TechNote

BEST PRACTICES

SonicWALL SonicPoint Deployment Best Practices Guide

Overview

This document will guide you through the design, installation, deployment, and configuration issues regarding SonicWALL's SonicPoint wireless access points. The information covered in this guide will allow site administrators to properly deploy SonicPoints in environments of any size. This document will also cover any related external issues that are required for successful operation and deployment.

Please note that SonicWALL cannot provide any direct technical support for any of the third-party Ethernet switches referenced in this document. The material is also subject to change without SonicWALL's knowledge when the switch manufacturer releases new models or firmware that may invalidate the information contained in this doc, as we do not have direct relationships with most of these manufacturers. The only exception to this rule is Hewlett-Packard, as SonicWALL is currently a member of HP's ProCurve Alliance program, and works closely with HP to ensure compatibility with the ProCurve switch product line.

Further information on this can be found at:

http://www.procurve.com/alliance/members/sonicwall.htm.

Prerequisites

- SonicPoints require the use of SonicOS Enhanced versions 3.0 and above on the SonicWALL UTM Appliance; newer versions of SonicOS Enhanced require public Internet access in order for the UTM Appliance to download and update the SonicPoint firmware images. If the device does not have public Internet access, you will need to obtain and download the SonicPoint firmware manually.
- One or more SonicWALL SonicPoint or SonicPoint-G wireless access points.
- If you are using a PoE switch to power the SonicPoint, it must be an 802.3af-compliant Ethernet switches. Vendor-specific switch programming notes can be found towards the end of this technote for HP, Cisco, Dell, and D-Link. If not, you will need to use the power adapter that ships with the SonicPoint, or SonicWALL's PoE Injector (http://www.sonicwall.com/downloads/SonicWALL_PoE_Injector_Users_Guide.pdf).
- It's strongly recommended you obtain a support contract for SonicWALL as well as the PoE switch; this will allow you to update to new versions if issues are found on the switch side or on the SonicWALL side, or when new features are released.
- Be sure do conduct a full site survey before installation (see section below).
- Check wiring and cable infrastructure to verify end-to-end runs between SonicPoints and the Ethernet switches are CAT5, CAT5e, or CAT6.
- Check building codes for install points and work with building's facilities staff, as some desired install points may violate regulations.

SONICWALL

Recommended Versions

- SonicOS Enhanced 4.0.1.0 or newer strongly recommended if using PoE switches, as this version resolves discovery, stability, and throughput issues.
- SonicOS Enhanced 3.5.0.2 or newer if VAP support required.
- SonicOS Enhanced 3.2.x or newer if SonicPoint-G support required.
- Check with the switch vendor to determine recommended version; if using ProCurve switches please update to firmware releases from summer 2007 or newer.

Best Practices

UTM Appliances that support SonicPoints (assuming most current firmware release as of 1/8/08)

- NSA E7500– supports 32 on each interface, 128 total
- NSA E6500– supports 32 on each interface, 128 total
- NSA E5500 – supports 32 on each interface, 96 total
- PRO 5060 – supports 128 on each interface, 128 total
- PRO 4100 – supports 128 on each interface, 128 total
- PRO 4060 – supports 64 on each interface, 64 total
- PRO 3060 – supports 64 on each interface, 96 total
- PRO 2040 – supports 64 on each interface, 96 total
- PRO 1260 – supports 32 on each interface, 32 total
- TZ 190/W – supports 16 on OPT interface, 16 total
- TZ 180/W – supports 16 on OPT interface, 16 total
- TZ 170/W/SPW – supports 8 on OPT interface, 8 total

Layer 2 and Layer 3 considerations for SonicPoints

- SonicWALL uses two proprietary protocols (SDP and SSPP) and both *cannot* be routed across any layer 3 device. Any SonicPoint that will be deployed must have an Ethernet connection back to the provisioning SonicWALL UTM appliance, in the same broadcast domain/network.
- SonicWALL UTM appliance must have interface or sub-interface in same VLAN/broadcast domain as SonicPoint.
- SonicPoints must be able to reach the DHCP scope on the SonicWALL; make sure other DHCP servers are not present on VLAN/broadcast domain.
- Sharing SSIDs across SonicPoints attached to multiple interfaces may case connectivity issues as wireless client roams to different SonicPoint subnet.

Tested switches

- Most Cisco switches work well; however SonicWALL does not recommend deploying SonicPoints using the “Cisco Express” switch line.
- SonicWALL does not recommend deploying SonicPoints using Netgear PoE switches.
- If you are using D-Link PoE switches, you will need to shut off all their proprietary broadcast-control/storm control mechanisms, as they will interfere with the provisioning and acquisition mechanisms in the SonicPoint (see section regarding this).
- Dell; make sure to configure STP for fast start on SonicPoint ports.
- Extreme; make sure to configure STP for fast start on SonicPoint ports.
- Foundry; make sure to configure STP for fast start on SonicPoint ports.
- HP ProCurve; make sure to configure STP for fast start on SonicPoint ports.

Wiring Considerations

- Make sure wiring is CAT5, CAT5e, or CAT6 end to end.
- Due to signaling limitations in 802.3af and Ethernet cable runs cannot go over 100 meters between PoE switch and SonicPoint.
- You will need to account for PoE power loss the longer the cable run is; this can can be up to 16%, and due to this that port will require more power to be supplied.

Site Survey and Planning

- Conduct a full site-walk of all areas SonicPoints will be deployed in with a wireless spectrum scanner; note any existing AP’s and the channels they are broadcasting on. SonicWALL currently recommends using Fluke or AirMagnet products to conduct full site surveys. You may also wish to try out NetStumbler/MiniStumbler, which while free does a decent job of surveying, providing it works with your wireless card.

- Blueprints of floor plans are helpful; here you can mark the position of Access Points and the range of the wireless cell. Make multiple copies of these as during the site-survey results may cause the original design not to be the best and a new start will be needed. As well you see where walls, halls and elevators are located, that can influence the signal. Also, areas in which users are located – and where not - can be seen. During the site-survey keep an eye open for electrical equipment that may cause interference (microwaves, CAT Scan equipment, etc…) In area’s were a lot of electrical equipment is placed, also take a look at the cabling being used. In areas with a lot of electrical equipment UTP should not be used, FTP or STP is required.

- Survey three dimensionally, wireless signals cross over to different floors.

- Determine where you can locate APs based on power and cabling. Remember that you shouldn't place APs close to metal or concrete walls and you should put them as close to the ceiling as possible.
- Use the wireless scanning tool to check signal strengths and noise. Signal to noise ratio should at least be 10dB (minimum requirements for 11 Mbps), however 20dB is preferred. Both factors influence the quality of the service.

- Relocate the AP’s and re-test, depending of the results of your survey.

- Save settings, logs and note the location of the AP for future reference.
- If you find that certain areas, or all areas are saturated with existing overlapping 802.11b/g channels, you may wish to deploy SonicPoints using the 802.11a radio. This provides a much larger array of channels to broadcast on, although the range of 802.11a is limited, and the SonicPoint does not allow for the addition of external antennas (only the SonicPoint-G model allows this).
- When planning, make sure you note the distance of cable runs from where the SonicPoint will be mounted; this must be 100 meters or less. If you are not using PoE switches, you will also need to account for the power adapter or PoE injector for the SonicPoint or SonicPoint-G. Make sure you are not creating an electrical or fire hazard.
- Be wary of broadcasting your wireless signal into areas that you do not control; check for areas where people might be able to leach signal and tune the SonicPoints accordingly.
- For light use, you can plan for 15-20 users for each SonicPoint. For business use, you should plan for 5-10 users for each SonicPoint.
- Plan accordingly for roaming users – this will require tuning the power on each SonicPoint so that the signal overlap is minimal. Multiple SonicPoints broadcasting the same SSID in areas with significant overlap can cause ongoing client connectivity issues.
- Use the scheduling feature in SonicOS Enhanced to shut SonicPoints when not in use – it's recommended that you do not operate your SonicPoints during non-business-hours (off nights and weekends).

Channels

The default setting of SonicPoints is auto-channel. When this is set, at boot-up the SP will do a scan and check if there are other wireless devices are transmitting. Then it will try to find an unused channel and use this for transmission. Especially in larger deployments, this can cause trouble. Here it is recommended to assign fixed channels to each SonicPoint. A diagram of the SP's and their MAC-Addresses helps to avoid overlaps, best is to mark the location of the SP's and MAC-Addresses on a floor-plan.

Wireless Card Tuning

If you are experiencing connectivity issues with laptops, check to see if the laptop has an Intel embedded wireless adapter. The following Intel chipsets are publicly known and acknowledged by Intel to have disconnect issues with third-party wireless access points such as the SonicWALL SonicPoint and SonicPoint-G:

- ✓ Intel PRO/Wireless 2100 Network Connection
- ✓ Intel PRO/Wireless 2100A Network Connection
- ✓ Intel PRO/Wireless 2200BG Network Connection
- ✓ Intel PRO/Wireless 2915ABG Network Connection
- ✓ Intel PRO/Wireless 3945ABG Network Connection

These wireless cards are provided to OEM laptop manufacturers and are often rebranded under the manufacturers name – for example, both Dell and IBM use the above wireless cards but the drivers are branded under their own name.

To identify the adapter, go to Intel's support site and do a search for 'Intel Network Connection ID Tool'. Install and run this tool on any laptop experiencing frequent wireless disconnect issues. The tool will identify which Intel adapter is installed inside the laptop.

Once you have identified the Intel wireless adapter, go to Intel's support site and download the newest software package for that adapter – it's recommended you download and install the full Intel PRO/Set package and allow it to manage the wireless card, instead of Windows or any OEM-provided wireless network card management program previously used. As of January 2007 the most recent version of the full Intel PRO/Set Wireless software driver/manager is 10.5.2.0. SonicWALL recommends you use this version or newer.

Be sure to use the Intel wireless management utility and to disable Microsoft's Wireless Zero Config management service – the Intel utility should control the card, not the OS.

In the 'Advanced' section, disable the power management by unchecking the box next to 'Use default value', then move the slidebar under it to 'Highest'. This instructs the wireless card to operate at full strength and not go into sleep mode. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

In the 'Advanced' section, adjust the roaming aggressiveness by unchecking the box next to 'Use default value', then move the slidebar under it to 'Lowest'. This instructs the wireless card to stay stuck to the AP it's associated as long as possible, and only roam if the signal is significantly degraded. This is extremely helpful in environments with large numbers of access points broadcasting the same SSID. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

If you continue to have issues, you may also try adjusting the Preamble Mode on the wireless card. By default the Intel wireless cards above are set to 'auto'. All SonicWALL wireless products by default are set to use a 'Long' preamble, although this can be adjusted in the Management GUI. To adjust the Intel wireless card's preamble setting, go to the 'Advanced' section and uncheck the box next to 'Use default value', then select 'Long Tx Preamble' from the drop-down below it. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

PoE

- A SonicPoint and SonicPoint-G's draw at full power is 6-10 Watts.
- SonicPoints are set to Class 0 PD (meaning that it can be 0.44W minimum up to 12.95W maximum). A mismatch in Class will cause confusion in the handshake and reboot the SonicPoint.
- Full 802.3af compliance is required on any switch that will be supplying PoE to a SonicPoint or SonicPoint-G. Do not operate SonicPoints on non-compliant switches as SonicWALL does not support it.
- Turn off pre-802.3af-spec detection as it may cause connectivity issues.
- Long cable runs cause loss of power; 100 meter runs between SonicPoint and PoE switch may incur up to 16% power/signal degradation; because of this the PoE switch will need to supply more power to the port to keep the SonicPoint operational.
- Because of this, make sure each port can get 10 Watts guaranteed if possible, and set the PoE priority to critical or high.
- One thing to be particularly careful to plan for is that not all PoE switches can provide the full 15.4 watts of power to each of its PoE ports – it might have 24 but it can't actually have all ports with PoE devices attached without the addition of an external redundant power supply. You will need to work closely with the manufacturer of the PoE switch to ensure that enough power is supplied to the switch to power all of your PoE devices.

Spanning-Tree

- When an Ethernet port becomes electrically active, most switches by default will activate the spanning-tree protocol on the port to determine if there are loops in the network topology. During this detection period of 50-60 seconds the port does not pass any traffic – this feature is well-known to cause problems with SonicPoints. If you do not need spanning-tree, disable it globally on the switch, or disable it on each port connected to a SonicPoint device.
- If this is not possible, check with the switch manufacturer to determine if they allow for "fast spanning-tree detection", which is a method that runs spanning-tree in a shortened time so as to not cause connectivity issues. Please refer to the switch-specific sections at the end of this technote for programming samples on how to do this.

VTP and GVRP

- Turn these trunking protocols off on ports connected directly to SonicPoints, as they have been known to cause issues with SonicPoints – especially the high-end Cisco Catalyst-series switches.

Port-Aggregation

- Many switches have port aggregation turned on by default – this causes a lot of issues and should be deactivated on ports connected directly to SonicPoints.
- PAGP/Fast EtherChannel/EtherChannel – turn this off on the ports going to SonicPoints.
- LACP – turn this off on the ports going to SonicPoints.

Broadcast Throttling/Broadcast Storm

- This feature is an issue on some switches, especially D-Link. Please disable on per port basis if possible, if not disable globally.

Speed and Duplex (and how to troubleshoot)

- At present, auto-negotiation of speed and duplex is the only option for SonicPoints.
- Lock speed and duplex on switch and reboot SonicPoint -- this may help with connectivity issues.
- Check port for errors, as this is the best way to determine if there is a duplex issue (port will also experience degraded throughput).

Troubleshooting Older SonicPoints

- If you have an older SonicPoint and it's consistently port flapping, or doesn't power up at all, or is stuck reboot cycling, or reports in the GUI as stuck in provisioning, check to see if you are running a current version of firmware, and that the SonicWALL UTM appliance has public internet access. You may need to RMA for a newer SonicPoint.

VAP Issues

- You will need to manually adjust the broadcast/beacon timing when using multiple SSIDs, if using versions of SonicOS Enhanced older than 4.0.1.0 (set beacon to 800).
- Only VLAN-supported SonicWALL platforms can offer VAP features for existing releases. Each SSID should be associated with the unique VLAN ID to segment traffic in different broadcast domains. SDP/SSPP protocol packets must be untagged before reaching SonicWALL WLAN interface or SonicPoint.
- The switch between SonicWALL and SonicPoint must be configured properly to allow both untagged SDP/SSPP traffic and tagged traffic with VLAN ID for each VAP SSID.
- If at all possible assign each VAP to its own VLAN/Security Zone -- this will provide maximum security and although not explicitly required for PCI compliance, puts you solidly in the "green" zone.
- If you use VLAN's, do not use the parent interface and do not use the default VLAN.

Troubleshooting

- When creating a Wireless zone and interface, make sure to configure the interface for the number of SonicPoints you wish to support -- new interfaces are set to 'No SonicPoints' by default. If you do not do this, the UTM appliance will not create the necessary DHCP scope and will not acquire any SonicPoints added to the interface.
- If you added SonicPoints and only a certain number were detected and acquired, check interface settings as noted above, as it might be set for too few SonicPoints.
- If throughput seems sluggish, check to see how many SonicPoints you have on an interface – in large deployments it's advisable to spread them across more than one. Try to limit the interfaces to a 4-to-1 oversubscription ratio. For example, if you have a 100Mbps, you can safely attach up to 20 SonicPoints to it and expect reasonable performance.
- Given throughput on SonicPoints only 20-22 Mbps at best – this is a limitation of the 802.11a and 802.11g and not the SonicPoint.
- If you are still experiencing throughput issues, please upgrade to SonicOS 4.0.1.0 or newer, as it contains several fixes that will help.
- Make sure your security zone (the default WLAN, or your own custom wireless zone) has the right settings – they might be blocking traffic for various reasons. The 'WiFiSec Enforcement' setting is enabled by default, and because of this it will not pass traffic in the clear until this feature is disabled.
- If the SonicPoints are not acquiring, check DHCP scopes; they might be off, or missing. entirely.

- It is NOT advisable to use the same SSID for the 802.11bg and the 802.11a radios, as clients with tri-band cards may experience disconnect issues – name them separately.
- Stuck in provisioning mode? Unplug, clear from config, reboot and plug back in.
- The most current version of the SonicPoint Administrator's Guide can be found here: http://www.sonicwall.com/downloads/SonicPointAdministratorsGuide.pdf.
- All versions of SonicOS Enhanced after version 3.5 no longer contain the SonicPoint firmware image, and in order for a SonicPoint to be discovered and provisioned, the UTM appliance must
- Please note that SonicPoints have a 'Standalone Mode' which they will transition to if they can't find a SonicWALL UTM appliance. If you have more than one SonicPoint, you may have issues as all of the SonicPoints will revert to the same default IP address of 192.168.1.20/24.
- When troubleshooting wireless issues, logging, Syslog, and SNMP are your friends – SonicWALL's Global Management System (GMS) package can centralize all of these for all of your SonicWALL devices, regardless of location. A free alternative is Kiwi's Syslog Daemon, which can accept Syslog streams and SNMP traps from all SonicWALL UTM appliances. The most current version can be found here: http://www.kiwisyslog.com/kiwi-syslog-daemon-download/.
- Check the network cabling. Is shielded or unshielded TP cable being used?

Resetting the SonicPoint

The SonicPoint has a reset switch inside a small hole in the back of the unit, next to the console port.
You can reset the SonicPoint at any time by pressing the reset switch with a straightened paper-clip, a
tooth pick, or other small, straight object.

The reset button resets the configuration of the mode the SonicPoint is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the SonicPoint is operating in, and the amount of time you press the reset button, the SonicPoint behaves
in one of the following ways:

- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint.

- Press the reset button for **more than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.

- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint.

- Press the reset button for **more than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.

Switch Programming Tips

Sample HP ProCurve switch commands (per-interface)

- name 'link to SonicPoint X'
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (note: global command)
- speed-duplex 100-half (note: only if you are seeing FCS errors)
- spanning-tree xx admin-edge-port (note: replace xx with port number)
- mdix-mode mdix

Sample Cisco Catalyst switch config

Any Cisco POE Switch: On the connecting interface/port, issue the command 'Power inline static 10000'

2900/3500-series:
1. On the connecting interface/port, issue the command 'spanning-tree portfast', which will greatly reduce the time STP is performed on the interface/port.
2. If you are using a 2950 or 3550 switch, issue the command 'switchport mode access' to disable trunking on the interface/port.
3. On the connecting interface, issue the commands 'speed 100' (or 'speed 10') and 'duplex full' (or 'duplex half') to lock the speed and duplex of the port.

2948/2980/4000/4500/5000/5500/6500-series running CatOS:
1. On the connecting interface/port, issue the command 'set spantree portfast __/__ enable' (fill in first blank with module number, and second blank with port), which will greatly reduce the time STP is performed on the interface/port.
2. On the connecting interface/port, issue the command 'set port channel __/__ off' (fill in first blank with module number, and second blank with port range), which will disable EtherChannel (PAgP) on the interface/port.
3. On the connecting interface/port, issue the command 'set port trunk __/__' (fill in first blank with module number, and second blank with port), which will disable trunking on the interface/port.
4. On the connecting interface/port, issue the command 'set port speed __/__ 100' (fill in first blank with module number, and second blank with port), which will lock the speed to 100Mbps on the interface/port (you can also lock it to 10Mbps if you wish).
5. On the connecting interface/port, issue the command 'set port duplex __/__ full' (fill in first blank with module number, and second blank with port), which will lock the duplex to full on the interface/port (you can also lock it to half duplex if you wish).

SPECIAL NOTE: Cisco switches running CatOS 5.2 and newer have a special macro command called 'set port host __/__' that sets the interface/port for portfast, disables trunking, and disables EtherChannel. You will still have to manually set the speed/duplex for the port(s), however.

1900/2820-series:
1. 1900-series switch have portfast enabled by default on the 10mbps ports and disabled on the 100 Mbps ports. If you are using the 100mbps ports to connect to a SonicWALL device, issue the command 'spantree start-forwarding', which will greatly reduce the time STP is performed on the interface/port.

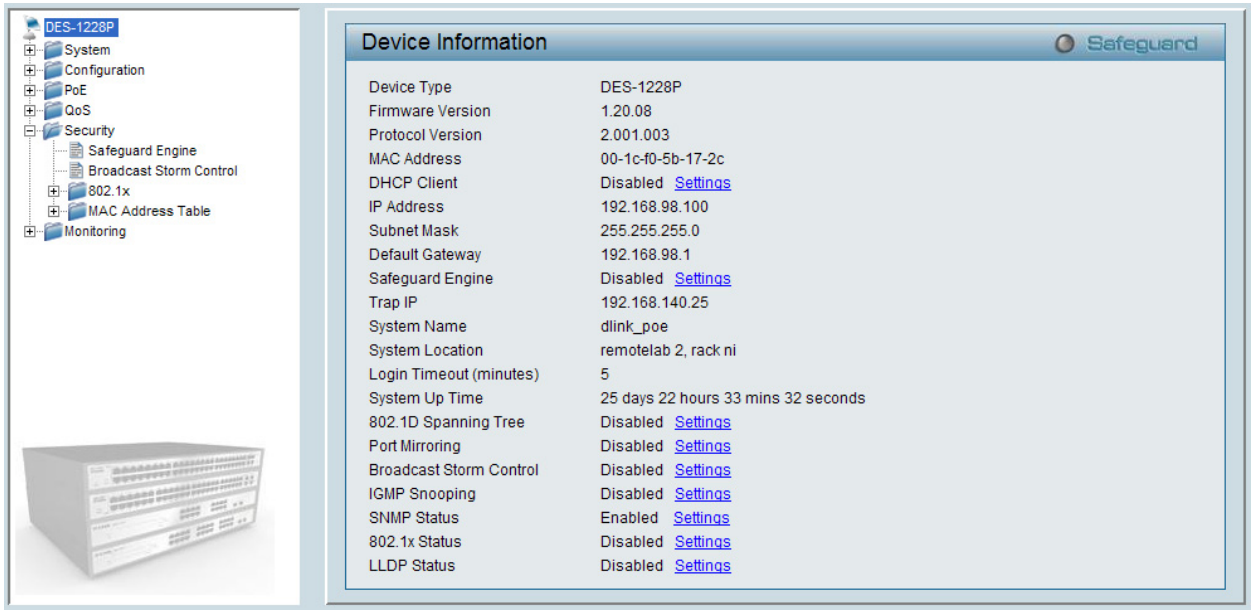
Sample Dell switch config (per interface)

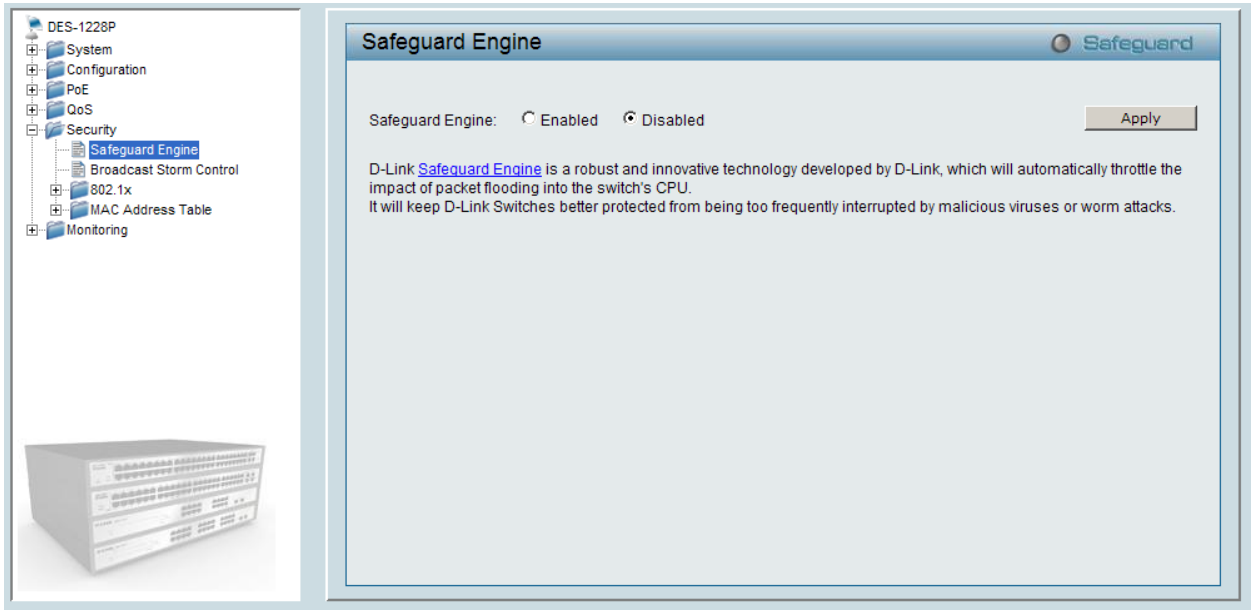
- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (note: only if you are seeing FCS errors)
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

Sample D-Link switch config

The D-Link PoE switches do not have a CLI, so you will need to use their web GUI. Please note that D-Link recommends upgrading to Firmware Version 1.20.09 if you are using multicast in your environment.

Please disable spanning-tree, broadcast storm control, LLDP and the Safeguard Engine on the switch before adding SonicPoints to the switch, as all may impact their successful provisioning, configuration, and functionality.


DES-1228P
System
Configuration
PoE
QoS
Security
Safeguard Engine
Broadcast Storm Control
802.1x
MAC Address Table
Monitoring
Device Information
Safeguard
Device Type DES-1228P
Firmware Version 1.20.08
Protocol Version 2.001.003
MAC Address 00-1c-f0-5b-17-2c
DHCP Client Disabled Settings
IP Address 192.168.98.100
Subnet Mask 255.255.255.0
Default Gateway 192.168.98.1
Safeguard Engine Disabled Settings
Trap IP 192.168.140.25
System Name dlink_poe
System Location remotelab 2, rack ni
Login Timeout (minutes) 5
System Up Time 25 days 22 hours 33 mins 32 seconds
802.1D Spanning Tree Disabled Settings
Port Mirroring Disabled Settings
Broadcast Storm Control Disabled Settings
IGMP Snooping Disabled Settings
SNMP Status Enabled Settings
802.1x Status Disabled Settings
LLDP Status Disabled Settings


DES-1228P
System
Configuration
PoE
QoS
Security
Safeguard Engine
Broadcast Storm Control
802.1x
MAC Address Table
Monitoring
Safeguard Engine
Safeguard
Safeguard Engine: Enabled Disabled
Apply
D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU.
It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

Contacting SonicWALL

If you require technical assistance for your SonicWALL UTM appliance or SonicPoint, check these online SonicWALL resources:

The support site: http://www.sonicwall.com/us/Support.html

The interactive online Knowledge Portal:
http://www.nohold.net/noHoldCust22/Prod_3/Articles53234/sw_launch_frames.html

If you cannot find the information you need, contact SonicWALL telephone support at one of these numbers:

North America Telephone Support
U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Australia	+ 1800.35.1642
Austria	+ 43(0)820.400.105
EMEA	+ 31(0)411.617.810
France	+ 33(0)1.4933.7414
Germany	+ 49(0)1805.0800.22
Hong Kong	+ 1.800.93.0997
India	+ 8026556828
Italy	+ 39.02.7541.9803
Japan	+ 81(0)3.5460.5356
New Zealand	+ 0800.446489
Singapore	+ 800.110.1441
Spain	+ 34(0)9137.53035
Switzerland	+ 41.1.308.3.977
UK	+ 44(0)1344.668.484

Note: If you find that the number appropriate to your geographic region does not work, please visit http://www.sonicwall.com/us/support/3001.html for the latest technical support telephone numbers.

More Information on SonicWALL Products
Contact SonicWALL, Inc. for information about SonicWALL products and services at:
Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408) 745-9300

Author: dparry@sonicwall.com
Prepared by SonicWALL, Inc
Version 1.3, Updated January 2008