Using Blocking/ Filtering Technologies

As Part of an Overall School Internet Safety Policy

Filtering can play a role in protecting children from the consequences of inappropriate risk behaviors while they learn how to behave appropriately online. It is not the solution to all inappropriate Internet behaviors and should be viewed as only one aspect of a comprehensive Internet education program. For example, it may be perfectly appropriate for a student to access a research article but certainly not appropriate for him or her to plagiarize that article for a term paper. No filter can determine how the student intends to use the content accessed.

The first challenge in filtering is determining what material should be filtered. For some content, the decision is easy: gambling or pornography, for example. But should sex education materials also be filtered? Should any site that includes a profanity be blocked? Is every book that contains profanity unacceptable? What about a nude painting or a photograph of Michelangelo's *David*? Will filtering for students in a 3rd-grade classroom be different from filtering for 12th graders? Will game sites be blocked? What about educational games? Facebook? These are policy decisions that schools must address prior to implementing filtering technology.

Once these decisions are made, in an ideal world, the school's Internet filter would block every piece of content judged to be inappropriate and allow every piece of content that is deemed appropriate. But filtering technology is not perfect. In addition, the Internet is naturally resistant filtering and censorship. As John Gilmore* of the Electronic Frontier Foundation puts it, "The Net interprets censorship as damage and routes around it." But filtering technologies have evolved and improved, becoming more sophisticated than in the past.

Evaluating a Filter Technology

When considering a filtering technology, you must evaluate three issues: frequency of filtering errors, resistance to circumvention, and cost of implementation:

- *Frequency of filtering errors.* Sometimes the filter will fail to block content that should be blocked (false positives), while other times it will block content that should not be blocked (false negatives). Minimizing error is an important goal of effective Internet filtering.
- *Resistance to circumvention.* Sometimes users' access of inappropriate material is unintentional. But they may attempt to circumvent your filtering technology. This can quickly develop into a technological arms race.
- *Cost of implementation.* Filtering technologies can be expensive. Upfront costs include licenses for software and hardware purchases. But there may also be hidden costs: staff time needed to implement and maintain the filter, performance costs to the network, and time or information lost by users due to false positives. Schools should purchase a system that performs all desired functions for the least possible cost.

BY RUDY SCOTT AND ANNETTE MELGOSA

Types of Internet Filtering

Internet filters work by examining and analyzing network traffic, and in some cases modifying it. Filters can be classified by the type of traffic they analyze and modify. Internet filters work in concert with other aspects of a network security system such as firewalls and anti-malware systems. Two common types of filter are discussed below.

DNS Filters

The backbone of the Internet is the Domain Name System, which ensures that Website names that look familiar to users (e.g., google.com, wallawalla.edu, adventist.org) are translated into Internet addresses that are meaningful to the routers that circulate data around the Internet. This process is called "domain name resolution" and can be used to implement Internet filtering. A domain name server that has been alerted to Web-sites that must be blocked can refuse to provide the Internet address of the blocked site to the client. A client might instead be redirected to another page—for example, one that provides information about why the site is blocked.

DNS filtering is usually easy and quick to implement: Simply change the DNS server used by your school's computers. This can often be done from a central location such as a router/gateway or through Active Directory group policy. DNS-based filtering can be readily hosted offsite and often is, meaning you don't need any special hardware or software to implement it. Another benefit of DNS hosting is that it may also automatically block connections to sites known to contain malware. For more information on implementing DNS filtering, see the section on OpenDNS filtering for schools.

DNS filtering works on the site level, so it is not possible to block a single page of a Website while allowing other pages. This can prevent access to pages that should not be blocked. DNS filtering systems generally cannot be configured to provide different filtering levels for different users. Thus, 3rd graders and 12th graders—and even faculty—may have to function within the same filtering rules. OpenDNS (see Section II) provides a paid service that can circumvent this limitation.

If countermeasures have not been taken, it is relatively easy for a user with administrative privileges on a computer to change its settings to use a different DNS server in order to circumvent filtering. Administrators can use group policy or operating system security settings to prevent users from modifying DNS settings on school-owned computers, or configure a local DNS server and their network firewall to force users to use the local server.

Fighting circumvention can quickly consume a lot of resources and increase the cost of implementation. Schools should decide on the appropriate level of deterrence and avoid getting caught in a technological arms race with circumventers. Such a race may be impossible to win.

Remember, filtering is only one element of an overall In- ternet education policy. An effective technology use plan that includes specific consequences and is consistently enforced may be more effective at deterring circumvention (and less expensive) than technological measures.

Remember, filtering is only one element of an overall Internet education policy. An effective technology use plan that includes specific consequences and is consistently enforced may be more effective at deterring circumvention (and less expensive) than technological measures.

HTTP Filtering

HyperText Transport Protocol (HTTP) is the protocol through which Web pages travel. Another method of filtering involves using "proxy servers" or "Web proxies," which analyze and possibly modify HTTP content as it travels between school computers and the Internet. To implement HTTP filtering, Web traffic must be redirected to travel through the proxy server. This can be done by modifying settings on each client unit directly or, in a Windows domain, through Active Directory group policy.

Alternately, a "transparent proxy" can be set up in order to allow a proxy server to operate without modifying client settings. Using a transparent proxy may reduce implementation costs by avoiding client configuration. But transparent proxies cannot effectively filter SSL-encrypted traffic, so students can bypass a transparent proxy that blocked Facebook, for example, by simply going to https://facebook.com (which enables SSL encryption) rather than going to http://facebook.com.

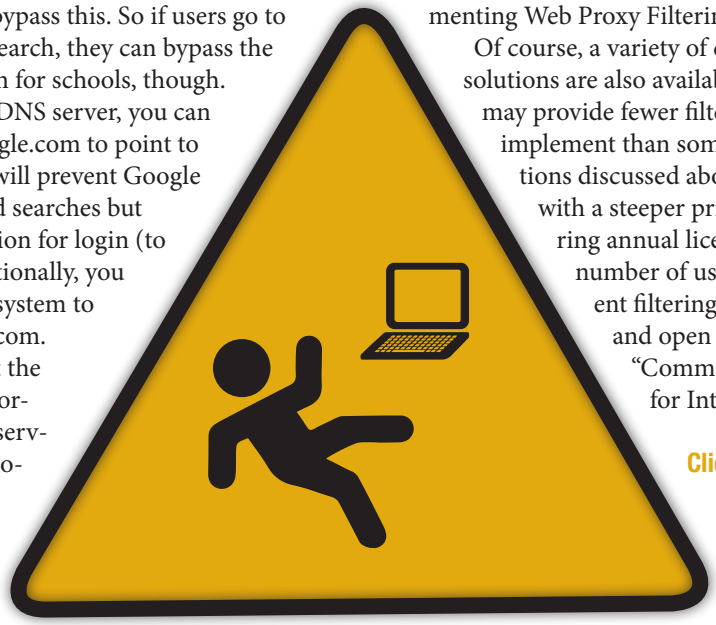
Proxy servers can use complex rules to implement filtering. This includes filtering based on domain name (used in DNS filtering), but also inspecting the content of a page. For example, a content filter might search for certain keywords which would indicate that a page should be blocked. Proxy servers can also be configured to apply varying rules to different machines or users, which means that the school can set up different filtering configurations for 3rd graders than for 12th graders or faculty.

Technology has not, however, reached the point where filters can analyze images. To assess whether or not an image

is inappropriate, a filter has to rely on the surrounding textual context. While this is often effective at blocking inappropriate images, it poses a particular problem for image search sites. Why? Because search engines like http://images.google.com return an array of images with very little surrounding text. Therefore, filtering proxy servers can't rely on the contextual text to identify which images may be inappropriate.

Many search engines, including Google, implement their own filtering technologies, and in some cases, a proxy server can be configured to work with these technologies. For example, in Google's "safe search" mode, proxies can be configured to append "&safe=strict" to every Google search.

However, this doesn't solve all the problems of access to undesirable content. Because SSL encrypts traffic, secure (SSL) searches (using https) will still bypass this. So if users go to https://google.com to do their search, they can bypass the filter. Google has a nifty solution for schools, though. If your school operates its own DNS server, you can create a CNAME (alias) for google.com to point to "nosslsearch.google.com". This will prevent Google from performing SSL-encrypted searches but still provide SSL secure encryption for login (to protect users' passwords). Additionally, you should configure your filtering system to block https://encrypted.google.com.



Proxy servers may also affect the school's computer network performance, particularly if its proxy server does not have sufficient memory and/or processing power for the number of users. However, proxy servers can also, in some cases, improve network performance by caching frequently used pages, so that requests for these pages return local data from the proxy server without having to go out to the Internet. Most proxy servers include options for configuring local Web caching and other network functions like traffic shaping (creating search engine-optimized links and shortening Uniform Resource Locators [URLs]).

Linux servers are one popular way to implement Web proxies. A popular open-source proxy server called Squid (http://www.squid-cache.org/) can work with open-source filtering software, DansGuardian (http://dansguardian.org/), to provide a free filtering solution for schools. The original developer of DansGuardian now operates a company called Smoothwall (http://www.smoothwall.org), which provides both free and paid open-source, turn-key proxy server solutions. Commercial support is also available.

The North American Division's (NAD) Technology and Distance Education Committee (TDEC) has endorsed a Linux-based commercial proxy filter solution called ComSifter (http://www.comsifter.com), a hardware appliance with a filtering proxy preinstalled as well as telephone and e-mail support. ComSifter also includes a client that allows users to login and identify themselves so as to get different filtering configurations.

My favorite way to implement proxy server technology is with another open source Linux distribution called ClearOS (http://www.clearfoundation.com/). ClearOS includes Squid and DansGuardian and a nice Web interface that makes them easier to configure and administer. It also includes a variety of other Linux tools including a Web and e-mail server, a file server, Internet firewall, and more. You can turn the tools you want to use on and off, so you only have to use components you need. ClearOS comes in both free and paid versions, and ClearOS also sells monthly updates for DansGuardian blacklists (lists of sites to be blocked). For more information on setting up a ClearOS proxy server, see Section III, "Implementing Web Proxy Filtering with ClearOS."

Of course, a variety of quality commercial filtering solutions are also available. Many of these solutions may provide fewer filtering errors and be easier to implement than some of the open-source solutions discussed above—but they may also come with a steeper price tag, and usually a recurring annual licensing fee, often based on the number of users. For a list of some different filtering options—both commercial and open source—refer to Section IV, "Commercial and Open Source Tools for Internet Filtering."

Client-Side Filtering

In this article, we have focused on server-side filtering solutions. Server-side filtering is usually more cost effective and more difficult to bypass than client filtering for schools. Parents often ask me about solutions for filtering at home. Client filtering (where a program on the local computer does the filtering) is a good solution when there are a small number of computers to be filtered. I often recommend K9 by BlueCoat (http://www1.k9webprotection.com/) to parents because it has both server and client-side filtering solutions, including a free client-side solution for home use. BlueCoat also provides commercial proxy filtering and security solutions for schools and enterprises.

Proxies: A Double-Edged Sword

While proxy servers can provide filtering services, they are also a powerful tool for circumventing filtering. A public proxy server can provide content from sites all over the Internet to a user inside your network but make it appear that all the content is coming from one site, the proxy. If the proxy site is not blocked, the filtering system allows whatever it provides, which could come from anywhere—including blocked sites. Most filtering systems include configuration options to block proxy servers. But new proxies are constantly being created, so keeping up with them is a real challenge.

Worse yet, a circumventer who is technically savvy may set up his or her own private proxy server. This proxy won't be known to the filtering community at large, so it won't show up on blocked lists. This type of circumvention is extremely difficult to thwart. It requires careful monitoring of the network and traffic pattern analysis.

Firewalls and Peer-to-Peer File Sharing

While DNS and HTTP are the basics of Web browsing, they are only two of many application protocols that travel over the Internet. Another category of protocols that can be particularly problematic for school networks is peer-to-peer file sharing (P2P).

P2P is so named because files are exchanged between users' computers directly without a server hosting the files. Because of its decentralization, P2P has become very popular for sharing illegal content such as pirated music, videos, and pornography. A high percentage of P2P files are also infected with viruses. Additionally, because P2P is often used to share large files (like music and videos), it can quickly consume Internet bandwidth, choking out the school's other Internet-based activities. Napster, Gnutella, and Kaaza were early P2P-sharing programs. But the most popular P2P protocol today is called BitTorrent. It is estimated that P2P may constitute as much as 40 to 70 percent of all Internet traffic.

Of course, P2P can be used for legitimate purposes. But because of the aforementioned problems, it is frequently advantageous for a school to block P2P traffic. A firewall is a tool (software or hardware) designed to block certain types of traffic from passing through it. Simple firewalls may categorize traffic based on the port (number assigned to communication packets sent through the Internet to help categorize and identify it). But P2P software often uses a wide range of ports and may dynamically shift which ports it uses. More sophisticated firewalls analyze the packets of data coming through to determine their protocol and contents (without relying on the port). These firewalls are sometimes called Layer 7 filters or "stateful packet inspectors" (SPI). These are the best tools to combat peer-to-peer file sharing and are often combined with Web proxies.

School Internet Safety Policy

As mentioned earlier, filtering should constitute only one aspect of a school's Internet education policy, which should also include teacher supervision, a detailed acceptable-use policy with clear consequences, and training and education about appropriate and ethical use of information technologies, including the Internet.

If a school chooses to use filtering as part of its overall policy, DNS filtering and proxy solutions can be used together. Offsite DNS filtering can be used to block items that no one at a school should be visiting, like pornography Websites. Proxy servers can be used to block more selectively. For example, you might block Facebook in a computer lab during class time but allow it on student laptops during lunch. Or you might block YouTube for students but allow it for faculty members. Firewalls can be used to block P2P traffic and help prevent circumvention of Internet filtering.

Nonetheless, schools must recognize that no filtering system is perfect. No matter how sophisticated, these systems can be circumvented by technology-savvy users. It may be prudent to avoid getting into a technology battle with students and instead focus on educating users and encouraging them to comply with use policies. (See the main article in the February/March 2013 issue of the Journal for more information about Internet safety education.)

Complying With School Policy

As mentioned above, education is the best way to encourage compliance with school Internet policy. Including student representatives in the committee tasked with designing the school's Internet-use policy is another good way to engender compliance. Students can contribute their ideas to the discussion and report back to their classmates about the process and outcomes. Once the policy is set up, a good way to encourage compliance is with a Computer Use Contract. A sample contract used by Walla Walla Valley Academy in College Place, Washington, can be found here: http://bit.ly/W9c0A1.

SECTION I Summary

Filtering can be one valuable component in a comprehensive Internet safety policy. DNS and Web proxies are two methods of filtering that have unique advantages and disadvantages. The two methods may also be used together. Web filtering should be used in combination with a firewall and other anti-malware measures. A variety of options, both commercial and open-source, are available for implementing effective filtering methods. However, no filtering method is perfect. Filters make mistakes and can be circumvented. Internet safety and education should be about much more than just filtering.

---

* John Gilmore, quoted in Philip Elmer-Dewitt, "First Nation in Cyberspace," *Time International* 49 (December 6, 1993):49: http://www.chemi.fu-berlin.de/outerspace/internet-article.html. Accessed August 13, 2012.

Implementing Open-DNS Filtering

While Internet filtering alone cannot protect students from all inappropriate content, it is an important component in a school's Internet use and safety policy. This article will examine, in some detail, how to implement OpenDNS to provide Internet filtering and security for a small school network. It will focus on client computers running Microsoft Windows and using a TCP/IP v4 network.

OpenDNS (http://opendns.com)

OpenDNS provides services for Domain Name Service (DNS)-level Web filtering. Founded in 2005, the company now provides services to a third of United States public schools. OpenDNS is easy to implement and to use, and its basic services are free. If you are looking for an easy, quick way to get started with filtering, OpenDNS is a good choice.

Implementing OpenDNS: A Step-by-Step Overview

- **Step 1:** If you have an internal DNS server, configure it to forward DNS requests to OpenDNS and skip to Step 3. Otherwise, proceed to Step 2.
- **Step 2:** If you have a Dynamic Host Configuration Protocol (DHCP) server, configure it to use OpenDNS servers. Otherwise, manually configure each workstation to use OpenDNS.
- **Step 3:** Determine whether you have a static external IP address (recommended) or dynamic address.
- **Step 4:** Create an OpenDNS account, and configure your custom filtering settings.
- **Step 5:** Consider OpenDNS Enterprise or Umbrella.
- **Step 6:** Take measures to prevent users from bypassing your filter.
- **Step 7:** Maintain and monitor your OpenDNS configuration.

Let's look at each of these steps in more detail. OpenDNS also provides a nice overview of this process and more detailed directions at: http://www.opendns.com/support/category/2/

Configuring Your Computers to Use OpenDNS

How you configure your computers to use OpenDNS depends on how your network is set up. Your ultimate goal is to get your computers to use the OpenDNS servers to resolve DNS requests. Two OpenDNS servers are: 208.67.222.222 and 208.67.220.220.

Step 1: Configure Your Internal DNS Server to Forward Requests to OpenDNS

If you use a Microsoft server and Microsoft Active Directory, you probably host your DNS internally. In this case, you'll need to configure it to forward unresolved requests to OpenDNS. You'll do that by adding the two addresses above to the Forwarders tab on the configuration page of your Microsoft DNS server.

BY RUDY SCOTT AND ANNETTE MELGOSA

You may have another type of internal DNS server. OpenDNS has detailed instructions for a variety of server types here: https://store.opendns.com/setup/server/

If you do not have an internal DNS server, proceed to Step 2. Otherwise, skip to Step 3.

Step 2: Configure Your DHCP Server (or Each Workstation) to Use OpenDNS

During this step, you will configure your workstations to use OpenDNS' servers either directly or through a DHCP server. If you have a DHCP server, you will only need to configure it and will not need to configure each workstation as the DHCP server will provide this information to the workstations. If you do not have a DHCP server, you will need to configure each workstation to use the OpenDNS servers. If you have an internal DNS server that you configured in Step 1, skip this step and proceed to Step 3.

If you don't use internal DNS but do use DHCP, you will need to locate and configure your DHCP server. A DHCP server provides each computer with an internal network address and some other configuration information (including the DNS server to use). In many small networks, a single device (small box) provides all the following services: Internet gateway/router, DHCP server, and Wireless Access point. Most combination gateway/router/DHCP servers have a Web interface for configuration. OpenDNS has detailed instructions for many different routers at https://store.opendns.com/setup/router/

Configure Workstations Manually

In some networks, DHCP may not be used—rather, each computer is configured manually. This makes it a little harder, as you will have to configure each unit to use OpenDNS rather than doing the configuring in one place (on the DHCP server). OpenDNS has instructions for different operating systems here: https://store.opendns.com/setup/computer/

Regardless of what method you have used, you can test whether you have successfully configured your computers to use OpenDNS by visiting this site on one of your computers: http://welcome.opendns.com/

Once you have successfully configured your network to use OpenDNS, you will need to configure OpenDNS to do the type of blocking and filtering that you want. Before you can do that, you must determine whether you have a static or dynamic external address.

Step 3: Determine Whether You Have a Static or Dynamic External Address

In most cases, Internet traffic from the school network travels through a gateway and is routed with an external address assigned by your Internet Service Provider (ISP). If your ISP provides you with a static configuration, this address stays constant. If you have a dynamic configuration, this address may change from time to time.

OpenDNS works best with a static IP address, but it can also be configured to work with a dynamic address. If you have a dynamic IP address, you'll need to follow the additional steps described here: http://www.opendns.com/support/article/61/

When you visit the OpenDNS Website, the address you are coming from will be displayed just beneath the logo at the top left. From a school network computer, go to OpenDNS.com to determine your IP address.

You can also allow or block specific domains. For example, you may want to block Facebook while allowing some other social network sites. If so, you can choose *Always block*, then enter *facebook.com* and *add*. Changes made to this page take a few minutes to take effect.

Step 4: Create and Configure Your OpenDNS Account

Next, you need to set up an account with OpenDNS. I recommend that you begin with a free OpenDNS Premium account here: https://store.opendns.com/get/premium-dns/ At a later time, you may want to upgrade to an OpenDNS Enterprise account as discussed in Step 5.

Once you have set up your account, you're ready to customize the filtering. Go to the **Settings** tab and select your network. Here you can choose from three defined filter settings: *High, Medium,* and *Low*; or choose *Custom* (recommended), and individually select the categories you want blocked. Keep in mind when choosing categories to block that the filter does not understand context. For example, you might think "violence" or "weapons" is a category you want to block (and it may be), but keep in mind that this may hamper a student researching World War II, for example.

You can also allow or block specific domains. For example, you may want to block Facebook while allowing some other social network sites. If so, you can choose **Always block**, then enter **facebook.com** and **add**. Changes made to this page take a few minutes to take effect.

Step 5: Consider OpenDNS Enterprise or Umbrella

You may want to consider some of the premium settings OpenDNS can provide. OpenDNS now provides "Insights," which integrates with your active directory network. This setting allows you to do the following:

1. Customize filtering for specific users or groups. For example, you may wish to block Facebook for students, but allow it for faculty.

2. Track down malware to an individual computer. OpenDNS Umbrella is a new service that allows using

Library at Friedensau Adventist University Germany (Courtesy of Theologische Hochschule Friedensau).

OpenDNS filtering with mobile devices, such as laptops, tablets, or smart phones, even if they are operating outside of your network. Contact OpenDNS for more information about OpenDNS Enterprise or OpenDNS Umbrella or for pricing.

Step 6: Take Measures to Prevent Users From Bypassing Your Filter

OpenDNS filtering can be bypassed by simply reconfiguring computers to use another DNS server. However, you can do some things to prevent this. If you have an internal DNS server and a firewall, you can block other computers from contacting DNS. DNS traffic usually uses port 53, so you can configure your firewall to block port 53 for all traffic except that which comes from your internal DNS server. Be sure to remember to create an exclusion for your internal DNS server; otherwise, you will not be able to use the Internet!

Savvy students may be able to circumvent this by using another port. If your firewall supports stateful packet inspection (SPI), you can configure it to block DNS traffic no matter what port it uses.

For networks using Microsoft Active directory, you can also use **Group Policy**. You can configure a group policy to set the DNS on every workstation manually (either to an internal DNS server or to OpenDNS). More information is available here: http://www.grouppolicy.biz/2010/04/group-policy-setting-of-the-week-22-dns-servers/

Step 7: Maintain and Monitor Your OpenDNS Settings

The OpenDNS dashboard allows you to create a number of useful reports. It will also notify you when you log in of malware activity detected on your network. If you have the Enterprise Insights package (paid version), it will even tell you which computers are infected. It can also give you information about overall traffic and what sites your users are visiting (or having blocked). It's a good idea to log in to your dashboard and review these reports periodically. The dashboard can't do everything, however—for example, it will not be able to tell you if your filtering system is being bypassed.

Remember, if your external IP address changes, you'll need to update the address in the OpenDNS dashboard.

SECTION II Summary

OpenDNS is a useful tool for managing access to Internet content as well as detecting malware and botnet activity within your network. It does not replace your antivirus software or firewall, but it is a useful tool for small schools in managing Internet use and protecting students.

Using ClearOS Web Content Filtering

OpenDNS provides Domain Name System (DNS) content filtering. But DNS filtering has limitations because it looks only at the name of a site, not its content, in order to determine whether the site should be blocked. Another common Web content filtering alternative is a Web proxy server that examines Web content and requests before sending them on to the end user. DansGuardian is a content filter that works with the Squid Web proxy. These are both open-source projects that together can implement Web proxy filtering.

We will look at how ClearOS can be used to implement a DansGuardian/Squid filtering and firewall solution. ClearOS is a comprehensive server solution that bundles a number of open-source projects and features into a single unified package. ClearOS includes modules containing preconfigured versions of DansGuardian and Squid. (Other open-source firewall and proxy server packages include Untangle Lite, Smoothwall Express, IpCop, and eBox Platform.)

ClearOS sells subscriptions to updated filter definitions and includes a number of other functions useful to a small school network, such as a configurable firewall, file and printer server, and e-mail server. In this article, we'll discuss installing ClearOS as your router/gateway and configuring the network, content filter, and firewall modules. ClearOS includes many other features. To learn more, visit: http://www.clearcenter.com

This tutorial is more advanced than the OpenDNS tutorial in Section II and assumes some knowledge of Internet Protocol (IP) networking.

- **Step 1**: Decide Whether ClearOS Is a Good Fit for Your Network.
- **Step 2**: Determine Which Version of ClearOS Is Right for You.
- **Step 3**: Choose the Hardware (or Virtualized Hardware) on Which You Will Run ClearOS.
- **Step 4**: Determine Your Network Settings.
- **Step 5**: Install the ClearOS Software.
- **Step 6**: Choose Whether to Use a Transparent Proxy.
- **Step 7:** Configure Your Content Filter.
- **Step 8:** Activate the Web Proxy and Content Filter.
- **Step 9:** Configure the Firewall.
- **Step 10:** Consider Other Features of ClearOS.
- **Step 11:** Monitor and Maintain Your ClearOS Server.

Step 1: Decide Whether ClearOS Is a Good Fit for Your Network

The first step in installing ClearOS is to confirm that you want to do so. Adding an HTTP (HyperText Transfer Protocol Overview) proxy filter and replacing your router/gateway is a much bigger change to your network than setting up DNS-based filtering.

Reasons you may want to add ClearOS:

- ClearOS includes an advanced firewall that supports stateful packet inspection (SPI).
- It can replace your existing hardware router.
- If you don't have a Windows Server, ClearOS can pro-

BY RUDY SCOTT AND ANNETTE MELGOSA

vide many of the same features of a Windows Server, including file and printer sharing and user authentication.

- ClearOS may actually improve network performance by providing local caching.
- ClearOS allows you to set up individual filtering groups and apply different rules to different groups (this requires some advanced configuration that falls outside the scope of this article, however).

Reasons you may not want to install ClearOS:

- ClearOS does not filter secure (https) traffic when operating in transparent mode.
- ClearOS with Squid may disrupt network software that does not support or is not compatible with an HTTP proxy server.
- Your hardware router may already have an adequate firewall.
- Once you have configured filtering, if your ClearOS server goes down, the Internet will be unavailable for all users.
- ClearOS may degrade performance, especially if you have limited Random-Access Memory (RAM) on your ClearOS server.

ClearOS is not a good choice for every network. But if you are looking for a single unified solution to provide a variety of network services, or need more sophistication than your consumer hardware router/gateway provides, ClearOS may be right for your school.

Step 2: Determine Which Version of ClearOS Is Right for You

ClearOS comes in three versions: ClearOS Community, ClearOS Professional, and ClearOS Box. ClearOS Community is the free and open-source version and what we'll be referring to in the remainder of this article.

You can read more about the differences here: http://www.clearcenter.com/Software/clearos-overview.html/

ClearBOX is a preconfigured hardware appliance running ClearOS Professional. You can learn more about ClearBOX here: http://www.clearcenter.com/Hardware/clearbox-hardware.html/

The major advantages of ClearOS Professional are:

- **The ability to connect/synchronize with a Microsoft Windows Active Directory server or with Google Apps.**
- **Very good anti-malware protection created by industry leader Kaspersky.**

Step 3: Choose the Hardware (or Virtualized Hardware) on Which You Will Run ClearOS

Once you have decided to install ClearOS, you will need to choose hardware on which to run it. The more users, the more powerful processor and memory you will need. For fewer than 50 users, an older Xeon processor with a small memory upgrade will generally work well. You can read more about recommended system requirements here: http://www.clearcenter.com/support/documentation/clearos_professional_6/user_guide/system_requirements/

Since having the ClearOS server become inoperable will mean no Internet for your users, you may also want to consider installing a RAID (Redundant Array of Independent Disks) array configured for high availability (RAID-1 mirroring, for example). The installer for the current version is nearly 700 megabytes, so you will also need a CD or DVD-drive, at least for installation.

One last consideration: Be sure the hardware you select is compatible with Red Hat Linux. You can find more information about compatibility here: http://www.clearcenter.com/support/documentation/clearos_professional_6/user_guide/compatibility/

This can be of particular concern with network cards. Since you are configuring this server as a router/gateway, you will need two network cards, one for the Internet Wide Area Network (WAN) interface, and one for the Local Area Network (LAN) interface. I recommend not skimping on networking hardware; keep in mind that this server will be working primarily with network traffic. Consider buying a name-brand network card such as 3COM or Intel.

Step 4: Determine Your Network Settings

When you install ClearOS, you will need to configure the two network interfaces, as the server will provide the gateway between (1) the Internet or WAN interface and (2) the LAN interface.

A detailed explanation of Internet Protocol (IP) and address spaces is beyond the scope of this article, so if you aren't comfortable with these concepts, you will probably want to consult an IT expert.

If you are replacing an existing router/gateway, you may be able to simply copy the WAN and LAN settings from the existing router. In many networks, the Internet (WAN) interface can be configured automatically via Dynamic Host Configuration Protocol (DHCP). For the LAN side, you will need to know an IP address and a subnet mask, which allows IP networks to be subdivided for security and performance reasons. Again, you may be able to copy this from your existing router.

If you are setting up a new network, you can choose an address block from the non-routable address space, for example: 192.168.99.1 with subnet mask 255.255.255.0. It is often considered a best practice to choose the first address in your address space for the gateway. Also, consider that if you later decide to allow outside users to access your network via a VPN (Virtual Private Network), you will need an address space that does not overlap with the connecting network.

Because of this, I try to avoid the spaces commonly used by home routers, such as 192.168.0.1/24, 192.168.1.1/24 or 192.168.2.1/24.

Step 5: Install the ClearOS Software

The first step to installing ClearOS software is to download the installation media—usually an ISO image for burning a DVD. But there are also special packages for virtual machine installation (if you use virtual servers in your network). You can find the downloads here: http://www.clearfoundation.com/Software/downloads.html/

If your hardware is 64-bit capable, I recommend the 64-bit ISO. Once you have downloaded the ISO, you will need to burn this to a CD or DVD (ClearOS is big, so make sure you have a 700 megabyte CD if you use a CD). If you don't already have software for burning an ISO, I recommend this free program: http://www.imgburn.com/

Once you have created a CD/DVD, you're ready to insert it in your computer and boot from it. You may need to configure the Basic Input/Output System (BIOS) to ensure that the computer can boot from the CD/DVD drive. Once you have booted, you can choose your preferred language and keyboard layout. This is a new install, so choose **Install** at the next prompt rather than **Upgrade**. Installing ClearOS will ERASE everything on the existing hard drive, so you will need to follow the instructions to confirm that you want to do this. Better yet, start with a new hard drive so you don't risk losing any data. Then choose "Gateway" mode, since you will be using this device as an Internet gateway with two network interfaces.

Now, you will need to configure these network interfaces using the information you gathered in the prior step. For the WAN interface, you can likely choose to use DHCP—but in some cases, you may need to configure a static WAN IP address, subnet mask, and gateway. For the LAN side, you'll also use the information gathered in the prior step and enter the LAN IP address (this will be the local address of the ClearOS server) and the subnet mask.

Next, choose a strong password, and store it in a secure location. You will need this password to configure the server later.

Now you can choose which modules to install. If you want to do filtering, you will need to include the Web Proxy Filter and the Content Filter Server. For my example here, I am also going to install DHCP and Caching DNS Servers, Intrusion Detection and Prevention, DMZ and 1-to-1 NAT Firewall, Multi-WAN Support, Bandwidth Manager, VPN – Point-to-Point Tunneling Protocol (PPTP) Server, and VPN – Internet Protocol Security (IPSec) Server. These give me some additional network functionality that I may find useful in the future. If you want this box to be a mail, Web, file, print, or database server, you can install additional modules here. If you think you might use a feature and you have plenty of hard drive space, go ahead and install it. You can always disable it in the control panel until you need it.

ClearOS will now install on your system with the options and modules that you have selected. This process may take a few minutes. Once finished, you can click **Reboot**, and you have a new ClearOS server ready to go!

Additional information and a nice video of this process are available here: http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/installation_wizard/

You can now connect your Internet feed to the WAN network interface and your local network to the LAN interface.

Step 6: Choose Whether to Use a Transparent Proxy

Whenever a proxy server is used, client computers send and receive Web information from the proxy, instead of directly from the Internet through the gateway. Therefore, the client computers must be configured to use the proxy. There are two ways to do this:

1. Configure each computer in your network to use the proxy. If you use a Windows Active Directory server, this can be done through group policy, but otherwise it is a little difficult because you have to make changes on every computer. Worse, some browsers (like Mozilla Firefox) do not use the system settings, so if you use this method, you will have to configure them manually to use a proxy. The same may be true for other software programs.

2. Use a transparent proxy, which basically intercepts requests destined for the gateway and reroutes them to the proxy. Transparent proxies are easier to set up; no configuration is required on the workstations. But they do have limitations. For example, transparent proxies cannot filter secure (https) traffic, and they are not compatible with all software.

If you choose to use a transparent proxy, use the directions in Step 8. If you decide not to use a transparent proxy, directions for configuring clients are listed below.

Windows 7: http://answers.oreilly.com/topic/675-how-to-configure-proxy-settings-in-windows-7/

Windows XP: http://www.ehow.com/how_2033238_configure-internet-explorer.html/

Step 7: Configure Your Content Filter

To configure the content filter, you first need to log into the ClearOS server's administration panel. To do this, go to a computer connected to your LAN and open a Web browser. In the Web browser address bar, enter the IP address you chose for the ClearOS server, followed by a colon and an 81 (this is the default port for the server's interface). For example, if your server address is 192.168.99.1, you would enter "https://192.168.99.1:81" in the address bar. You may get a security warning message from your browser because it does not recognize the security certificate provided by the server. This is normal because you have not purchased a security certificate for your server. Simply instruct the browser to proceed anyway (NOTE: In general, ignoring certificate warnings is NOT a good practice, but in this case, it is all right). Next you will log in by entering the username **root** and the password you chose during the installation.

This is the Web interface, which allows you to configure many aspects of the ClearOS server. You want to configure the content filter, so go to **Gateway**, then **Proxy** and **Filtering,** then **Content Filter**. On this page, you will see a variety

of options related to filtering. Of particular interest is the **Sensitivity** setting, which allows you to adjust the filter's sensitivity from "very low" (few sites will be filtered) to "very high" (many sites filtered). Clicking the **Edit** button next to the "Blacklists" category will allow you to select which categories you wish to block. You can also allow or block specific sites by clicking on **Edit** next to the **Site Lists** button. The **Phrases** button allows you to block sites containing specific phrases. Once you have the content filter configured, you are ready to move on to the next step. You can read more about configuring the content filter and watch a video here: http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/content_filter/

Advanced users may also configure DansGuardian directly. The forums are a good resource for more advanced configuration issues: http://www.clearfoundation.com/component/option,com_kunena/Itemid,232/catid,27/func,showcat/

Step 8: Activate the Web Proxy and Content Filter

Once you have configured the content filter, it is time to turn it on. To do this, start by clicking on Web Proxy. Now under **Web Proxy Mode,** change the option **Content Filter** from **Disabled** to **Enabled**. If you want to use transparent proxy mode, also change **Transparent Proxy** to **Enabled.** Finally, click on the **Update** button to activate your changes.

If everything has gone well, your content filter is now up and working!

For additional information on configuring your Web proxy server, visit: http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/web_proxy/

Step 9: Configure Your Firewall

Another great feature in ClearOS is the firewall. The firewall can be configured under **Network Settings**, **Firewall**. The "Incoming" and "Outgoing" sections allow you to set up standard firewall rules based on IP address and ports. You can also forward ports coming from the outside network to a machine inside your LAN under "Port Forwarding." Details on how to configure a firewall to secure your network are beyond the scope of this article—but a good rule of thumb is to open only ports and services that you absolutely need.

The **Protocol Filter** module provides stateful packet inspection (SPI). This can be extremely useful in blocking peer-to-peer sharing protocols. To block all peer-to-peer traffic, select **Peer-to-Peer** from the drop-down menu, then click on the **Block All** button. You also need to make sure the protocol filter is active by clicking on the **Start** button if it is stopped. You should also click on **Auto-start** so that the filter starts automatically whenever the server is restarted. Enabling the protocol filter requires additional system resources.

Step 10: Consider Other Features of ClearOS

You may wish to consider configuring additional functionality on your ClearOS server, which can provide a variety of services for your network including DHCP, DNS, file and printer sharing, Web server, database server, and other features. However, many IT professionals consider it a best practice to limit a server to a single role for security and stability reasons. You might consider installing additional ClearOS servers to provide other network functions. For more information on the features available in ClearOS, visit: http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/start/

Additionally, ClearCenter provides paid services supporting ClearOS. One such service is content filter updates. This service provides monthly updates to the blacklisted categories blocked by the filter, enhancing its effectiveness.

Step 11: Monitor and Maintain Your ClearOS Server

Your Web proxy server is now a critical component in your network. If the server becomes unavailable, your users will not be able to access the Internet, so it is important to monitor and maintain the server. The **System** tab will allow you to back up the server settings (but not data). Be sure to regularly back up important data, too, and store copies in a safe location.

In the **Reports** section, there are a variety of reports including a section for "Web Proxy." This section can give you an overview of traffic through your server as well as details for a specific user or IP address.

Under **System**, the "Logs," the "Hardware Report," and "Resources Report" can be very useful for troubleshooting errors and monitoring system performance.

SECTION III Summary

ClearOS is one of several open-source packages that can provide Web filtering and firewall services for schools. ClearOS is not appropriate for every network environment, but it does unify a large number of open-source tools under a user-friendly Web-based interface. Advanced users can still configure the Linux packages directly for greater control. Beginning users can implement the Web-based interface to control a variety of powerful features. ClearCenter also provides commercial services and support.

Commercial and Open Source Tools for Internet Filtering

Product	Contact	Business Model	Pricing*	Hardware
ComSifter Endorsed by the North American Division TDEC Committee. Discounts available for Adventist schools	www.comsifter.com	Commercial	$$	Yes
ClearOS Community Multifunction firewall/filter/server User-friendly Web interface	www.clearfoundation.com	Open source	FREE (Filter Updates - $)	No
ClearOS Professional Commercially supported version of ClearOS	www.clearcenter.com	Commercial	$	Optional Clearbox $$$
OpenDNS Premium Offsite DNS hosting Easy to use/set up	www.opendns.com	Commercial	FREE	No
OpenDNS Enterprise/Insights Active Directory Integration Filter groups/malware tracking	www.opendns.com	Commercial	$$/$$$	No
OpenDNS Umbrella Filtering for mobile devices such as laptops, tablets, and smart phones. Works even outside your network.	www.umbrella.com	Commercial	$$/$$$	No
K9/BlueCoat Great free product for home (good for parents) Quality commercial filtering for schools also available	www1.k9webprotection.com	Commercial	FREE for Home $$ for School	Available $$$

Product	Contact	Business Model	Pricing*	Hardware
Untangle Multifunction firewall/filter/server User-friendly Web interface	www.untangle.com	Open source	FREE	
Untangle Education Standard Premium Commercial version of Untangle	www.untangle.com/store/education-premium-conf.html/	Commercial	$$/$$$	Available $$$
Smoothwall Express Widely used firewall and filtering solution	www.smoothwall.org	Open Source	FREE	
Zentyal Community (Formerly eBox Platform)	www.zentyal.org	Open Source	FREE	No
Zentyal SMB/Enterprise Commercial version of Zentyal	www.zentyal.org	Commercial		
Sophos Commercial antivirus/malware that includes filtering features	www.sophos.com	Commercial	$$$	No
pfSense FreeBSD-based firewall/gateway/router	www.pfsense.org	Open Source	FREE	Third Party
Lightspeed Quality commercial filtering solution	www.lightspeedsystems.com	Commercial	$$$	Yes
Barracuda Commercial hardware appliances	www.barracudanetworks.com	Commercial	$$$	Yes
zScaler Cloud-based filtering and threat protection	www.zscaler.com	Commercial	$$$	No
SquidGuard Highly reviewed filtering plugin for Squid (list based/ACLs)	www.squidguard.org	Open Source	FREE	No
URLBlacklist Not filtering software per se, but a large (two million-plus entries) blacklist used by other products (Untangle, for example). It can be purchased separately and used with SquidGuard directly.	www.urlblacklist.com	Commercial	$	No

* Pricing Code (as of November 2012): $ — less than U.S.$250 per year; $$ — U.S.$250 to U.S.$750 per year; $$$ — more than U.S.$750 per year (prices are approximate and subject to change; optional features will drive up the costs).

Rudy Scott *owns and operates Pacific Computer Technologies in College Place, Washington. He can often be found fixing computers at nearby Walla Walla Valley Academy or Milton-Stateline Adventist School, and has taught K-12 computing classes and an occasional educational computer technology course for Walla Walla University.*

Annette Melgosa *works as Instruction Librarian at Walla Walla University in College Place, Washington. In addition to an M.A. in Information and Library Studies, she holds an M.Ed. in Educational Technology and is pursuing doctoral studies in the same field.*