▷ SONICWALL TECH NOTE:

Using VLANs With SonicWALLs

Introduction

This whitepaper will document how to integrate a VLAN-capable Ethernet switch with a SonicWALL PRO 4060 or PRO 5060 device running SonicOS Enhanced 3.0 firmware.

VLAN's (Virtual Local Area Networks) can be described as a 'tag-based LAN multiplexing technology' because through the use of IP header tagging, VLAN's can simulate multiple LAN's within a single physical LAN. Just as two physically distinct, disconnected LAN's are wholly separate from one another, so too are two different VLAN's, however the two VLAN's can exist on the very same wire. VLAN's require VLAN-aware networking devices to offer this kind of virtualization – switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags in accordance with the network's design and security policies.

VLAN's are useful for a number of different reasons, most of which are predicated on the VLAN's ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN's into smaller virtual LAN's, as well as to bring physically disparate LAN's together into a logically contiguous virtual LAN. The benefits of this include:

- Increased performance – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- Decreased costs – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLAN's, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLAN's as needed.
- Virtual workgroups – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLAN's allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- Security – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

VLAN support on SonicOS Enhanced is achieved by means of sub-interfaces, which are logical interfaces nested beneath a physical interface. Every unique VLAN ID requires its own sub-interface. VLAN sub-interfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, Wireless/SonicPoint support, 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.

Recommended Firmware Versions

- SonicOS Enhanced 3.0.0.6 or newer

Customers with current service/software support contracts can obtain updated versions of SonicWALL firmware from the MySonicWALL customer portal at https://www.mysonicwall.com. Updated firmware is also freely available to customers who have registered the SonicWALL device on MySonicWALL for the first 90 days.

Tested Switches

- NetGear FS526T/FSM726/FSM726S
- Dell PowerConnect 3324
- Extreme Summit-Series
- Intel Express Gigabit Switch
- Cisco Catalyst 2900xl-series
- Cisco Catalyst 2950-series
- Cisco Catalyst 3500-series

SonicWALL's VLAN implementation will work with any Ethernet switch that supports the 802.1Q trunking protocol. The switches listed above are the ones that SonicWALL tested in-house and are known to interoperate with a SonicWALL PRO 4060 and PRO 5060 device.

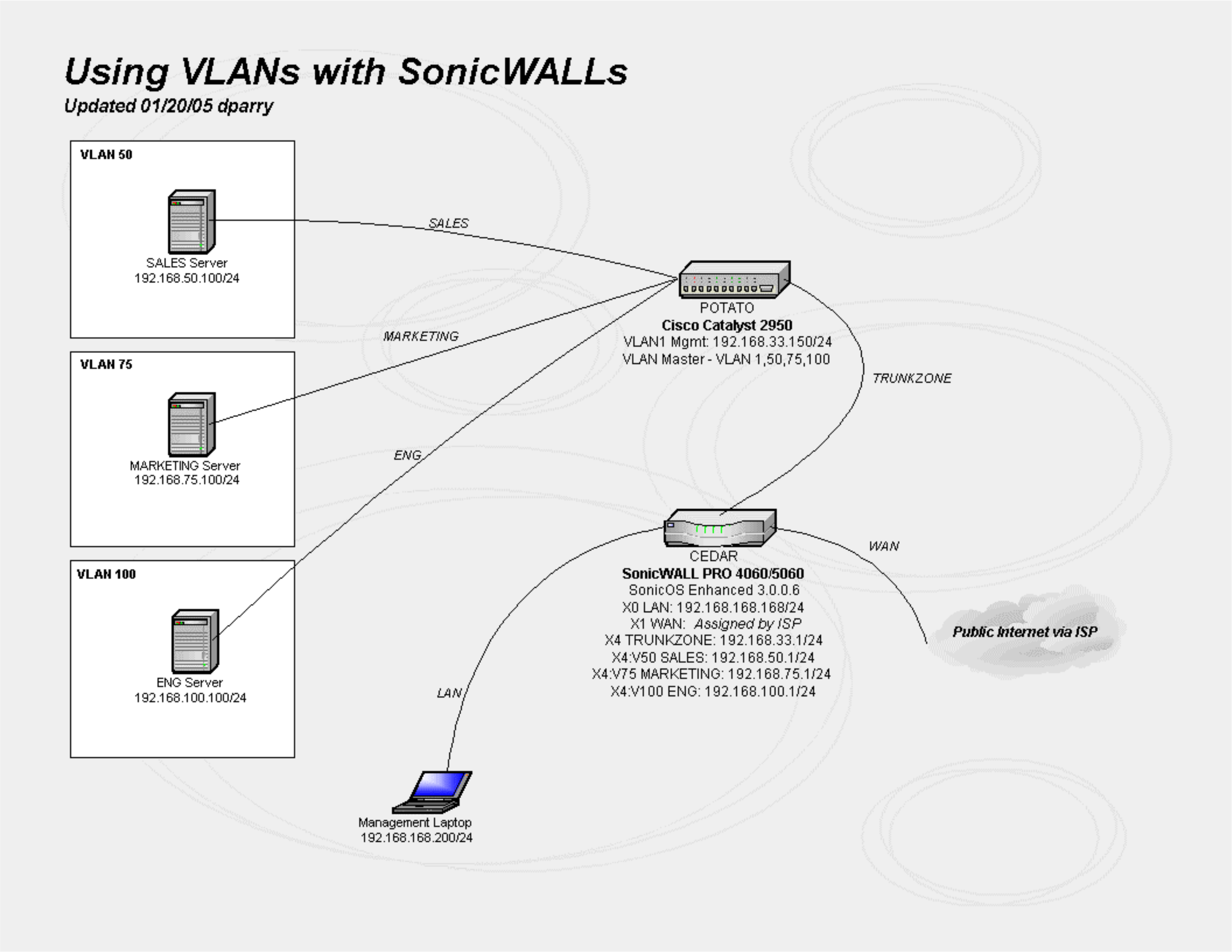
Caveats

- Many older Cisco Catalyst-series switches are set to use ISL (Inter-Switch Link) as the default trunking protocol, instead of 802.1Q. You will need to explicitly program the trunk port for 802.1Q in order for it to interoperate with the SonicWALL device, as SonicWALLs do not support ISL (only 802.1Q). The command to change the switch from ISL to 802.1Q is: 'switchport trunk encapsulation dot1q'.
- SonicWALLs do not support VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol) – you will need to explicitly force trunking on the switch port that's connected to the SonicWALL device, as it will not auto-negotiate the trunk.
- You can create up to 200 subinterfaces on PRO 4060, and up to 400 subinterfaces on the PRO 5060
- You can create up to 20 zones on the PRO 4060, and up to 64 zones on the PRO 5060
- No VLAN/Subinterface support on models other than PRO 4060 and PRO 5060
- VLAN/Subinterface support is a feature of SonicOS Enhanced 3.0 and newer, and is not included with any version of SonicOS Standard
- Make sure to use good CAT5e/CAT6 cabling between the Ethernet Switch and the SonicWALL device, as we'll be locking the speed to 100Mbps and the duplex to full on both sides.
- You do not have to assign the SonicWALL's interface that will connect to the switch's trunk port to a zone and assign it an interface address. However, doing so will allow the switch to be reached via telnet/SSH for manageability, and send logging/SNMP info to an external source.

A Note about Management VLANs

Most VLAN-capable switches, by default, are set to use VLAN1 as the native/management VLAN, and the switch manufacturers' do not recommend installing users or networking devices in VLAN1. Also note that VLAN1 is not a tagged (explicit) VLAN, but rather a port (implicit) VLAN, and VLAN 1 should **not** be used for tagging. On an 802.1Q trunk port, the native VLAN frames are not tagged.

Sample Diagram



Tasklist

- Configure native VLAN (usually VLAN1) management interface's IP addressing information on switch
- Configure VLANs on Ethernet switch
- Configure IP routing information on switch
- Assign switch ports to respective VLANs, configure ports, plug in devices to switch
- Configure trunk port on switch and connect to SonicWALL
- Configure X4 as trunk port on SonicWALL, assign IP information
- Create zones and subinterfaces on SonicWALL, tag VLAN ID's to respective VLANs
- Create DHCP Scopes for each subinterface
- Test configuration
- [Optional] Integrate SonicPoints on designed wireless VLAN

Before You Begin

In this whitepaper, we'll be using a Cisco Catalyst-series switch for all examples. If you are using another manufacturer's VLAN-capable Ethernet switch, please refer to their documentation on how to configure the switch for VLANs, trunking, fast spanning-tree, and speed/duplex locking. Also make sure the SonicWALL is fully configured for public Internet access via it(s) WAN port(s) before configuring any of the proceeding steps.

Setup Steps

Switch Config

As noted, we're using a Cisco Catalyst-series switch for the examples in this whitepaper. The commands noted here are applicable for most of the low-end Catalyst-series devices, but do not apply to the higher-end Catalyst-series, such as the 4500-series & 6500-series. Before you begin, make sure you know the switch's console, enable, and enable-secret passwords.

1. Using the Switch's console port, enter exec mode, log into the device's config menu ('config t') and access the 'VLAN1' management interface. Assign the VLAN1 management interface an IP address using the command 'ip address 192.168.33.150 255.255.255.0'.
2. Assign the switch a default IP gateway using the command 'ip default-gateway 192.168.33.1'.
3. Exit the config menu and return to the exec (#) prompt. At this prompt, type 'vlan database' and hit return. Depending upon the switch IOS version, you may receive a warning that this command will be deprecated in the future, which can be ignored. In the VLAN configuration submenu, enter the following commands: 'vlan 50 name SALES', 'vlan 75 name MARKETING', and 'vlan 100 name ENG'. When done, enter the command 'apply' to save and activate these new VLANs, then exit the VLAN submenu and return to the exec prompt.
4. Type 'config t' at the exec prompt to return to the config menu. Pick an open interface on the switch to be used as the trunk port. In this example, we're using FastEthernet0/24 as our trunk port to the SonicWALL device. In the interface's configuration submenu, enter the following commands: 'description trunk link to sonicwall', 'switchport mode trunk', 'switchport nonegotiate', 'no cdp enable', 'speed 100', 'duplex full', and 'spanning-tree portfast'. Exit this interface's submenu by typing 'exit'.
5. While still in the config menu, pick an open interface to assign to the new SALES VLAN 50. For each interface, enter the following commands: 'spanning-tree portfast', and 'switchport access vlan 50'. Exit this interface's submenu by typing 'exit'.
6. While still in the config menu, pick an open interface to assign to the new MARKETING VLAN 75. For each interface, enter the following commands: 'spanning-tree portfast', and 'switchport access vlan 75'. Exit this interface's submenu by typing 'exit'.
7. While still in the config menu, pick an open interface to assign to the new ENG VLAN 100. For each interface, enter the following commands: 'spanning-tree portfast', and 'switchport access vlan 100'. Exit this interface's submenu by typing 'exit'.
8. When done, return to the exec prompt and type 'copy run start' (or the older command 'wr mem') to save and activate these changes.

Your Cisco Catalyst-series switch config should look something like this:

```
redwood#sho runn
Building configuration...

Current configuration : 2053 bytes
! Last configuration change at 10:22:00 PST Wed Jan 26 2005
! NVRAM config last updated at 10:22:13 PST Wed Jan 26 2005
version 12.1
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service dhcp
hostname redwood
!
no logging console
enable secret 5 $1$.5zS$AB6RhN1TqfRu/.p5lDzzC.
enable password 7 13000117190B162F2E2A
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
```

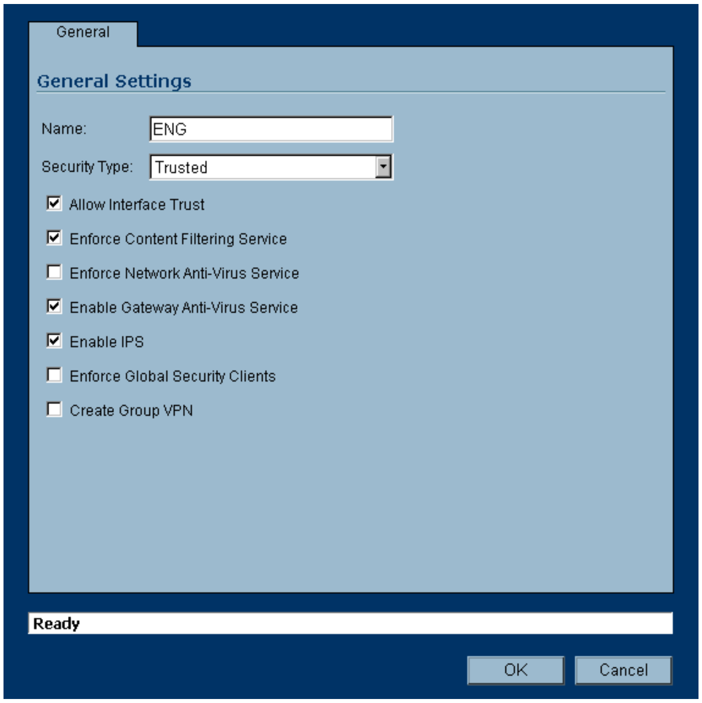
```
!
ip domain-name vpntestlab.com
ip name-server 192.168.1.5
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 50
 spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 75
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 100
 spanning-tree portfast
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
 description link to SonicPoint-1
 switchport access vlan 125
 spanning-tree portfast
!
interface FastEthernet0/18
 description link to SonicPoint-2
 switchport access vlan 125
 spanning-tree portfast
!
interface FastEthernet0/19
 description link to SonicPoint-3
 switchport access vlan 150
 spanning-tree portfast
!
interface FastEthernet0/20
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 description trunk link to sonicwall
 switchport mode trunk
 switchport nonegotiate
 speed 100
 duplex full
 no cdp enable
 spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.33.150 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.33.1
no ip http server
!
line con 0
line vty 0 4
 session-timeout 20
 password 7 045E1D031D265E4B0C17
 login
line vty 5 15
 session-timeout 20
 password 7 045E1D031D265E4B0C17
 login
!
ntp clock-period 17179893
ntp server 192.43.244.18
!
end
```

SonicWALL Config

For this whitepaper, a SonicWALL PRO 4060 running SonicOS Enhanced 3.0.0.6 was used for the examples listed below. In our example, we're using interface X4 as the connecting port to the Cisco Catalyst switch trunk port, which in the previous section, we assigned interface FastEthernet0/24 as.

1. From a system in the SonicWALL's LAN zone (X0), log into the SonicWALL's web-management GUI.
2. Go to the 'Network > Zones' page and create four new zones, named 'trunkzone', 'SALES', 'MARKETING', and 'ENG". Assign all three of these new zones a security type of 'Trusted'. If your SonicWALL PRO 4060/5060 is licensed for Content Filtering Service, Network Anti-Virus, Gateway Anti-Virus, or Intrusion Prevention Service, and you wish to enforce these services on this zone, check the boxes next to these services, then click on the 'OK' button to save and activate the change. See Figure 1 on the next page for an example.



Name: ENG

Security Type: Trusted

☑ Allow Interface Trust

☑ Enforce Content Filtering Service

☐ Enforce Network Anti-Virus Service

☑ Enable Gateway Anti-Virus Service

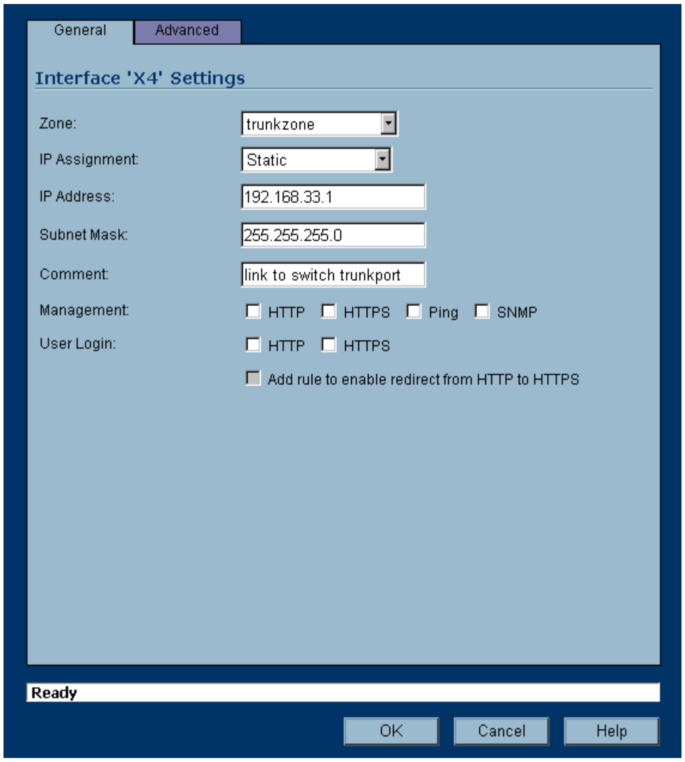
☑ Enable IPS

☐ Enforce Global Security Clients

☐ Create Group VPN

Figure 1 – Creating a new 'ENG' Zone to attach to VLAN 100

3. Go to the 'Network > Interfaces' page and click on the 'Configure' icon next to interface X4. In the pop-up menu that appears, assign it to zone 'trunkzone' and give it an IP address of '192.168.33.1'. Then, click on the 'Advanced' tab and set the X4 interface to be locked at 100Mbps full-duplex, since we previously set the switch's trunk port for the same thing. When done, click on the 'OK' button to save and activate the changes. See Figure 2 below for an example.



Zone: trunkzone

IP Assignment: Static

IP Address: 192.168.33.1

Subnet Mask: 255.255.255.0

Comment: link to switch trunkport

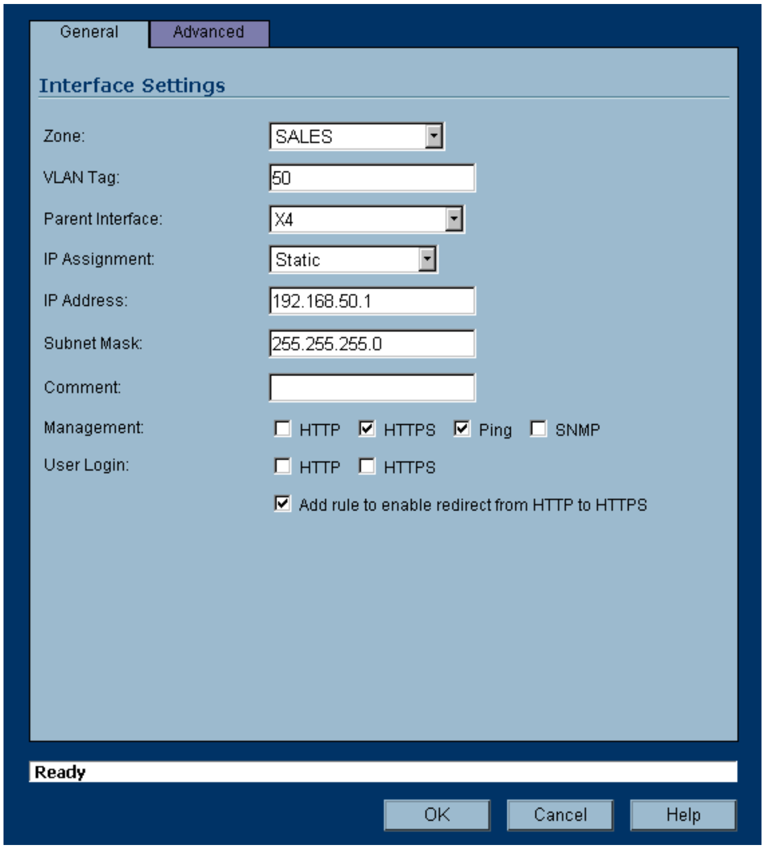
Management: ☐ HTTP ☐ HTTPS ☐ Ping ☐ SNMP

User Login: ☐ HTTP ☐ HTTPS

☐ Add rule to enable redirect from HTTP to HTTPS

Figure 2 – Attach interface X4 to the 'TRUNKZONE' zone

4. On the ‘Network > Interface’ page, click on the ‘Add Interface…’ button. From the pop-up menu that appears, assign the subinterface to zone ‘SALES’, enter the VLAN tag/ID as ‘50’, assign the parent interface as ‘X4’, assign the subinterface an IP address of ‘192.168.50.1’, check the boxes next to ‘HTTPS’ and ‘Ping’ for management, then click on the ‘OK’ button to save an activate the changes. See Figure 3 below for an example (NOTE: generic example).
5. On the ‘Network > Interface’ page, click on the ‘Add Interface…’ button. From the pop-up menu that appears, assign the subinterface to zone ‘MARKETING’, enter the VLAN tag/ID as ‘75’, assign the parent interface as ‘X4’, assign the subinterface an IP address of ‘192.168.75.1’, check the boxes next to ‘HTTPS’ and ‘Ping’ for management, then click on the ‘OK’ button to save an activate the changes. See Figure 3 below for an example (NOTE: generic example).
6. On the ‘Network > Interface’ page, click on the ‘Add Interface…’ button. From the pop-up menu that appears, assign the subinterface to zone ‘ENG’, enter the VLAN tag/ID as ‘100’, assign the parent interface as ‘X4’, assign the subinterface an IP address of ‘192.168.100.1’, check the boxes next to ‘HTTPS’ and ‘Ping’ for management, then click on the ‘OK’ button to save an activate the changes. See Figure 3 below for an example (NOTE: generic example).



Interface Settings

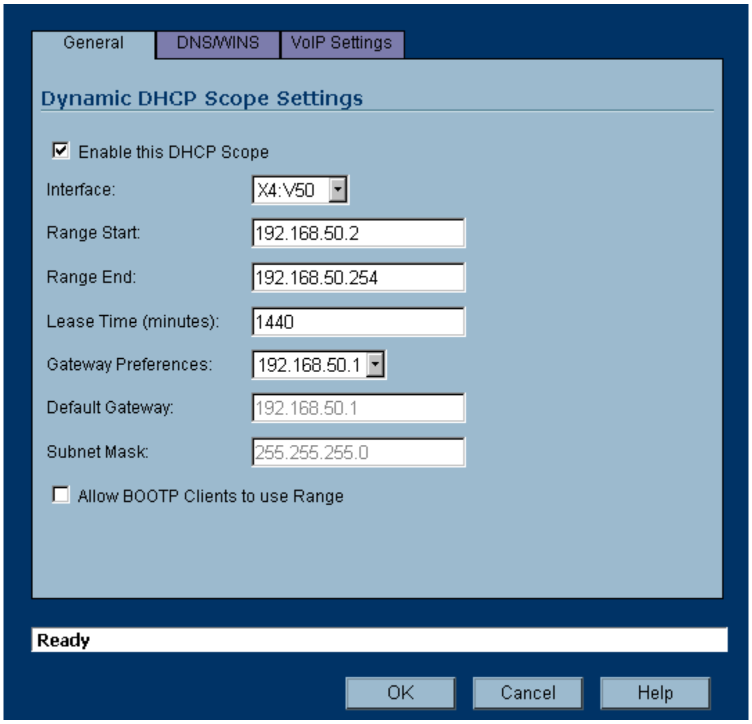
Zone: SALES
VLAN Tag: 50
Parent Interface: X4
IP Assignment: Static
IP Address: 192.168.50.1
Subnet Mask: 255.255.255.0
Comment:
Management: ☐ HTTP ☑ HTTPS ☑ Ping ☐ SNMP
User Login: ☐ HTTP ☐ HTTPS
☑ Add rule to enable redirect from HTTP to HTTPS

Ready

Figure 3 – Creating a subinterface

7. Go to the ‘Network > DHCP Server’ page. Make sure the checkbox next to ‘Enable DHCP Server’ is checked. Click on the ‘Add Dynamic’ button. From the pop-up that appears, choose ‘X4:V50’ from the drop-down next to ‘Interface’, make sure the box next to ‘Enable this DHCP Scope’ is checked, accept all defaults, and click on the ‘OK’ button to save and activate the scope. See figure 4 on the next page for an example (NOTE: generic example).
8. Go to the ‘Network > DHCP Server’ page. Click on the ‘Add Dynamic’ button. From the pop-up that appears, choose ‘X4:V75’ from the drop-down next to ‘Interface’, make sure the box next to ‘Enable this DHCP Scope’ is checked, accept all defaults, and click on the ‘OK’ button to save and activate the scope. See figure 4 on the next page for an example (NOTE: generic example).

9. Go to the 'Network > DHCP Server' page. Click on the 'Add Dynamic' button. From the pop-up that appears, choose 'X4:V100' from the drop-down next to 'Interface', make sure the box next to 'Enable this DHCP Scope' is checked, accept all defaults, and click on the 'OK' button to save and activate the scope. See figure 4 below for an example (NOTE: generic example).



Dynamic DHCP Scope Settings

☑ Enable this DHCP Scope

Interface: X4:V50

Range Start: 192.168.50.2

Range End: 192.168.50.254

Lease Time (minutes): 1440

Gateway Preferences: 192.168.50.1

Default Gateway: 192.168.50.1

Subnet Mask: 255.255.255.0

☐ Allow BOOTP Clients to use Range

Ready

Figure 4 – Creating DHCP Scopes for the subinterfaces

The SonicWALL will automatically create all necessary address objects, address groups, and NAT Policies necessary for these new VLAN/Subinterfaces to function correctly. When done with this section, please proceed to the Testing/Troubleshooting section of this whitepaper, unless you wish to integrate SonicPoints. If this is the case, please proceed to the steps in the next section.

Optional Steps – Wireless Integration

If you have SonicWALL SonicPoint wireless devices, the use of VLAN/Subinterfaces with a VLAN-capable switch is an ideal method to deploy multiple SonicPoint devices in your networking environment. In the examples below, we'll be attaching three SonicPoint devices onto the Cisco Catalyst-series switch; two of these will be for internal employee use, and a third will be for guest users. We'll be using VLANs to separate the wireless devices, and the features of the SonicWALL to completely secure the network for wired and wireless users alike.

Switch Side

NOTE: full command details for the following steps can be found on page 4 of this whitepaper.

1. On the switch, create two additional VLAN's: VLAN 125, and VLAN 150.
2. Assign two open interfaces on the switch to VLAN 125, and one open interface to VLAN 150. Program all three ports for 'spanning-tree portfast'.
3. Exit to the exec prompt and save all changes.
4. Plug the three SonicPoints into their respective switch ports and power them on.

SonicWALL Side

NOTE: full command details for many of following steps can be found on pages 6-9 of this whitepaper.

1. On the SonicWALL, go to the 'SonicPoint > SonicPoint' page and click on the 'Add' button. From the pop-up that appears' create a new SonicPoint profile named 'EMPLOYEES", using a SSID of 'employee' for the 802.11a and 802.11b/g radios. Leave all other default settings as-is, then click on 'OK' to save and activate the changes.
2. On the SonicWALL, go to the 'SonicPoint > SonicPoint' page and click on the 'Add' button. From the pop-up that appears' create a new SonicPoint profile named 'GUESTS", using a SSID of 'guest' for the 802.11a and 802.11b/g radios. Leave all other default settings as-is, then click on 'OK' to save and activate the changes.
3. Go to the 'Network > Zones' page and create a new zone called 'WIRELESS_GUESTS' and assign it a security type of 'Wireless'. Click on the 'Wireless' tab on this pop-up, uncheck the box next to 'WiFiSec Enforcement', and select 'GUESTS' as the 'SonicPoint Provisioning profile'. Then, click on the 'Guest Services' tab on this pop-up and check the boxes next to 'Enable Wireless Guest Services', 'Enforce Guest Login over HTTPS', 'Bypass AV Check for Guests', and 'Enable Dynamic Address Translation'. When done, click on the 'OK' button to save and activate these changes.
4. Go to the 'Network > Zones' page and click on the 'Config' icon next to the pre-existing 'WLAN' zone. On the pop-up that appears, click on the 'Wireless' tab, and select 'EMPLOYEES' as the 'SonicPoint Provisioning Profile'. Also make sure that the checkbox next to 'WiFiSec Enforcement' is enabled (it should be by default). When done, click on the 'OK' button to save and activate these changes.
5. Create a new subinterface on the X4 interface, assign it to VLAN/ID 125, assign it to the 'WLAN' zone, and assign it an IP address of '192.168.125.1'.
6. Create a new subinterface on the X4 interface, assign it to VLAN/ID 150, assign it to the 'WIRELESS_GUESTS' zone, and assign it an IP address of '192.168.150.1'.
7. Since these are wireless zones, the SonicWALL will automatically create and activate DHCP scopes.
8. You may wish to modify the default firewall rule for WIRELESS_GUESTS zone to WLAN zone to 'Deny'. This way, wireless guest services users cannot access any of the wireless employees.
9. You may wish to modify the default firewall rule for WLAN zone to WIRELESS_GUESTS zone to 'Deny'. This way, wireless employees cannot access any of the wireless guests.
10. If you wish the WLAN zone to access LAN resources, modify the default firewall rule for WLAN zone to LAN zone to 'Allow'.
11. Go to the 'Users > Local Users' page and create a test account named 'testone' with a password of 'cranberry'.
12. Go to the 'Users > Guest Services' page and click on the 'Generate…' button. In the pop-up that appears, enter '10' into the field next to 'Number of Accounts:', then click on the 'OK' button to automatically generate 10 wireless guest services users and passwords. To see the guest user names and passwords, simply click on the little printer icon next to each account.
13. Go to the 'VPN > Settings' page. Check the box next to 'Enable VPN' (it should be by default). Then, check the box next to 'Enable' for the 'WLAN Group VPN' VPN Policy.
14. Check the 'SonicPoint > SonicPoints' page. You should see all three SonicPoints as successfully provisioned with a status of 'Operational'. If not, reboot the SonicWALL device and check again.
15. Get a wireless laptop, install SonicWALL's Global VPN Client version 2.1 or later, attach the wireless card to SSID 'employee', activate GVC with the 'office gateway' profile, enter in username of 'testone' and password of cranberry. Test for access.
16. Get a wireless laptop, attach the wireless card to SSID of 'guest', open a web browser and attempt to access site on public Internet. You should be redirected to a login/authentication page. When prompted, enter in a guest services account and password, then test for access.

Testing/Troubleshooting

To test, install a desktop or server into each port you assigned to each VLAN, and set the desktop/server to retrieve its IP address via DHCP. From a command prompt on each system, issue the windows commands ‘ipconfig/release’ and ‘ipconfig/renew’. If everything was configured correctly, each system should receive a DHCP lease for its respective subnet. If this was successful, test connectivity from each system to the public Internet, and between each system (keeping in mind any firewall rules between the zones you may have created and have active). If there are connectivity problems, please review all steps in this whitepaper to ensure that all devices are configured correctly.

The most common mistakes seen are: failure to bind the subinterface to the proper physical interface (page 8, steps 4-6), failure to enter the correct VLAN/ID tag on the subinterface (page 8, steps 4-6), and failure to tag the interface connecting the switch as a 802.1Q trunk port (page 4, step 4).

Created: 01/15/04
Updated: 02/02/04
Version 1.2