Appropriate Monitoring for Schools

September 2019

Monitoring Provider Checklist Reponses

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. 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."

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

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

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
Monitoring 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.	🟨

Monitoring Content

Monitoring providers should ensure that they:

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.
- Utilisation of IWF Hash list to identify the storage or transmission of known child abuse images	🟧	SonicWall does not currently utilise the IWF Hash list.
- Work with CTIRU '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

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content	🟩	Through appropriate web filtering, application inspection we are able to identify and control attempted access to illegal content. The solution allows administrators/staff etc. to monitor in realtime, receive automated alerts and access historical reports. Access to monitoring, alerting and reporting is via an intuitive web interface.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others	🟩	The solution provides multiple layers of enforcement, monitoring and alerting to assist in the management and control of bullying or related situations. Enforcements means blocking access to sites, applications or materials which could be misused. Monitoring provides for near real-time reporting on user activity, including keywords etc. Finally, alerting provides immediate notification upon policy violation or given a defined set of criteria e.g. search terms, site access or keyword usage.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual	🟩	As with bullying, the solution provides multiple layers of

	relationship. This may include encouragement to meet	🟩	enforcement, monitoring and alerting to assist in the management and control of potential child exploitation. Enforcements means blocking access to sites, applications or materials which could be misused. Policies being applied in an age appropriate way. Monitoring provides for near real-time reporting on user activity, including keywords etc. Finally, alerting provides immediate notification upon policy violation or given a defined set of criteria e.g. search terms, site access or keyword usage. Integration with the IWF CAIC list ensures access to restricted sits is blocked.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity	🟩	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. As with other content, the solution is able to provide near realtime monitoring, alerting and historical reporting.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Specific filtering capabilities and category for Illegal drugs and drug use. The solution is able to then report activity, generate alerts and provide scheduled reports. The solution is also able to alert/report on search terms.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Dedicated category for Radicalisation and Extremism containing the HMO polices approved list. There are additional categories which cover more general violence/hate and racism. The solution provides the ability to alert and report on user/group/category activity etc.

Pornography	displays sexual acts or explicit images	🟩	Specific categories to filter access to pornography and adult content. Policies can be used to enforce Google/Bing safe search, YouTube restricted content. The solution will also report on sites accessed/blocked, alert on search terms etc.
Self Harm	promotes or displays deliberate self harm	🟩	Specific categories for filtering sites that promote violence or racism, illegal activities/skills and also cult/occult sites. Combined with monitoring, historical reporting and alerting on site access, use of specific search terms etc. or keywords etc.
Suicide	Suggest the user is considering suicide	🟩	The solution combines a range of inappropriate website categories that may contain content which an individual may try to access. This can be monitored and if appropriate, blocked. Inspection of searches, keywords used in chat session or submitted to websites may also be monitored and if appropriate alerts generated.
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, monitoring, reporting and alerting on site access, blocked sites, search terms 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 25 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+

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 (Capture Threat Centre), 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.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community based access	🟩	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. Policies can also be implemented based on IP/MAC/Subnet etc. where user information may not be available such as games consoles etc.

- Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided	🟩	The reporting/alerting platform provides dedicated management of alerting options. This allows the administrator to create custom alerts with granular triggers and also what evidence to include in the alert and to whom the alert should be sent.
- BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location	🟩	BYOD provides a challenging environment given the potential for privacy infringements without user consent. As all inspection and control is applied at the network layer, then regardless of whether the endpoint is BYOD or owned by the organisation, the same policies can be applied. It is likely that in the case of BYOD, different policies will be required. These can be implemented at IP/device/subnets level and/or to user/group if user information is known. Deployment is at the network layer and does not require any agents/software to be installed on the client device. Monitoring of BYOD devices does need to managed carefully to ensure privacy. HTTPS website filtering can be maintained without the need to have SSL decryption enabled, however granularity and accuracy may be impacted. The solution allows policies to be applied appropriately with inspection

	🟩	restricted as deemed necessary. The solution does not provide for filtering/monitoring while off network. This would require an agent of some sort that would typically too intrusive to the user.
• Data retention –what data is stored, where is it (physically) stored and for how long	🟩	The solution would store raw syslog data and processed reporting information for a period defined by the administrator. This data is stored on the IT infrastructure where the reporting/monitoring solution is installed.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers	🟩	The solution does not require software to be deployed onto devices in order to provide the filtering and monitoring services described. There is client web filtering software for Windows, Mac and Chrome book which allows policies to be enforced on devices when off network.
• Flexibility – schools ability to amend (add or remove) keywords easily	🟩	An easy to use user interface and ability to delegate administrative control means support staff or teachers could potentially make the required changes. This could be to amend allow/block lists or update keywords. The solution also allows for blocked site bypassing for a limited period by teachers/staff by entering a passcode.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	SonicWalls Capture Security Centre 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.
• Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?	🟩	Monitoring and filtering policies are the output of the schools defined and documented KCSIE processes and procedures. As such, these should be communicated to staff and students as part of ongoing education and training process. The technology can be used to augment and remind users, through the use of Consent pages etc. which a user must agree to before web access is allowed. We are able to provide support and guidance directly to schools or through our network of partners.
• 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.
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?	🟩	Prioritisation of alerts is defined as part of the policy design process. This relies heavily on KCSIE policies and

	🟩	procedures developed by the school. We (or our partners) will work directly with the school to develop the required monitoring and alerting policies and who should be contacted/alerted in event of a violation or defined event. These can be modified quickly and easily through the graphical user interface.
• Reporting – how alerts are recorded within the system?	🟩	Alerts are generate by the solution and received via email. Alerts are recorded within the system logs and can be accessed as required.

Please note below opportunities or enhancements to support schools (and other settings) with their obligations around Keeping Children Safe in Education?

SonicWALL and our partners will work closely with education setting to understand their requirements 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.

MONITORING 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.