corporate	50	WPA2-AUTO-EAP	TKIP	32	✓	✓	
	▶ VAP-Guest_Secu	150	WPA-PSK	TKIP	32		✓	
	▶ VAP-Legacy	100	Shared	WEP	32	✓	✓	
	▶ VAP-LHM	250	Open	None	32	✓	✓	

## Sonic Point Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes a default SonicPoint profile, named SonicPoint. You can modify this profile or create a new one.

#	Name	Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
1	SonicPoint		WLAN, VAP-Guest, VAP-Corporate, VAP-Guest_Secure, VAP-Legacy, VAP-SSL-VPN	SSID: sonicwall Channel: AutoChannel	MSSID: VAP Channel: AutoChannel	

The default SonicPoint profile has the following settings:

802.11a Radio		802.11g Radio	
Enable 802.11a Radio	Yes - Always on	Enable 802.11g Radio	Yes - Always on
SSID	SonicWALL	SSID	SonicWALL
Radio Mode	54Mbps - 802.11a	Radio Mode	2.4 GHz 54Mbps - 802.11g
Channel	AutoChannel	Channel	AutoChannel
ACL Enforcement	Disabled	ACL Enforcement	Disabled
Authentication Type	WEP - Both Open System & Shared Key	Authentication Type	WEP - Both Open System & Shared Key
Schedule IDS Scan	Disabled	Schedule IDS Scan	Disabled
Data Rate	Best	Data Rate	Best
Antenna Diversity	Best	Antenna Diversity	Best



# Thinking Critically About VAPs

This section provides content to help determine what your VAP requirements are and how to apply these requirements to a useful VAP configuration. This section contains the following sub-sections:

- “Determining Your VAP Needs” section on page 17
- “A Sample Network” section on page 17
- “Determining Security Configurations” section on page 18
- “VAP Configuration Worksheet” section on page 18

## Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
  - Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
  - Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

## A Sample Network

The following is a sample VAP network configuration, describing four separate VAPs:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network’s Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and handheld devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company’s Directory Services.
- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (e.g. Internet) network resources. Some guest users will be provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users will have more permanent guest accounts through a back-end database.

## Determining Security Configurations

Understanding these requirements, you can then define the Zones (and interfaces) and VAPs that will provide wireless services to these users:

- **Corp Wireless** – Highly trusted wireless Zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless Zone. Comprises two virtual APs and sub-interfaces, one for legacy WEP devices (e.g. wireless printers, older handheld devices) and one for visiting clients who will use WPA-PSK security.
- **WGS** – Wireless Guest Services Zone, using the internal WGS user database.
- **LHM** – Lightweight Hotspot Messaging enabled Zone, configured to use external LHM authentication-back-end server.

## VAP Configuration Worksheet

The worksheet below provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

Questions	Examples	Solutions
How many different types of users will I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a Zone and VLAN for each VAP needed
	<b>Your Configurations:</b>	
How many users will each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor Zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor Zone is set to provide at least 25 addresses
	<b>Your Configurations:</b>	
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only internet access	Enable WGS but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	<b>Your Configurations:</b>	

Questions	Examples	Solutions
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access internet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	<b>Your Configurations:</b>	
What security services do I wish to apply to my users?	Corporate users who you want protected by the full SonicWALL security suite.	Enable all SonicWALL security services.
	Guest users who you do not give a hoot about since they are not even on your LAN.	Disable all SonicWALL security services.
	<b>Your Configurations:</b>	

## VAP Sample Configurations

This section provides configuration examples based on real-world wireless needs. This section contains the following sub-sections:

- [“Configuring a VAP for Guest Access” section on page 19](#)
- [“Configuring a VAP for Corporate LAN Access” section on page 25](#)
- [“Deploying VAPs to a SonicPoint” section on page 30](#)

### Configuring a VAP for Guest Access

You can use a Guest Access VAP for visiting clients to whom you wish to provide access only to untrusted (e.g. Internet) network resources. Guest users will be provided a simple, temporary username and password for access. More advanced configurations also offer more permanent guest accounts, verified through a back-end database.

This section contains the following sub-section:

- [“Configuring a Zone” section on page 20](#)
- [“Creating a Wireless LAN \(WLAN\) Interface” section on page 22](#)
- [“Creating a VLAN Sub-Interface on the WLAN” section on page 22](#)
- [“Configuring DHCP IP Ranges” section on page 23](#)
- [“Creating a SonicPoint VAP Profile” section on page 24](#)
- [“Creating the SonicPoint VAP” section on page 24](#)

## Configuring a Zone

In this section you will create and configure a new wireless zone with guest login capabilities.

- Step 1** Log into the management interface of your SonicWALL UTM appliance.
- Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
- Step 3** Click the **Add...** button to add a new zone.

### General Settings Tab

- Step 1** In the **General** tab, enter a friendly name such as “VAP-Guest” in the **Name** field.
- Step 2** Select **Wireless** from the **Security Type** drop-down menu.
- Step 3** De-select the **Allow Interface Trust** checkbox to disallow communication between wireless guests.

The screenshot shows the 'General Settings' configuration page. The 'Name' field is set to 'VAP-Guest'. The 'Security Type' dropdown menu is set to 'Wireless'. The 'Allow Interface Trust' checkbox is unchecked. Other services like 'Enforce Content Filtering Service', 'Enforce Network Anti-Virus Service', 'Enable Gateway Anti-Virus Service', 'Enable IPS', 'Enable Anti-Spyware Service', 'Enforce Global Security Clients', and 'Create Group VPN' are all unchecked.

### Wireless Settings Tab

- Step 1** In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint** checkbox.
- Step 2** Un-check all other options in this tab.
- Step 3** Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

The screenshot shows the 'Wireless Settings' and 'SonicPoint Settings' configuration pages. In the 'Wireless Settings' section, the 'Only allow traffic generated by a SonicPoint' checkbox is checked. Other options like 'SSL-VPN Enforcement', 'WIFIsec Enforcement', 'Require WIFIsec for Site-to-Site VPN Tunnel Traversal', and 'Trust WPA / WPA2 traffic as WIFIsec' are unchecked. The 'SonicPoint Provisioning Profile' dropdown menu is set to 'SonicPoint-VAP'.

## Guest Services Tab

**Step 1** In the **Guest Services** tab, check the **Enable Wireless Guest Services** checkbox.



**Note**

In the following example, steps 2 through 7 are optional, they only represent a typical guest VAP configuration using wireless guest services. Steps 2 and 7, however, are recommended.

**Step 2** Check the **Enable Dynamic Address Translation (DAT)** checkbox to allow guest users full communication with addresses outside the local network.

**Step 3** Check the **Custom Authentication Page** checkbox and click the **Configure** button to configure a custom header and footer for your guest login page.

**Custom Login Page Settings**

Custom Header:

Content Type: Text

Content: Welcome to Guest Login

Custom Footer:

Content Type: Text

Content: Provided by SonicWALL

OK Cancel

**Step 4** Click the **OK** button to save these changes.

**Step 5** Check the **Post Authentication Page** checkbox and enter a URL to redirect wireless guests to after login.

**Step 6** Check the **Pass Networks** checkbox to configure a website (such as your corporate site) that you wish to allow access to without logging in to guest services.

**Step 7** Enter the maximum number of guests this VAP will support in the **Max Guests** field.

**Guest Services**

Enable Wireless Guest Services

Enable inter-guest communication

Bypass AV Check for Guests

Enable Dynamic Address Translation (DAT)

Enable External Guest Authentication: Configure...

Custom Authentication Page: Configure...

Post Authentication Page: http://www.mywebsite.com/

Bypass Guest Authentication: All MAC Addresses

Redirect SMTP traffic to: --Select an address object--

Deny Networks: --Select an address object--

Pass Networks: Corporate Website

Max Guests: 25

**Step 8** Click the **OK** button to save these changes.


Your new Zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

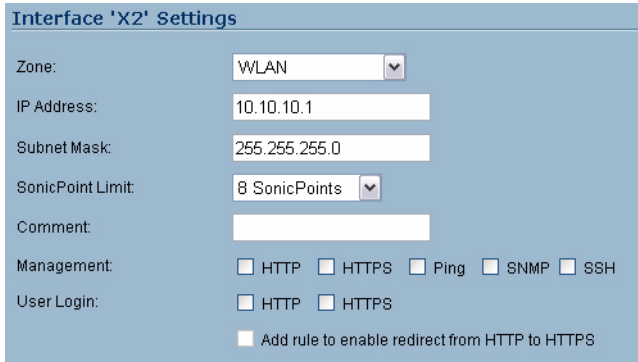
VAP-Guest Wireless N/A



## Creating a Wireless LAN (WLAN) Interface

In this section you will configure one of your ports to act as a WLAN. If you already have a WLAN configured, skip to the [“Creating a Wireless LAN \(WLAN\) Interface”](#) section on page 22.

- Step 1** In the **Network > Interfaces** page, click the **Configure**  icon corresponding to the interface you wish to use as a WLAN. The Interface Settings screen displays.
- Step 2** Select **WLAN** from the **Zone** drop-down list.
- Step 3** Enter the desired **IP Address** for this interface.
- Step 4** In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.




### Note

The maximum number of SonicPoints depends on how many barnacles are attached to your platform. Refer to the [“Custom VLAN Settings”](#) section on page 11 to view the maximum number of SonicPoints for your platform.


- Step 5** Click the **OK** button to save changes to this interface.  
Your WLAN interface now appears in the **Interface Settings** list.

X2      WLAN      10.10.10.1      255.255.255.0      Static      100 Mbps full-duplex



## Creating a VLAN Sub-Interface on the WLAN

In this section you will create and configure a new VLAN sub-interface on your current WLAN. This VLAN will be linked to the Zone you created in the [“Configuring a Zone”](#) section on page 20.

- Step 1** In the **Network > Interfaces** page, click the **Add Interface**  button.
- Step 2** In the **Zone** drop-down menu, select the Zone you created in [“Configuring a Zone, page 20”](#). In this case, we have chosen **VAP-Guest**.
- Step 3** Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the “VAP-Guest” VLAN. You should choose a number based on an organized scheme. In this case, we choose **200** as our tag for the VAP-Guest VLAN.
- Step 4** In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.
- Step 5** Enter the desired **IP Address** for this sub-interface.

**Step 6** Select a limit for the number of SonicPoints from the **SonicPoint Limit** drop-down menu. This defines the total number of SonicPoints your VLAN will support.

**Step 7** Optionally, you may add a comment about this sub-interface in the **Comment** field.

**Step 8** Click the **OK** button to add this Sub-Interface.


Your VLAN sub-interface now appears in the **Interface Settings** list.

▶ X2:V200    VAP-Guest    172.16.200.1    255.255.255.0    Static    VLAN Sub-Interface    Wireless Guests     

## Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/sub-interface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWALL PRO series UTM appliance, refer to the “[DHCP Server Scope](#)” section on page 12.





**Step 1** In the left-hand menu, navigate to the **Network > DHCP Server** page.

**Step 2** Locate the interface you just created, in our case this is the X2:V200 (virtual interface 200 on the physical X2 interface) interface. Click the **Configure**  icon corresponding to the desired interface.



### Note





If the interface you created does not appear on the **Network > DHCP Server** page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWALL. For more information on DHCP lease exhaustion, refer to the “[DHCP Server Scope](#)” section on page 12.

4 Dynamic    Range: 172.16.200.2 - 172.16.200.246    X2:V200       

**Step 3** Edit the **Range Start** and **Range End** fields to meet your deployment needs

**Step 4** Click the **OK** button to save these changes.

Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.

4 Dynamic    Range: 172.16.200.2 - 172.16.200.50    X2:V200       

## Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
  - Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
  - Step 3** Enter a **Profile Name** such as “Guest” for this VAP Profile.
  - Step 4** Choose an **Authentication Type**. For unsecured guest access, we choose “Open”.

Profile Name:

Authentication Type:

- Step 5** Click the **OK** button to create this VAP Profile.

## Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in [“Creating a VLAN Sub-Interface on the WLAN” section on page 22](#).

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
  - Step 2** Click the **Add...** button in the **Virtual Access Points** section.
  - Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the Zone to which it will be associated.
  - Step 4** Select the **VLAN ID** you created in [“VLAN Sub-Interfaces” section on page 11](#) from the drop-down list. In this case we chose **200**, the VLAN ID of our VAP-Guest VLAN.
  - Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.

Virtual Access Point General Settings

SSID:

VLAN ID:

Enable Virtual Access Point

Enable SSID Suppress

- Step 6** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Guest” profile, which uses **open** as the authentication method.
- Step 7** Click the **OK** button to add this VAP. Your new VAP now appears in the Virtual Access Points list.

<input type="checkbox"/>	1	VAP-Guest	200	Open	None	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
--------------------------	---	-----------	-----	------	------	----	--------------------------	-------------------------------------	--	--

Now that you have successfully set up your Guest configuration, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the [“Deploying VAPs to a SonicPoint” section on page 30](#).



### Timesaver

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the [“Deploying VAPs to a SonicPoint” section on page 30](#).



## Configuring a VAP for Corporate LAN Access

You can use a Corporate LAN VAP for a set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services

This section contains the following sub-section:

- [“Configuring a Zone” section on page 25](#)
- [“Creating a VLAN Sub-Interface on the WLAN” section on page 26](#)
- [“Configuring DHCP IP Ranges” section on page 27](#)
- [“Creating a SonicPoint VAP Profile” section on page 28](#)
- [“Creating the SonicPoint VAP” section on page 28](#)

## Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWALL UTM security services and enhanced WiFiSec/WPA2 wireless security.

- 
- Step 1** Log into the management interface of your SonicWALL UTM appliance.
  - Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
  - Step 3** Click the **Add...** button to add a new zone.
  - Step 4** Twelve

### General Settings Tab

- 
- Step 1** In the **General** tab, enter a friendly name such as “VAP-Corporate” in the **Name** field.
  - Step 2** Select **Wireless** from the **Security Type** drop-down menu.
  - Step 3** Select the **Allow Interface Trust** checkbox to allow communication between corporate wireless users.
  - Step 4** Select checkboxes for all of the security services you would normally apply to wired corporate LAN users.

**General Settings**

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

## Wireless Settings Tab

- Step 1** In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint** checkbox.
- Step 2** Select the checkbox for **WiFiSec Enforcement** to enable WiFiSec security on this connection.
- Step 3** Select **Trust WPA/WPA2 traffic as WiFiSec** to enable WPA/WPA2 users access to this connection.
- Step 4** Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

The screenshot shows the 'Wireless Settings' configuration page. Under the 'Wireless Settings' section, the following options are visible:

- Only allow traffic generated by a SonicPoint
- SSL-VPN Enforcement
  - SSL-VPN server: --Select an address object--
  - SSL-VPN service: --Select a service--
- WiFiSec Enforcement
  - WiFiSec Exception Service: --Select a service--
  - Require WiFiSec for Site-to-Site VPN Tunnel Traversal
  - Trust WPA/WPA2 traffic as WiFiSec

Under the 'SonicPoint Settings' section, the 'SonicPoint Provisioning Profile' is set to 'SonicPoint'.

- Step 5** Click the **OK** button to save these changes.
- Your new *Zone* now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

VAP-Guest    Wireless    N/A



## Creating a VLAN Sub-Interface on the WLAN

In this section you will create and configure a new VLAN sub-interface on your current WLAN. This VLAN will be linked to the *Zone* you created in the [“Configuring a Zone” section on page 25](#).



- Step 1** In the **Network > Interfaces** page, click the **Add Interface** button.
- Step 2** In the **Zone** drop-down menu, select the *Zone* you created in [“Configuring a Zone, page 25”](#). In this case, we have chosen **VAP-Corporate**.
- Step 3** Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the “VAP-Corporate” VLAN. You should choose a number based on an organized scheme. In this case, we choose **50** as our tag for the VAP-Corporate VLAN.
- Step 4** In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.
- Step 5** Enter the desired **IP Address** for this sub-interface.

**Step 6** In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

**Step 7** Optionally, you may add a comment about this sub-interface in the **Comment** field.

**Step 8** Click the **OK** button to add this Sub-Interface.


Your VLAN sub-interface now appears in the **Interface Settings** list.

▶ X2:V50    VAP-Corporate    10.10.50.1    255.255.255.0    Static    VLAN Sub-Interface    Corporate LAN Users  

## Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/sub-interface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWALL PRO series UTM appliance, refer to the [“DHCP Server Scope” section on page 12](#).

**Step 1** In the left-hand menu, navigate to the **Network > DHCP Server** page.

**Step 2** Locate the interface you just created, in our case this is the X2:V50 (virtual interface 50 on the physical X2 interface) interface. Click the **Configure**  icon corresponding to the desired interface.



### Note

If the interface you created does not appear on the **Network > DHCP Server** page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWALL. For more information on DHCP lease exhaustion, refer to the [“DHCP Server Scope” section on page 12](#).

3 Dynamic    Range: 10.10.5.2 - 10.10.5.190    X2:V50       

**Step 3** Edit the **Range Start** and **Range End** fields to meet your deployment needs

**Step 4** Click the **OK** button to save these changes.

Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.

3 Dynamic    Range: 10.10.5.2 - 10.10.5.50    X2:V50       

## Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
  - Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
  - Step 3** Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.
  - Step 4** Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
  - Step 5** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
  - Step 6** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN.
  - Step 7** Click the **OK** button to create this VAP Profile.

## Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in “[Creating a VLAN Sub-Interface on the WLAN](#)” section on page 26.

### General Tab

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
  - Step 2** Click the **Add...** button in the **Virtual Access Points** section.
  - Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the Zone to which it will be associated.
  - Step 4** Select the **VLAN ID** you created in “[Creating a VLAN Sub-Interface on the WLAN](#)” section on page 26 from the drop-down list. In this case we chose **50**, the VLAN ID of our VAP-Corporate VLAN.
  - Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.
  - Step 6** Check the **Enable SSID Suppress** checkbox to hide this SSID from users

**Virtual Access Point General Settings**

SSID:

VLAN ID:

Enable Virtual Access Point

Enable SSID Suppress

- Step 7** Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.

<input type="checkbox"/>	1	VAP-Guest	200	Open	None	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
--------------------------	---	-----------	-----	------	------	----	--------------------------	-------------------------------------	--	--

## Advanced Tab (Authentication Settings)

- Step 1** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to [Create More / Deploy Current VAPs, page 29](#).
- Step 2** In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
- Step 3** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
- Step 4** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN.

## Create More / Deploy Current VAPs

Now that you have successfully set up a VLAN for Corporate LAN access, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the [“Deploying VAPs to a SonicPoint”](#) section on page 30.



### Timesaver

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the [“Deploying VAPs to a SonicPoint”](#) section on page 30.

## VAP and the Domesticated Rabbit

Humans' relationship with the European or ‘true’ rabbit was first recorded by the Phoenicians over 1,000 years BC, when they termed the Iberian Peninsula ‘i-shephan-im’ (literally, ‘the land of the rabbit’), which the Romans converted to the Latin form, “Hispania,” and hence the modern word “Spain.”



The European Rabbit (*Oryctolagus cuniculus*) is the only species of rabbit to be domesticated. All pet breeds of rabbits - such as dwarf lops, angoras, etc. - are of this species. However, rabbits and people interact in many different ways beyond domestication. Rabbits are an example of an animal which is treated as food, pet and pest by the same culture. In Europe the rabbit is commonly eaten as food.

## Deploying VAPs to a SonicPoint

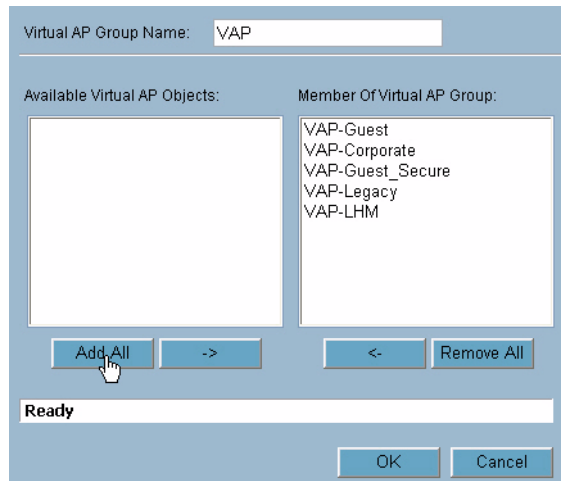
In the following section you will group and deploy your new VAPs, associating them with one or more SonicPoint Radios. Users will not be able to access your VAPs until you complete this process:

- [Grouping Multiple VAPs, page 30](#)
- [Creating a SonicPoint Provisioning Profile, page 30](#)

### Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SonicPoint(s).

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add Group...** button in the **Virtual Access Point Group** section.
- Step 3** Enter a **Virtual AP Group Name**.
- Step 4** Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.



- Step 5** Press the **OK** button to save changes and create the group.

### Creating a SonicPoint Provisioning Profile

In this section, you will associate the group you created in the “[Grouping Multiple VAPs](#)” section on page 30 with a SonicPoint by creating a provisioning profile. This profile will allow you to provision settings from a group of VAPs to all of your SonicPoints.

- 
- Step 1** In the left-hand menu, navigate to the **SonicPoint > SonicPoints** page.
- Step 2** Click the **Add** button in the **SonicPoint Provisioning Profiles** section.
- Step 3** Click the **Enable SonicPoint** checkbox to enable this profile.
- Step 4** In the **Name Prefix** field, enter a name for this profile.
- Step 5** Select a **Country Code** from the drop-down list.

- Step 6** From the **802.11 Radio Virtual AP Group** pull-down list, select the group you created in the “[Grouping Multiple VAPs](#)” section on page 30.

- Step 7** To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your SonicPoint VAPs will function.
- Step 8** Click the **OK** button to save changes and create this SonicPoint Provisioning Profile.
- Step 9** Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.

## Associating a VAP Group with your SonicPoint

If you did not create a SonicPoint Provisioning Profile, you can provision your SonicPoint(s) manually. You may want to use this method if you have only one SonicPoint to provision. This section is not necessary if you have created and provisioned your SonicPoints using a SonicPoint Profile.

- Step 1** In the left-hand menu, navigate to the **SonicPoint > SonicPoints** page.
- Step 2** Click the **Configure** button next to the **SonicPoint** you wish to associate your Virtual APs with.
- Step 3** In the Virtual Access Point Settings section, select the VAP group you created in [Grouping Multiple VAPs, page 30](#) from the **802.11g (or 802.11a) Radio Virtual AP Group** drop-down list. In this case, we choose **VAP** as our Virtual AP Group.

- Step 4** Click the **OK** button to associate this VAP Group with your SonicPoint.
- Step 5** Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.



### Note

If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages. For more information on configuring guest services, refer to the SonicOS Enhanced Administrator's Guide.

# Document Version History

<b>Version Number</b>	<b>Date</b>	<b>Notes</b>
1	6/21/2006	The document structure was created.
2	6/28/2006	Content written by Patrick Lydon and Khai Tran.
3	7/10/2006	Incorporated new content by Joe Levy
3	7/14/2006	Content additions completed for draft review.
4	8/2/2006	Reworked with feedback from Joe Levy.