Appropriate Filtering for Education settings

November 2023

Filtering Provider Checklist

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Palo Alto Networks
Address	22 Bishopsgate London
Contact details	Keir Williams & Oliver Wells
Filtering System	NGFW - STRATA - Palo Alto Networks
Date of assessment	10/11/2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Palo Alto Networks is one of the highest contributors to the IWF and we work in constant collaboration with the IWF and other agencies in the UK and around the world, to help make the Internet a safer place for Children https://www.iwf.org.uk/membership/our-members/
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Palo Alto Networks URL filtering is required to block all IWF listed Illegal Child Abuse Images and all other Illegal content . Our solution takes a direct feed from the IWF URL block list. https://www.iwf.org.uk/membership/benefits-of-membership/
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Palo Alto Networks URL filtering solution actively integrates with the Police assessed List of unlawful terrorist content produced by the home office and the counterterrorism referral unit.
• Confirm that filters for illegal content cannot be disabled by the school		The URL Filtering is a subscription module that is not included as in the base licence with our firewall. As this is an additional subscription we can not enforce the filtering without the subscription being in place. All URL filters must be locally configured on the appliance by a super admin, however once configured the end-users such as students and staff members could not disable this.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Palo Alto Networks URL Filtering Provides an 'Extremism' related category enabling schools and colleges to block websites that promote terrorism, racism, facism and other related extremist views that discriminate against people or groups from different ethnic backgrounds, religions, faiths or beliefs.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Palo Alto Networks URL filtering provides an 'Abused Drugs' related category that enables the blocking of sites promoting the abuse of both legal and illegal drugs and substances, as well as the promotion of the sale or manufacturing of drugs or related paraphernalia.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Palo Alto Networks URL Filtering Provides an 'Extremism' related category enabling schools and colleges to block websites that promote terrorism, racism, facism and other related extremist views that discriminate against people or groups from different ethnic backgrounds, religions, faiths or beliefs.
Gambling	Enables gambling		Palo Alto Networks URL Filtering Provides an 'Gambling' related category enabling schools and colleges to block websites that promote and offer both legal and illegal gambling activities
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Palo Alto Networks URL filtering provides a 'Malware' and 'Hacking' Categories which enable the blocking of sites of sites that relate to illegal or questionable access to or the use of communications equipment/ software. The development and distribution of programs, how-to-advice or tips that may result in the compromise of a network. This also includes sites that facilitate the bypass of licensing and digital rights systems and protections, or sites containing and distributing malicious content, executables, scripts, viruses trojans and other malicious code. This solution can also provide further protection against 'command and control' if this category is enabled for URLs and domains used by hackers and Malware to

			take control of compromised or vulnerable systems. Surreptitiously communicating with the attackers remote servers to send and receive malicious commands or exfiltrate the organisations data. Palo Alto has also been ranked as a leader in the industry for offering Firewall and Filtering systems by third party testing and Benchmarking bodies, such as Gartner@ and Forrester@ for over 11 years for offering Anti Malware and Hacking protection.
Pornography	displays sexual acts or explicit images		Palo Alto Networks URL Filtering Provides an 'adult' Category which enables the blocking of sites containing sexually explicit materials, media (including language) art and/ or products, online groups or forums that are secually explicit in nature. Sites that promote adult services such cas video/ telephone conferencing escort services, strip clubs etc. Anything containing adult content (even if it's games or comics) will be categorised as adult. We also provide a further ' nudity' category which enables the blocking of sites that contain nude or seminude depictions of the human body, regardless of context or intent, such as artwork that includes nudist or naturis sites containing this kind of content and images.
Piracy and copyright theft	includes illegal provision of copyrighted material		Palo Alto Networks URL filtering Provides a ' copyright infringement' category which enables the blocking of web pages and services that are dedicated to illegally offering the access to videos, movies and other media and software for download which infringes copyright law. Should you wish to stop Peer-to-Peer file exchange services or general streaming of media, we can also enable the the 'peer-to-peer' category specifically for sites that provide access to or clients to share and d
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Palo Alto Networks URL Filtering Provides a ' 'Questionable' category which enables the blocking of sites that contain tasteless humour, offensive content and targeting specific demographics of individuals or groups of people, criminal activity, illegal

			activity, violence, suidide and pyramid / get rich quick schemes .
Violence	Displays or promotes the use of physical force intended to hurt or kill		Palo Alto Networks URL Filtering Provides a ' 'Questionable' category which enables the blocking of sites that contain tasteless humour, offensive content and targeting specific demographics of individuals or groups of people, criminal activity, illegal activity, violence, suidide and pyramid / get rich quick schemes .

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Machine and deep learning powered detection can automate and enable rapid, highly accurate web filtering to eliminate threats live. This can also be used to help improve the category filtering by applying the same techniques to improve the detection of newly registered or unknown URLs live. The URL filter can review image content, language to determine benign or malicious content. We use text and language analysis to draw correlations between website copy, the context in which the copy is used, and urls to precisely categorise websites. Images from websites are broken down and compared to previous examples using sophisticated algorithms to assist in the determination of possible malicious content link Phishing attacks. By Examining each component of an individual page and applying multiple machine learning classifiers, we combine accuracy, speed and continual adaption in the face of changing attack techniques.
Content analysis; Palo Altos NGSWs URL filtering uses crawlers to scrutiny multiple websites attributes for malicious indicators and to help categories the websites. Correlated domain data, the presence of forms, and the location of specific types of content are among the attributes our learning classifiers process. Every URL we analyse adds to our data library, continually informing and improving our ability to provide an up to date library of websites that may pose a security or safeguarding risk.
Text Analysis; URl filtering scans websites text and its context to determine the most accurate category classifications. Keyword filtering can block users from accessing and seeing inappropriate language.
Image Analysis; To Avoid detection, phishing pages increasingly use obfuscated javascript and images on web pages instead of actual text. By Automatically analysing the image content of each URL we can compare website code with visual indicators to more accurately determine whether a URL poses a phishing threat. We can also block inappropriate images by enforcing safesearch.
Tight controls over common Policy Evasion Techniques; Palo Alto can enforce tight controls and common policies using user-ID and user based the application control and URL filtering policies
Search Engine-Cached Result prevention; The Palo Alto URL filtering policies can be enforced even when users use common evasion tactics, such as cached results and language translation sites.
Translation Site Filtering; Palo Alto networks URL filtering can block access to these sites that are often used to evade URL filtering.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained.

Retention and logging : Retention times for data logging on the firewall are established by your system administrator. Requests for categorisation or uncashed urls sent to PAN-DB URL filtering are entertained for six months.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Customizable Categories; Although the URL filtering can apply predefined categories, different organisations may wish to customise this around age, risk and tolerance and compliance and area of study. To meet this requirement administrators can apply custom categories by combining multiple existing categories to create new ones or apply different rules based on the user-ID or group.
Customizable Administrator / End-user Notifications; Administrators can create custom reports and schedule these to be sent to non technical members of the team, we can also create email alerts based on rules and policies breaches too.
URL Filtering Continued; When a user accesses pages that may pose a risk to the organisation or the user themselves the url filtering can present them with a custom warning page with a continue option if required. This presents the user with an opportunity to educate themselves or at least be aware of the risk before proceeding.
URL Filtering Override; Palo Alto's NGFW can also provide an override option for specific predefined categories that may be required for specific areas of study that need authorisation to access. This can be provided to senior members of the SLT to apply at the appropriate times.
Warning pages; When a user accesses pages that may pose a risk to the organisation or themselves the url filtering can present them with a custom warning page with a continue option if required or just a block page. This presents the user with an opportunity to educate themselves or at least be aware of the risk before proceeding.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff		Using the Pan-OS User ID schools and colleges can create user and group based security policies. This means that the IT team can allow, deny and monitor all of the users online activity, including URL categories or specific websites and applications to stop users from misusing the system and only access age appropriate content.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		Palo Alto Networks NGSW provides tight controls over common policy evasion

		techniques employed by users. The URL filtering policies can be enforced even when users use common evasion tactics, such as cached results and language translation sites. Blocking Search Engine Chased Results, Palo Alto is able to block a common tactic used to evade controls, accessing cached results within popular search engines. Embedded activity within applications, some applications can mask activity and hinder the ability to enforce safe search, Palo Alto has the ability to enforce users to only access approved applications to help Safe Search enforcement. Translation sites, Palo Alto networks URL filtering can block access to these sites that are often used to evade URL filtering.
• Control – has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		The Palo Alto networks NGFW solution is fully customisable and the administrator remains in full control of all reports and filtering on the system at all times. Any required changes, audits or reports can be applied or run instantly at any time. Providing full granular control of the system.

• Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked, this would include AI generated content. For example, being able to contextually analyse text on a page and dynamically filter.		Palo Alto has the ability to apply keyword filters by creating a Custom URL category with search queries for specific predefined words. We can do this by Creating a Log Forwarding Profile with a filter for the URL categories to be alerted
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Palo Alto Networks filtering can be fully customised to meet your safeguarding and prevent needs. a Full list of our category filters can be found on our website.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Palo Alto has the ability to provide Group or multi site management with central policies via our panorama management and reporting platform that can centrally control multiple firewalls.
• Identification - the filtering system should have the ability to identify users		Palo Alto Networks provides the ability to identify individual users, what content and what applications they are accessing at any time on any device by syncing with the active directory and your wireless / authentication system.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps		Palo Alto Networks URL Filtering and Application control can help to contain users to only approved and monitored applications. This includes Mobile and device applications for both managed and unmanaged devices.
• Multiple language support – the ability for the system to manage relevant languages		Palo Alto Networks Supports over 41 different languages

		which can be found on our website.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		user-ID can be configured to monitor and filter authenticated events at a network level. This allows User-ID to associate a user with the IP address of the device from which they are logged in and does not therefore rely on any other form of software.
• Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		Palo Alto can secure all managed devices remotely using a Global protect client installed on the device. This can enforce the same level of filtering on the device anytime anywhere. This solution can be enforced to be always on and supports windows and Mac in the base licence and Android, IOS and a limited set of Chrome and linux devices in the premium licence. You can learn more about this in our Supporting Remote Learning white paper
• Reporting mechanism – the ability to report inappropriate content for access or blocking		All of the created reports can be scheduled to be sent to all appropriate members of the team both technical and non technical, at set intervals or times during the day. We can also create alerts if specific categories or filters are hit.
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		The IT department can get visibility into all student online activity from a fully

		customisable set of reports. These predefined or fully customisable reports can be scheduled to show all URL and user activity. Our granular reports can show individual users activity, highlight all applications in use and by which user, URL categories visited and which were blocked, specific URLs visited by which users, as well as including times and dates and stamp of these activities too. Palo Alto also has the ability to capture and log the referrer which will indicate if the user proactively searched this content, or if they were directed to the site via an advert or popup. All URL activity reports are fully customisable to meet the safeguarding needs of the school or college and can be set to report Categories visited, activity by user, Websites and categories that were blocked and blocked users etc.
• Safe Search – the ability to enforce 'safe search' when using search engines		SafeSearch can be enforced on all users' devices, regardless of if they are managed or unmanaged. This can be enabled in the URL filtering policy for all users and will enforce safe search on all approved browser applications such as Edge and Chrome, ensuring that students and staff have approved

		access to the internet. The safe search results are updated and maintained by google and not Palo Alto.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Palo Alto Networks Cyber Academy offers Faculty Training, hands-on Labs, Modularized curriculum and virtual firewall training at no cost to qualified academic institutions. A list of institutions that we already work with in the UK can be found here:- https://www.paloaltonetworks.co.uk/services/education/authorized-academy-centers/authorized-academy-centers#emea

Furthermore, Palo Alto Network Provides Free Online tools and resources to help enhance anyone's cybersecurity knowledge, these tools are available for staff and students alike:- https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

Palo Alto Networks Education Services offers free digital courses so that you can learn at your own pace. These courses cover all elements of our technology, from product fundamentals to specialised role-based learning.
https://live.paloaltonetworks.com/t5/digital-learning/ct-p/Digital_Learning
https://beacon.paloaltonetworks.com/student/catalog

We also have an education program for Lower education, Cyber A.C.E.S. includes Activities in Cybersecurity Education resources to help demystify cybersecurity through interactive learning, designed for children ages 5 to 15 with an understanding of how to protect their digital future.
https://start.paloaltonetworks.com/cyber-aces.html

Cyber A.C.E.S. provides the cybersecurity basics students need to have safer online experiences and become good digital citizens. Lessons are designed so they can be facilitated by anyone, regardless of their knowledge level, with each module tailored to a specific age group.

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Keir Williams
Position	Public Sector Regional Sales Manager
Date	10-11-23
Signature