Appropriate Filtering for Education settings

September 2019

Filtering Provider Checklist Reponses

Schools 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, 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. Children should not be able to access harmful or inappropriate material from the school or colleges 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."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

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	SonicWall
Address	Matrix House Basing View Basingstoke Hampshire UK RG21 4DZ
Contact details	Andrew Walker-Brown – Sales Engineering Director abrown@sonicwall.com Mike Awford – Channel Sales Director mawford@sonicwall.com
Filtering System	SonicWALL TZ, NSa range Next Generation Firewalls, FastVue for SonicWALL
Date of assessment	19th November 2019

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	🟩	SonicWALL has been a member of the IWF for many years and is committed to supporting the values and aims of the IWF.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	SonicWALL fully supports and implements blocking access to illegal Child Abuse Images via the IWF CAIC list.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	HMO police assessed list fully integrated into web filtering solution and categorised separately.

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.	🟩	Filtering of sites that promote hate, violence, racism etc. are fully integrated and allows for reporting and searches for inappropriate terms. Application control beyond HTTP/S means ability to manage user activity such as access to chat/IM and also inspect ALL SSL/TLS encrypted content regardless of port or protocol.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	SonicWALL has specific filtering capabilities and category for Illegal drugs and drug use. Ability to report on search terms and sites visited per user/group. Separate categories for smoking/tobacco and alcohol.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	We have a dedicated category for Radicalisation and Extremism containing the HMO polices approved list. There are additional categories which cover violence/hate and racism. Ability to apply and report on user/group/category activity etc.
Malware / Hacking	promotes the compromising of systems including anonymous	🟩	SonicWALL provides filtering of access to sites that promote

	browsing and other filter bypass tools as well as sites hosting malicious content	🟩	hacking, filtering avoidance and malware tools. We also provide extensive application control which is able to block proxy avoidance tools such as Ultrasurf/Tor/PSiphon etc.
Pornography	displays sexual acts or explicit images	🟩	We have specific categories to filter access to pornography and adult/mature content. We also ability to enforce Google/Bing safe search and YouTube restricted content on a per-policy basis.
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	We provide filtering of sites that would allow download of copywritten material through Freeware/Software Downloads/Multimedia category etc. We are also able to block file sharing applications such as BitTorrent which would evade traditional web filtering technology.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Specific categories for filtering sites that promote violence or racism, illegal activities/skills and also cult/occult sites. Combined with monitoring and alerting on site access, use of specific search terms etc. or keywords.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Specific category for filtering sites that promote violence or racism, illegal activities/skills and also cult/occult sites. Again, further reporting and alert on site accessed, search terms used etc.

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

SonicWALL content filtering solutions are based on firewall technology developed over more than 20 years. Entirely designed in-house and using our own threat research, SonicWALL has been a recognised market leader in the provision of firewall, UTM and subsequently Next Generation Firewalls.

By providing a fully integrated security solution, SonicWALL not only offers web filtering (HTTP and HTTPS) but also full inspection of every single packet traversing the firewall, regardless of port or protocol. This means, that in real-time, administrators can see exactly what is happening on their network and apply appropriate levels of control. Be that blocking certain applications (or features of an application), through to bandwidth management and prioritisation.

With the increased use of TLS encrypted traffic (for very good reasons), it's still critical to be able to inspect and manage this, again regardless of port or protocol. SonicWALL solutions will decrypt SSL/TLS regardless of port/protocol and apply the same policies as for unencrypted traffic.

Combined with comprehensive intrusion prevention, inspection of files of any size for 50M+ viruses, botnet control and anti-spyware, the solution provides class leading security and safety.

Our multi-engine Sandbox technology (Capture) provides that ultimate additional protection against zero-day-threats, including complex CPU and side-channel attacks. Capture inspects and evaluates unknown content (executables, PDF, office docs etc) for previously unseen malware and is able to block that content in real-time before it enters the network.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

Logfile and report data retention is fully configurable as part of the customer specific deployment. Log retention can be configured based on database size or time period.

The solution will also provide expected storage requirement given the retention time and volume of logging being received.

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

Any solution is built on a number of critical foundations to deliver appropriate and effective security. By developing its own technology for over 25 years and by investing in our own threat research (the Capture Threat Labs), SonicWALL has complete control over its products and service.

The architecture of the technology allows for granular policies to be designed and implemented. This ensures controls are applied to the appropriate users/groups and devices, avoiding over blocking (or under blocking!).

By undertaking our own threat research, analysing 10,000's of malware samples daily, analysing and categorising web content from 100,000's of sources means we are able to provide accurate intelligence for our solutions to use. That means, correctly categorised URLs, rapid development and deployment of malware signatures used by 100,000's of appliances worldwide. If a website needs to be assessed/reassessed quickly, we do it, not a third party. If a new vulnerability is found, we develop a solution, test and deploy, not a third party. And if there is an issue, we resolve it quickly, not a third party.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	🟩	Policies can be designed and implemented in an age appropriate way e.g. based on Active Directory user group/OU such that a

	🟩	given policy only applies to specific users/groups. Monitoring and reporting on activity can be based around policy violation or more generically around site access and associated with Active Directory groups to identify age etc. of users.
● 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.	🟩	SonicWall NGFW's utilise a full layer 7 inspection technology known as RFDPI. This inspects every packet traversing the firewall regardless of port or protocol to identify and control a broad range of applications. When combined with SSL inspection across any port/protocol that implements TLS, the solution is able mitigate attempts to circumvent controls. Proxies, VPNs, Tor etc. can be controlled though this feature.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	Schools have the ability to update filtering policies through an easy to use and intuitive interface. The ability to delegate administrative control means support staff or teachers could potentially make the required changes. The solution also allows for sites to be unblocked I real-time through a password enabled "Bypass" feature or through used of dedicated allow/bock lists.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	SonicWALL uses a combination of electronic and human technology to quickly and accurately categorise websites without over-blocking.

	🟩	Users are able to directly request a site be re-rated in the event of miscategorising. Custom categories can also be used as a permanent override.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	SonicWalls Global Management system provides a central point of management and control across large complex estates of firewalls. Capable of supporting thousands of managed firewalls, GMS gives administrators a central point of management and control with role based management, change management and auditing.
● Identification - the filtering system should have the ability to identify users	🟩	The SonicWALL filtering solution is able to identify users a number of technologies such as integration with AD, captive portal, RADIUS Accounting and NTLM. This allows both application of policies to be user/group based and also reporting/alerting.
● 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)	🟩	SonicWALL NGFW provide control of network traffic through a patented technology “RF-DPI”. Simply put, this allows us to inspect and categorise every packet traversing the firewall regardless of port or protocol. This means we are able to identify applications regardless of the client device (PC, phone, table, iOS, Android etc.). Once identified we can then control the application (e.g. Dropbox, Facebook, Apple iTunes, Google Play Store).

● Multiple language support – the ability for the system to manage relevant languages	🟩	Technical implementation of policies is applied at the network layer and is to a greater extent agnostic of language. Assuming a given site has been categorised, or an application identified, the language used is irrelevant. For keyword based monitoring/alerting then those terms would need to be keyed in the desired language.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices	🟩	SonicWALL NGFW appliances utilise our RFDPI technology on the firewall for inspecting and categorising network traffic. No software is required on user devices in order to do this.
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	The SonicWALL solution provides a comprehensive reporting and alerting package that provide ease to use and detailed reports/alerts on all user activity. We are also able to integrate into 3rd party SEIM/reporting tools through SYSLOG/IPFix
● Reports – the system offers clear historical information on the websites visited by your users	🟩	Our solution provides configurable historical reporting of all user activity by user/group/OU etc. These can be generated/queried in realtime and also schedule and sent regularly via email etc.

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

SonicWALL and our partners work closely with schools/colleges and other setting to understand their requirements and to develop the most appropriate solution for them. We understand that one-size does not fit all and that tailoring a solution is key to making the technology work best for the customer needs.

We are also happy to work with customers at the early KCSIE policy development stage and share our experiences of what can be achieved and what may and may not be appropriate.

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
- 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	Andrew Walker-Brown
Position	Director, Sales Engineering
Date	19th November 2019
Signature	Andrew Walker-Brown.

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