Connected Learning Advisory
Te Ara Whītiki

Firewalls and Filtering

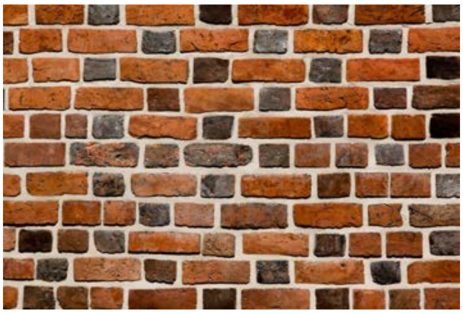

Image: wikipedia.org

This guide outlines what needs to be considered when thinking about the firewalling and internet filtering needs of New Zealand schools. It is aimed at school leadership and those who make decisions about firewalling and internet filtering. It is intended for a non-technical audience.

Firewalling and internet filtering, along with an effective digital citizenship strategy, are the primary means by which schools ensure the digital safety of learners. The rapidly evolving nature of technology means that schools should consider how firewalling and internet filtering can promote ethical and responsible digital citizenship of students and staff both in and out of school.

Contents

Once you have read this guide you are welcome to contact the Connected Learning Advisory to get more personal assistance. We aim to provide consistent, unbiased advice and are free of charge to all state and state-integrated New Zealand schools and kura. Our advisors can help with all aspects outlined in this guide as well as provide peer review of the decisions you reach before you take your next steps.

For more information visit www.connectedlearning.org.nz
Check out our resources at resources.connectedlearning.org.nz
Call us for personalised service on 0800 700 400
Make a personal inquiry via our online form at query.connectedlearning.org.nz
Email info@connectedlearning.org.nz

About Firewalls and Filters

What is a Firewall?

Firewalls are specialised computers, placed at the edge of a computer network, that control and monitor the internet traffic that enters and leaves the network. They often have additional functions to allow remote access to the network (e.g. a Virtual Private Network (VPN)) or provide IP addressing functions (e.g. DHCP and DNS). Firewall functions are usually combined with routing functions and the terms 'Router' and 'Firewall' are used interchangeably. In simple terms, firewalls prevent unwanted internet traffic from entering a computer network while simultaneously allowing permitted traffic to leave. Firewalls should be configured so that the allowed / not allowed internet traffic meets the needs of users.

What is Web Filtering?

Web filters work by routing internet traffic through a specialised device that inspects what internet sites are being requested by the user. The filter checks each request against a set of policies that have been defined for each school (or group or user if group/user filtering is in place) and accordingly allows or rejects the request. This process is usually invisible to the end-user. Web filtering allows schools to monitor and accordingly restrict or allow what users can access when browsing the internet. Web filters typically have the ability to filter sites based on:

- individual sites (e.g. ABC.com)
- pages within a site
- categories of sites (e.g. gambling, games, etc)
- IP addresses
- keywords (e.g. swear words)
- applications (e.g. chat functions within websites)

Schools implement internet filtering for 2 main reasons:

- To help prevent access to sites and applications not appropriate to a school environment
- To help prevent sites or applications that act as a source of distraction or time-wasting

Web Filtering Considerations and the Importance of Digital Citizenship

Responsibilities of schools

Schools have a duty of care toward students. Internet safety could be seen to be an area of school activity covered by National Administration Guideline 5 - “*provide a safe physical and emotional environment for students.”*

The New Zealand Curriculum’s Key Competencies are also relevant to how schools approach this topic. Additionally, the Code of Professional Responsibility and Standards for the Teaching Profession requires teachers to “*Manage the learning setting to … maximise learners’ physical, social, cultural and emotional safety.”.*

Schools have a responsibility to ensure that students are safe when using the Internet. How individual schools do this will vary but requires a combination of two complementary approaches:

- *educational*: digital citizenship: guiding young people’s learning in the digital world, and
- *protective*: web filtering: mitigating or buffering risk by protection, support or intervention.

Web filtering must be balanced with strategies that promote:

- development of skills and knowledge for safe and responsible use of digital technologies
- opportunities for students to be involved in decisions about the management of digital technologies at the school
- development of a pro-social culture of digital technology use, and
- cooperation of the whole community in preventing and responding to incidents

Internet access on student devices

In the past, schools were confident that once at school, students’ access to the Internet was always through the school’s connection. This connection was often faster than the connection that students had at home. Typically the school firewalled and filtered the connection. This ensured the students were protected while at school. It also gave the school a degree of protection: it was clearly seen to be proactive and acting responsibly.

Recent advances and availability of mobile data connectivity mean that this approach is no longer effective, particularly in secondary schools. A smartphone can access the Internet at speeds similar to or faster than the speed offered by the school's network and the connection may be shared with others by creating a wireless hotspot. In almost all cases, the mobile data connection will be unfiltered.

Schools have a responsibility to ensure students are safe while at school and this responsibility extends to student use of mobile Internet connections . Additionally, unless it is clearly endangering the emotional or physical safety of other students or detrimentally affecting the learning environment, school staff cannot ask to search a student-owned device, nor ask for the password to any device to access the content (for more information, see the Ministry's guidelines about the Safe and Responsible use of Digital Technologies in schools).

This means that the school cannot easily monitor the use of cell phone Internet access so the only way to ensure the school meets its digital safety obligations is to implement a comprehensive digital citizenship strategy. This is because effective digital citizenship:

- guides people at home and at school
- guides people on a mobile data or school Internet connection
- guides people on any device they choose to use.

What role does Internet filtering have in a digital citizenship strategy?

An appropriate level of internet filtering can help students develop Key Competencies and be a useful part of a digital citizenship strategy by:

- providing learners with opportunities to exercise digital citizenship skills in a supportive yet safe environment
- encouraging learners to use the school's internet connection while at school, rather than using unfiltered, personal mobile data connections.
- using the reporting functions of your filtering solution to prompt conversations about online behaviour with users

Managing Self - What does it really look like?

In the context of digital technologies, a student who is able to manage themselves will be able to:

- manage their time so that it is used efficiently and productively
- know the difference between appropriate and inappropriate content, that this varies contextually and make good decisions based upon the context
- actively make decisions to ‘do the right thing’

Older learners should be able to manage themselves more effectively than younger learners, and be more discerning about what self-management means for themselves in different contexts. Using your filtering reporting tools to inform conversations with learners about how they manage themselves can be a useful technique to allow students to increase their ability to be discerning digital citizens.

Firewalling and Web Filtering in New Zealand Schools

Funded Firewalling and Web Filtering from The Network for Learning (N4L)

Since 2004 the Ministry has given schools the option of a funded firewalling and web filtering solution. In 2013 the Network For Learning (N4L) started to roll out Ultra Fast Fibre (UFB) connectivity including a hardware firewall/router. The N4L solution includes a web filter that can be customised to fit the needs of schools. It has the ability to filter based on individual sites, categories of sites (e.g. gambling) and IP addresses. These filters can be applied to individual or groups of devices and individual or groups of people.

The N4L firewall is fully managed at no cost to schools. This support includes configuration changes and software and hardware upgrades. N4L has expertise and experience in working with schools to ensure their internet and firewalling needs are met and that they support teaching and learning. The N4L service, because it is a managed service, has some unique advantages that a custom firewall does not have:

- The firewall rules that N4L implement as standard mean that common applications such as Google Hangouts, video-conferencing and Skype will not require extra configuration by your school.
- Teachers and students are more likely to be able to use the applications or sites they want without requiring technical support or intervention.
- If a change is made by a service provider (e.g. Apple, Google or Microsoft) that will require a firewall change to be made, the N4L will make those changes on your behalf in order to ensure that teaching and learning can continue.

Schools may make requests of N4L to change firewall rules. For example, a school may require an on-site server to be capable of being accessed from the internet. N4L actions these change requests quickly, but also audits them to ensure they achieve their intended purpose securely. N4L is keen to work with schools that may require custom or specialised firewalling and will work to ensure the N4L service meets their needs.

Alternatively schools are able to procure their own firewalling and web filtering solutions.

Alternatives to using N4L Firewalling and Web Filtering

Schools are able to use the N4L connection, but to substitute N4L’s firewall and filter with their own firewalling and filtering solutions. If a school is considering whether or not to provide their own firewall and filtering solution, the key question to consider is: “given it is provided at no cost, will the provided N4L solution meet our needs?”. To help to answer this, the N4L firewall should be evaluated against any alternative firewall using criteria such as:

- **Functionality** - is the firewall capable of doing the job required of it? Will additional advertised features, such as more granular reporting or bandwidth management, actually be used? If you are unsure of this then contact the Connected Learning Advisory for further advice.
- **Ease of use** - will it be easy for any setup or configuration changes to be made?

- **Cost** - what is the cost of the hardware, subscription and time or labour charges for installation, support and configuration changes?
- **Support** - what is the availability, quality and type of support? For example, is the support proactive (anticipates issues before they happen), reactive (responds to problems reported by users), or both?
- **Overall Value** - is the alternative firewall better value than the N4L's fully funded firewall solution?

HTTPS/SSL - What's the fuss?

Over the last few years many (more than 50% as of 2017) internet sites have started to use encryption to ensure that communication between the user and the website is secure. This is commonly called HTTPS (the 'S' stands for secure) or SSL (Secure Sockets Layer). A detailed explanation of how SSL works is available for those who are interested. The impact of HTTPS/SSL on school internet filtering is significant. This is because of how the encryption prevents web filters from inspecting the contents of web communication. In practice, encryption prevents filtering systems from reading any part of a URL (internet web address) beyond (to the right of) the initial site address.

For example, a Google search for "cars" sends the following URL to Google:

https://www.google.co.nz/?gfe_rd=cr&ei=r9tcVq-yM7Du8wejmoAg#q=cars

Ordinary internet filters cannot read any part of the URL to the right of https://www.google.co.nz/

This means that the filter cannot know if the user is searching for "cars" or for anything else. So, students could search for and access inappropriate content without detection or being blocked by the filter.

Safe Search

Search engines like Google and Bing provide 'safe search' options. These are enforced by the N4L filter by default. They provide an additional level of filtering of the results that a particular search will produce. However, they are by no means completely safe: search results can still include images or links that are inappropriate.

Secure Website Inspection

Filtering HTTPS sites is possible if you wish to block the whole of a domain. For example, it is very easy to block the whole of https://facebook.com. Unfortunately this is not very useful as most students need to use HTTPS sites for learning.

An alternative approach that allows both inspection and filtering of HTTPS sites is by deploying certificates. Certificates are digital fingerprints that identify a computer and are used to decrypt and encrypt communications. Adopting a certificate based inspection and filtering system allows the filter to work with HTTPS sites. Using the example above, the filter would be able to see that “cars” were being searched for, and apply (probably allow) filtering policies to the request. N4L is able to support such Secure Website Inspection. Contact N4L if you wish to enable this for your school.

Certificate based filtering of HTTPS sites provides several advantages to schools:

- Allows filtering of HTTPS sites e.g. Google image searches, keyword searches etc
- Allows HTTPS applications to be blocked e.g. block Facebook chat or Youtube upload (as opposed to all of Facebook or Youtube)
- Allows different user groups to have different filtering policies applied to them with regard to HTTPS sites e.g. staff are allowed to access Facebook but students are not.
- Allows malware filters to inspect HTTPS communication for malware.

  Malware is the name given to malicious software. Malware attempts to cause damage to your computer, or computer network. Computer viruses are a type of malware. Most malware is transmitted to computers through the internet. It is essential that your internet filter blocks malware from entering your school. By default, the N4L’s filter does this. However, the increase in HTTPS communication means that malware filtering is only truly effective if HTTPS filtering with certificates is in place, and enabled for those categories that are likely to contain malware. If you use internet filtering other than the N4L filter, ensure that it is capable of blocking malware, including malware transmitted over HTTPS.

There are also disadvantages:

- The certificate must be installed on every device that uses a HTTPS site. Installing the certificate only needs to be done once every few years (certificates have an expiry date), and it only takes a few minutes per device, but nevertheless, this must be done. Your technical support provider will be able to help with installing the certificates.
- Configuring and testing filtering policies that incorporate HTTPS inspection can be time-consuming. However, once configured the policies will rarely need changing. N4L or your technical support provider will be able to help with creating and testing these policies.

To determine the most appropriate secure web filtering solution for a school we recommend that you:

- Involve stakeholders in your school/community before making a decision regarding inspecting and filtering secure traffic.
- Liaise with your community about the possible implementation of inspecting and filtering secure web traffic
- Be informed. There are many concerns, myths and misconceptions about security and privacy when using the Internet so it is important to understand the implications of remaining with your current solution or implementing a new one.
- Be mindful that a technology solution such as secure web inspection and filtering is only a small part of an effective overall strategy to help create the kind of digital learning experience that you want for your students. There are no quick fixes.

Appendix - School Scenarios

Introduction

The following scenarios are provided to help you understand how the principles outlined above can be put into practice.

Internet filtering uses categories to group web sites by their content. You will need to be familiar with the categories of sites used by N4L, as well as examples of each. Another, complementary approach to filtering, is to filter by web application. This means, for example, that certain functions of a web site can be restricted, e.g. Facebook chat, or the ability to upload videos to Youtube. Finally, keyword restrictions can limit the ability to browse or search for sites that contain a user-defined list of keywords (usually swear or obscene words).

Internet filtering for schools can be categorised into two broad categories: A baseline category of sites and web applications that are inappropriate for any user (staff or student) to access at any time or under any circumstances; and an optional category that includes all those not in the baseline category. By default, the N4L has a baseline category, that is applied to all N4L schools, that consists of the following categories:

Scenario 1

A large secondary school requires different filtering for staff and students. Additionally, the ability to give certain groups of students access to particular sites is required. The school has a BYOD program. What filtering scenario would meet these needs?

To satisfy these requirements, the school could implement SSL filtering using the N4L's firewall. The SSL certificate can be deployed to the school's desktops and laptops using group policies or scripts. The certificate can also be made available to students on the school's website alongside instructions on how to use it. Students should find it easy to install the certificate on their own devices, though a few may require help from the school technician. The school already had staff and students in different groups on the directory, therefore, with the help of the N4L, filtering policies need to be designed to fit the needs of the school. These are shown in the table below.

The school wished enabled access to social media sites for Y9. This can be done alongside actively monitoring how and when this is being used. This decision needs to taken in consultation with students after explaining the danger of unfiltered smartphone connections. Additionally, the school's digital citizenship strategy should be reviewed and changes made to it to more accurately reflect the responsibilities of schools learners and caregivers.

Web filtering category	Staff	Students
Adult	Block	Block
Advertisements		
Alcohol		
Astrology		
Auctions		Block
Business and Industry		
Chat and instant Messaging		Block
Cheating and Plagiarism		Block
Child Abuse Content	Block	Block
Computer Security		
Computers and Internet		
Dating	Block	Block
Digital Postcards		
Dining and Drinking		
Dynamic and residential		Block
Education		
Entertainment		
Extreme	Block	Block
Fashion		
File Transfer Services		Block
Filter Avoidance	Block	Block
Finance		
Freeware and Shareware		Block
Gambling	Block	Block
Games		
Government and Law		

Hacking		Block
Hate Speech	Block	Block
Health and Nutrition		
Humour		Block
Illegal Activities	Block	Block
Illegal Drugs	Block	Block
Infrastructure and Content Delivery Networks		
Internet Telephony		
Job Search		
Lingerie and Swimsuits		
Lotteries	Block	Block
Mobile Phones		
Nature		
News		
Non-Governmental Organisations		
Non-Sexual Nudity		Block
Online Communities		
Online Storage and Backup		
Online Trading		
Organisational Email		
Parked Domains		
Peer File Transfer		
Personal Sites		
Photo Searches and Images		
Politics		
Pornography	Block	Block
Professional Networking		

Real Estate		
Reference		
Religion		
SaaS and B2B		
Safe for Kids		
Science and Technology		
Search Engines and Portals		
Sex Education		
Shopping		
Social Networking		Allowed for Y9 and above. Could consider time-based policy so blocked during lessons)
Social Science		
Society and Culture		
Software Updates		
Sports and Recreation		
Streaming Audio		Block
Tobacco	Block	Block
Transportation		
Travel		
Unclassified		
Weapons		
Web Hosting		
Web Page Translation		
Web-Based Email		

Scenario 2

Primary school students have been deliberately viewing inappropriate images by using an image search. The BoT has been asked to explain why these images were not blocked. What response might they give?

The general order of reaction to incidents such as these should be to find out exactly what happened - obtain the evidence - and then respond accordingly. There are several possibilities that could result in the ability to view inappropriate images:

1. The school's internet filtering was wrongly configured. This is surprisingly common, though N4L's default policy should prevent much material that is inappropriate from being accessed over the N4L connection. Alternative things to look out for include images being shared or looked at through social media. A good starting point is to consider the scope and context of the incident. Widespread incidents will require a more general response than an incident involving just one or two students. Consider carefully how to balance the need for learners to work against enforcing a very restrictive filtering policy. You may also wish to consider using secure website inspection to gain greater visibility into the searches done.
2. The students may have been using browser extensions to access third party filters that bypass the school's filtering. Students should be reminded about any relevant internet agreements that apply. The school's filtering policy should be checked to see if 'Proxies' are blocked. If they are, N4L should be informed that a new proxy has been used. If 'Proxies' are not blocked, then scenario 1, above applies.
3. The students have been using and sharing a smart phone connection and directly by-passing the school's N4L connection. The school cannot search, nor ask to search, the student's smartphone. Student's will need to be remind about any relevant policies that apply to this scenario.

Note that in this scenario the largest element in any response should be education for digital citizenship as the students will potentially spend more time online using an unfiltered internet connection than the filtered N4L connection.

No kind of internet filtering will be able to block access to content that could be deemed inappropriate. A discussion must be had with all stakeholders from a digital citizenship perspective.

Scenario 3

Secondary school students have worked out that a browser extension can be used on their BYOD laptops to circumvent the N4L filter and give them access to blocked content like Instagram and Snapchat. What actions could the school take to reduce the risk of this happening?

The key element of this scenario is context. Were the browser extensions used to access tools they wished to use for school-work or was it a time-wasting activity? If it was the latter, had the students completed all work that had been set? Some possibilities to consider include:

1. Using time-based filtering to allow the applications at appropriate times. This solution encourages students to use the safe, N4L connection rather than unfiltered 3G or 4G connections.
2. Checking that the filtering blocks 'Proxies'.

This guide has been produced in response to a number of specific queries about Firewalls and Filtering from schools. It should not be read as a recommendation or endorsement of any specific product. The Connected Learning Advisory is a Ministry of Education supported service that provides schools with technology information relevant to their queries and does not recommend one product over another.

Last Update: 15/1/18