WHITE PAPER

Unfiltered Church Access

BUT SCHOOL REMAINS FILTERED

ComSifter®
protect web users now!

Article Update: September 2010

IN THIS DOCUMENT

OVERVIEW

The church, with associated school that shares an Internet connection, wants the school filtered, but open access to church parishioners and personnel.

Note: This workaround **does not work** with the following legacy ComSifter units: CS-1, CS-8

ISSUE DESCRIPTION

The school computers are setup properly, using the ComSifter as a filtering gateway. Additionally, all school computers are using ComSifter user authentication and network administrators are able to see usernames on the ComSifter. For this feature to work properly, port 113 on each computer must be open and ComsifService or ComsifConnection (deprecated) must be installed on each client computer. While school computers are typically static and are seldom changed, the opposite is the case for church access, where parishioners bring in laptops or other wireless devices.

The issue is the network administrator does not want to be burdened by installing ComsiftService and opening the firewall port on every parishioner's computer.

SOLUTION

In an ideal world, the church would have its own physical connection to the Internet. If this is not possible due to cost or physical plant issues, Comsift suggests the following solution.

Note: Before proceeding be sure that you understand the security implications of allowing non-controlled computers on your network. You will not know the Virus/malware status of the computers being connected to your network, nor will you be able to monitor what the computers are accessing.

It is assumed that the church computers will be connecting wirelessly. This document will outline how to setup one wireless device. Your physical requirements may require more than one device. If so the setup will be the same, but the IP addresses will change.

You will need a wireless router that fulfills the requirement of your church computers. It is strongly suggested that only wireless routers supporting WPA2 Personal/AES security be used, as all other security methods are trivially hacked.

Wireless Router Setup

- The WAN side of the wireless router should be set to a static IP on the same network as the ComSifter. For instance, if the ComSifter were on `192.168.1.x` then you would want the wireless router to be set to a static IP of `192.168.1.y`.
- Set the LAN side of the wireless router to a non-routable network range that is not used on your network. For example `10.0.1.1`.
- Turn on DHCP Server on the wireless router and ensure that you have enough available addresses on the `10.0.1.x` network.
- Set the wireless router security protocol and pass codes to your requirements.

CONTINUED

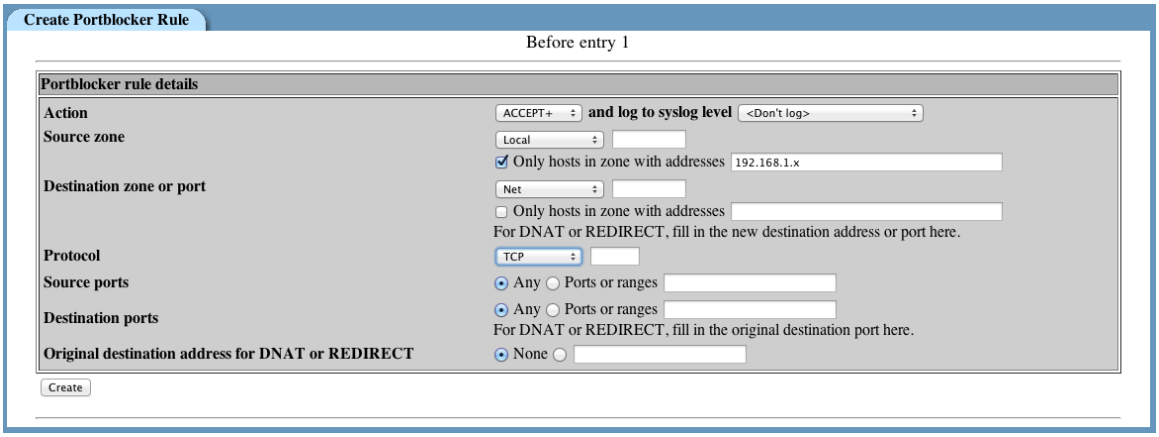
Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com

If all is set up properly, you should now be able to connect to the wireless router and receive an IP address in the `10.0.1.x` range. You should also be able to ping devices on your `192.168.1.x` network. You will not be able to reach the Internet, as the ComSifter is unable to identify your computer due to the wireless router being between your client computer and the ComSifter.

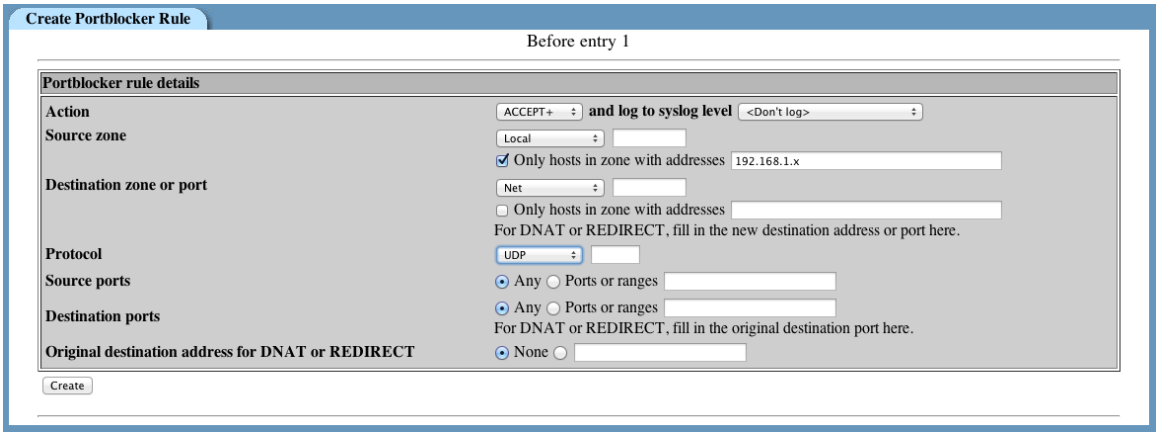
Allowing the Wireless Router Internet Access

Two (2) new rules need to be added to the ComSifter Portblocker/Firewall. This rule will allow any packets from the wireless router WAN IP address to go through the ComSifter without identification or filtering.

- On the ComSifter, go to Network > Portblocker Advanced (CS-1B, CS-8B) or Firewall Advanced (CS-8 Pro, CS-8 Pro NS) > Portblocker (or Firewall) Rules.
- On the first rule (first row), find the small blue UP arrow and click on it. This will open the Create Rule dialog, and save the rule at the top of the list when created.
- Configure the two (2) rules as shown below, substituting the shown IP with the static IP you have given the WAN side of the wireless router. (Be sure to use an ACCEPT+ rule). Note: The two rules are identical, except for the Protocol—one being TCP, and another being UDP.
- After creating the rules, click the Apply Configuration button on the main Portblocker/Firewall page. Client computers accessing the wireless router should now be able to reach the Internet—unfiltered and not identified.



TCP rule providing Internet Access to the Wireless Router



UDP rule providing Internet Access to the Wireless Router

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com