CHECK POINT
CIPA COMPLIANCE

CIPA COMPLIANCE

The Children's Internet Protection Act (CIPA), federal law HR4577, was signed into law by the USA Congress on December 21, 2000. CIPA imposes requirements on schools or libraries that are eligible for federal funding support for Internet access or internal connections through the E-rate program.

OVERVIEW

In today's classrooms, the Internet has become a critical tool for teachers and students alike. Teachers are using the internet to develop highly engaging lesson plans, and use simulations, videos, and interactive games and podcasts in the classroom to create interest, stimulate learning, and promote creativity. Students are increasingly using the internet for research, classwork, and often times in place of a printed textbook. As the continued use of the internet increases in K-12 education, the challenge of securing these networks and protecting children from cybercrime and inappropriate content grows exponentially.

In December 2000, The US Congress enacted The Children's Internet Protection Act (CIPA) to protect children from harmful content on the Internet.

In 2001, the Federal Communications Commission (FCC) issued regulations implementing CIPA.

WHAT CIPA REQUIRES

The CIPA regulation requires that K-12 schools and libraries participating in the E-Rate program must implement an Internet safety policy. They must use internet filters to protect children from harmful, obscene, and pornographic content. Protections must apply to all devices used by the school, and must prevent children from accessing dangerous and harmful content. Further, schools required to comply with CIPA must also certify that they have provisions to monitor the online activities of minors and that their security programs include provisions to educate minors about appropriate online behavior.

According to CIPA, the Internet safety policy must address all of the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors

For further reading about CIPA requirements visit FCC.gov

For schools, the policy must also include monitoring the online activities of minors. Note: beginning July 1, 2012, when schools certify their compliance with CIPA, they will also be certifying that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior, including

interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response. The school or library must enforce the operation of the technology protection measure* during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

CHECK POINT HELPS YOU MEET CIPA

As the global leader in network security, Check Point provides the best security solutions to help K-12 schools attain CIPA compliance, while both securing your network from latest threats and protecting your students from harmful content. The Check Point URL Filtering Software Blade enables an organization to efficiently and assuredly control access to millions of web sites by category, user or group. Administrators can block web traffic by category, such as Adult content, pornography, hate groups or gambling sites. Opt in the "Safe Search" option from the SmartDashboard and search requests are filtered as safesearches. Check Point URL Filtering condenses multiply sources.

For example the "Child Abuse" category enjoys both Check Point's content filtering repository as well as the "Internet Watch Foundation's" membership feeds.

URL Filtering Software Blade unifies enforcement for web security with complete control of websites and applications in one policy. Check Point unifies URL Filtering and Application Control to deliver:

- One common rule-base to simplify policy creation
- One management console for easier management
- One reporting system for improved visibility into web events.

No.	Hits	Name	Source	Destination	Applications/Sites	Action
1	1M	Block sites which may cause liability	Any	Internet	Hacking Hate/Racism Illegal / Questionable Illegal Drugs Violence Child_Abuse	Block Blocked Message
2	0	Block sex related sites	Any	Internet	Nudity Pornography	Block Blocked Message
3	235K	Block Critical/High risk applications/sites	Any	Internet	High Risk Critical Risk Phishing Spyware / Malicious Sites	Block High Risk Block
4	5K	Block Anonymizer	Any	Internet	Anonymizer	Block Blocked Message
5	815K	Block questionable sites	Any	Internet	Tasteless Gambling Weapons Alcohol	Block Blocked Message
6	224K		Any	Internet	Share Files Supports File Transfer P2P File Sharing Remote Administration Tool	Inform Access Notification Once a day
7	131K	Limit streaming and verify access reason	Any	Internet	Streaming Media Media Sharing Media Streams High Bandwidth	Allow Download_1Gbps Down: 1 Gbps
8	228K	Log all applications in the organization	Any	Internet	Any Recognized	Allow

Example: recommended policy for educational institute

The combined solution allows for unified enforcement and management of all aspects of web security for full Web and Web 2.0 protection, as well as user empowerment and education on web usage policy in real time. Through full integration in the gateway, this solution prevents bypass through external proxies.

CHECK POINT FEATURES

Prevention Measurement

The Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network. Multiple malware detection engines are utilized to protect the network, including signature and reputation engines, as well as a heuristic engine.

The Antivirus Software Blade provides extended protection by using ThreatCloud™ technology with real-time security intelligence. Customers can benefit from significantly more information, analysis and protection.

ThreatCloud™ feeds the security gateway with real-time security intelligence with its extensive security threat knowledge base of over 4.5 million malware signatures. ThreatCloud is dynamically updated using a worldwide network of threat sensors and leverages the Check Point install base to collect attack information that is shared among all gateways collectively. This allows identification of emerging outbreaks and threat trends that is delivered to the security gateways in real-time.

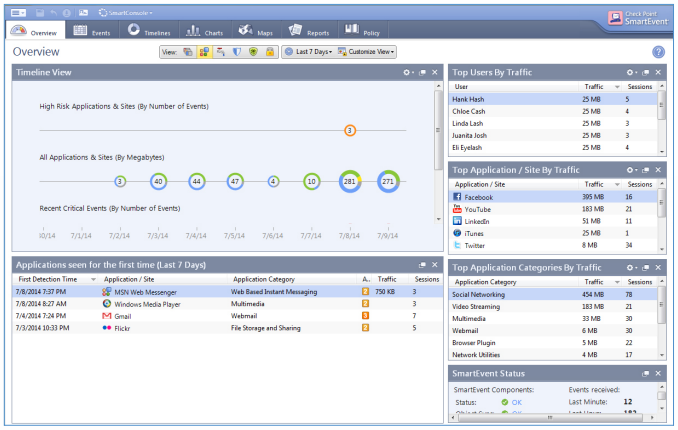
Education Tool

Users are an integral part of web security and control process. As such, it is highly important to engage and educate users. It is crucial that users surfing the web have the tools to identify and reduce exposure to potential risks. Check Point provides both the enforcement means to protect your network from harmful materials, and also offers an education platform. UserCheck empowers users with real-time alerts and educates them on corporate usage policy.

Visibility

As things can always go wrong, administrators are constantly seeking the most efficient tools to identify root causes and to remediate them effectively.

* A technology protection measure is a specific technology that blocks or filters Internet access.



Check Point Next Generation SmartEvent delivers real-time cyber threat visibility in the era of Big Data. It quickly searches and analyzes billions of data logs to identify critical security events from the clutter, easily moving from a high-level view to detailed forensic analysis. Administrators can leverage Next Generation SmartEvent to gain greater visibility into their network; they can more easily manage security and make faster, more informed security decisions

WHY CHECK POINT

Check Point, the global leader in network security software, provides the right solution for CIPA compliance. It does so by enforcing efficient security policy while also allowing your school to enjoy peace of mind.

Best Technology

Check Point combines the best technology to enforce protection measures. While the conventional approach to solve this problem involves a content control solution, Check Point has taken the next steps by leveraging its ThreatCloud technology to feed security gateway software blades with real-time security intelligence.

Integration with Premium Feeds

ThreatCloud IntelliStore is a unique threat intelligence marketplace that enables organizations to select from a diverse range of intelligence sources to supplement their current threat coverage. Customers can now customize intelligence feeds from a single platform based on their organization's geographical needs, vertical industries, and protection types. Through ThreatCloud, the intelligence feeds are automatically translated into security protections on Check Point Gateways.

Education Tool Included

Check Point UserCheck™ engages and educates users on corporate policy.

Compliance View at a Glance

Check Point's Compliance Blade provides an up to date CIPA compliance level report to help administrators understand their current implementation status.

SUMMARY

As the global leader in network security, Check Point provides the best security solutions to enable K-12 schools to attain and maintain CIPA compliance. Check Point Software Technologies can help schools and libraries ensure the safety and security of their students and protect them from cybercrime and harmful content. Check Point provides the right solution for CIPA compliance to enforce efficient security policy while also providing schools with peace of mind.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com