Web Filtering categories & websites

This document outlines the web filtering categories on a Palo Alto firewall for schools that have received their Managed Network Upgrade.

N4L's Web Filtering is fully funded as part of your Managed Network connection and is one of the tools available to help create a safer online environment for your students and staff. Our filtering can block website categories, individual websites and apps, but not specific content within a website. For example, YouTube is widely used to support learning. Schools can currently either allow YouTube, or block all access to it - it cannot filter out individual YouTube videos.

Our Web Filtering should always be used in conjunction with your school's own digital citizenship policy and acceptable use procedures. It's also important to remember that no filtering system is able to provide 100% protection from inappropriate content.

Recommended blocked categories

Websites categorised below are blocked as part of our Internet Safety & Security Services (previously known as Safe & Secure Internet) recommended settings. To unblock any of these will require the school to go through an opt-out process. In addition to these categories, schools can also ask us to block individual websites.

Abused Drugs

Websites that promote the abuse of both legal and illegal drugs, the use and sale of drug-related paraphernalia, or the manufacturing or selling of drugs.

Adult

Websites with any sexually explicit material, media (including language, games, or comics), art, or products and online groups or forums that are sexually explicit in nature; and websites that promote adult services, such as video or telephone conferencing, escort services, and strip clubs.

Command and Control

Command-and-control (C2) URLs and domains used by malware or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data.

Compromised Website

Benign or legitimate websites that have been hacked or infected with content such as malicious scripts, viruses, trojans, or executables.

Copyright Infringement

Domains with illegal content, such as content that allows the illegal download of software or other intellectual property, which poses a potential liability risk. Websites that provide peer-to-peer file exchange services or general streaming media belong to their own respective categories.

Cryptocurrency

Websites that promote cryptocurrencies, cryptomining (but not embedded crypto miners) websites, cryptocurrency exchanges and vendors, and websites that manage cryptocurrency wallets and ledgers.

Encrypted DNS

Websites for DNS resolver service providers, which offer security and privacy for end users by encrypting DNS requests and responses using protocols like DNS over HTTPS (DoH).

Extremism

Websites promoting terrorism, racism, fascism, or other views that discriminate against people or groups of different ethnic backgrounds, religions, and other beliefs. In some regions, laws and regulations may prohibit allowing access to extremist websites, and allowing access may pose a liability risk.

Grayware

Websites with content that don't pose a direct security threat but that display other intrusive behaviour and tempt end users to grant remote access or perform other unauthorised actions. Grayware includes the following:

- Hacked websites
- Typosquatting domains that don't exhibit malicious behaviour and are not owned by the targeted domain
- Websites with rogueware, adware, or other unsolicited applications, such as embedded crypto miners, clickjacking, or hijackers who change web browser elements
- Websites with content pertaining to illegal or criminal activities.

Hacking

Websites related to the illegal or questionable access to or use of communications equipment or software, including the development and distribution of such programs, how-to-advice, or tips that may result in the compromise of networks and systems. Includes websites that facilitate the bypass of licensing and digital rights systems.

Malware

Websites containing or known to host malicious content, executables, scripts, viruses, trojans, and code.

Not Resolved

This category indicates that the website wasn't found in the local URL filtering database or cache and the firewall was unable to connect to the cloud database to check the category.

Peer-to-peer

Websites that provide access to, or clients for, peer-to-peer sharing of torrents, download programs, media files, or other software applications. Primarily applicable to those websites with BitTorrent download capabilities. Excludes shareware or freeware websites.

Phishing

Web content that covertly attempts to harvest information, such as login credentials, credit card information, account numbers, PINs, and other personally identifiable information (PII), voluntarily or involuntarily, from victims using social engineering techniques. Includes technical support scams and scareware.

Proxy Avoidance and Anonymizers

Proxy servers and other methods that bypass URL filtering or monitoring. *Please note, VPNs with corporate-level usage fall under the Internet Communication and Telephony category.*

Questionable

Websites containing tasteless humor or offensive content targeting specific demographics of individuals or groups of people.

Ransomware

Websites known to host ransomware or malicious traffic involved in conducting ransomware campaigns that generally threaten to publish private data or keep access to specific data or systems blocked, usually by encrypting it, until the demanded ransom is paid. Includes URLs that deliver related stealers, wipers, and loaders that may carry ransomware payloads.

Scanning Activity (Advanced URL Filtering only)

Campaigns that are conducted by adversaries that can be indicators of compromise, or attempts at conducting targeted attacks or probing for existing vulnerabilities. These are usually part of reconnaissance activity conducted by adversaries.

Unknown

Websites that have not yet been identified by Palo Alto Networks. If availability of this website is critical to your school you must allow the traffic, alert on unknown websites, apply the best practice security profiles to the traffic, and investigate the alerts.

Additional categories

Below are additional categories that your school can choose to block. The description for each of these categories can be found here.

Suggested blocked categories - categories N4L strongly suggests blocking

Alcohol & Tobacco
Dating
Dynamic DNS
Gaming

Insufficient Content
Marijuana
Newly Registered Domain
Nudity

Parked
Swimsuits and Intimate Apparel
Weapons

Optional blocked categories - categories that are up to you to block at your own discretion

Abortion
AI Code Assistant
AI Conversational Assistant
AI Data and Workflow Optimizer
AI Media Service
AI Meeting Assistant
AI Platform Service
AI Website Generator
AI Writing Assistant
Artificial Intelligence
Games
Hunting and Fishing
Internet Communications and Telephony
Online Storage and Backup
Philosophy and Political Advocacy
Remote Access
Search Engines
Sex Education
Shareware and Freeware
Social Networking
Web-based Email

Other categories - categories you can choose to block, but you shouldn't need to

Auctions
Business and Economy
Computer and Internet Info
Content Delivery Networks
Educational Institutions
Entertainment and Arts
Financial Services
Government
Health and Medicine
Home and Garden
Internet Portals
Job Search
Legal
Military
Motor Vehicles
Music
News
Personal Sites and Blogs
Private IP Addresses
Real Estate
Recreation and Hobbies
Reference and Research
Religion
Shopping
Society
Sports
Streaming Media
Stock Advice and Tools
Training and Tools
Travel
Translation
Web Hosting
Web Advertisements

Recommended allowed search engine websites

The websites listed below are allowed by N4L due to their safe search functionality or content restrictions. All other known search engines will be blocked for schools under N4L's DNS Threat Protection service.

- Google
- Bing
- safe.duckduckgo.com

Nearly 99% of searches on the Managed Network are conducted through Google and Bing. Google and Bing can both enable SafeSearch which filters the majority of inappropriate images and searches, and N4L can enforce this setting for schools and kura that use DNS Threat Protection.

If you would like to block any of these categories or specific websites for your school or kura, please call our Customer Support team on 0800 532 764 or email support@n4l.co.nz.