SOLUTION BRIEF

PROTECTING STUDENTS FROM ONLINE THREATS BY ENFORCING CIPA

A10 NETWORKS' THUNDER CFW ENABLES SCHOOL DISTRICTS TO EFFECTIVELY COMPLY WITH CIPA

The US Congress enacted the Children's Internet Protection Act (CIPA) to shield minors from malicious content on the Internet. CIPA dictates that all K-12 schools and libraries take measures to block access to content that is obscene, pornographic or harmful in other ways. Incidents where students easily access materials related to extremism, crime, hate, drugs, weapons and acts of violence on school grounds are correspondingly on the rise. Exposure to such content can severely impact students, leading to bad behavior or worse. Students are also exposed to cyber threats and bullying on social media, in online chat rooms and more, and such exposure has been linked to a rise in depression and suicide rates.

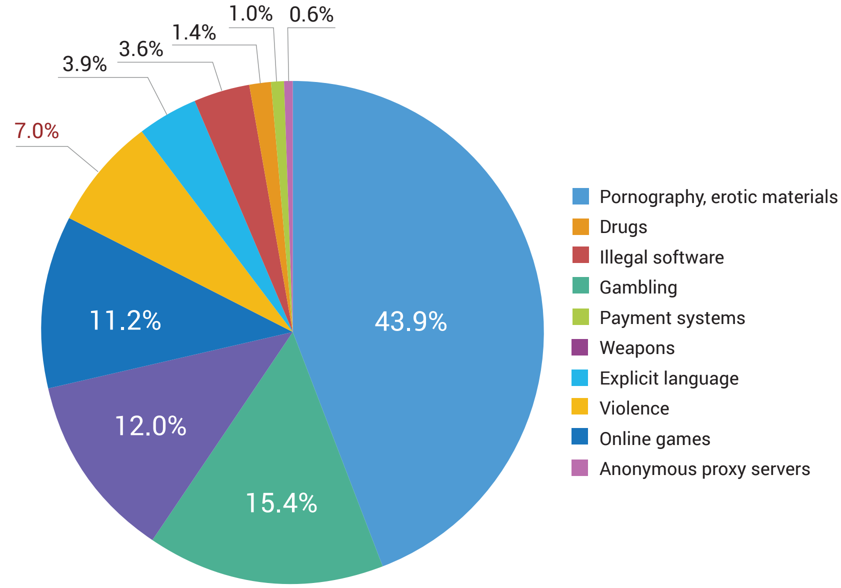

Figure 1: Proportion of visits to sites containing inappropriate content[1]

[1] https://securelist.com/children-online-the-security-formula/63866/

CHALLENGE

A rise in encryption over the Internet is making it hard to comply with CIPA mandates aimed at protecting and shielding school-age children from malicious and harmful content.

SOLUTION

A10 Thunder® CFW provides a comprehensive decryption and protection solution for students while enhancing the existing security infrastructure in educational institutions.

BENEFITS

- Enhances the existing security by decrypting SSL/TLS traffic without degrading network performance
- Helps enforce CIPA rules by enabling admins to restrict access and blacklist harmful content
- Defends against cyberattacks, whether initiated from within the network or outside
- Provides visibility into application traffic, allowing admins to block or limit access if students are violating school policies
- Provides selective decryption and inspection based on policies applied for different user groups

CIPA was enacted to help prevent the digital world from becoming a catalyst for violence and abuse for students. According to CIPA, "… schools and libraries subject to the act are required to adopt and implement an Internet safety policy addressing:

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

A10 Networks' Thunder Convergent Firewall (CFW) provides a highly effective solution for enforcing and applying all CIPA-related standards in today's learning environments.

WHY IS IT BECOMING MORE DIFFICULT TO PROTECT STUDENTS FROM ONLINE THREATS?

The rapid adoption of SSL/TLS encryption has led to over 80% of the Internet traffic in North America being encrypted, making it increasingly difficult for school districts to monitor what students are exposed to on the Internet. Without full visibility, schools are facing problems in creating and applying effective policies that would help protect students from being exposed to harmful or inappropriate content.

Legacy security solutions are not designed to inspect encrypted traffic, and since encryption is becoming a norm for most of the commonly used websites, apps and social networks including Facebook, Twitter, YouTube etc., these security solutions are left blind to what's going out of their network and what's coming in. Some network firewalls can decrypt encrypted traffic, but the process is resource-intensive. According to a recent NSS Labs report, these security solutions can experience over 90% performance degradation once decryption is enabled, adding so much latency that most network administrators don't turn on that feature, leaving them blind to hidden threats. Additionally, even though search engines like Google provide safe search options, they can easily be overridden by students, allowing them to gain access to anything and everything the Internet has to offer.

It is critical for our school districts to monitor network traffic coming in and going out of their networks. Having visibility into encrypted traffic can enable network administrators to monitor what's going on in their networks and provide them with the control they can leverage to minimize access to violent and malicious materials on the Internet, potentially saving lives.

A10 NETWORKS' THUNDER CONVERGENT FIREWALL (CFW) — A SUREFIRE SOLUTION

A10 Thunder CFW is a comprehensive security solution that provides complete protection for schools from cyber threats and malicious and inappropriate content. With its native SSL Insight technology, Thunder CFW provides high-performance SSL/TLS decryption which, when coupled with its advanced security features, enhances the entire security infrastructure within school and library environments, ensuring the application and enforcement of CIPA.

FEATURES AND BENEFITS

- **Decrypt** traffic for your entire security infrastructure including inline and passive devices like NGFW, IPS, IDS, ATP, etc., enabling them to inspect traffic to which they were otherwise blind. This decryption can be used to inspect both outgoing connections as well as connections coming in from the Internet.
- Prevent data loss and malware/virus downloads with the included **ICAP support** for DLP/AV systems. Enabling DLP installations to inspect encrypted payloads can ensure that no unauthorized data exports can happen.
- Block incoming traffic from malicious sources, protecting any hosted resources by using the included **Firewall** capabilities.

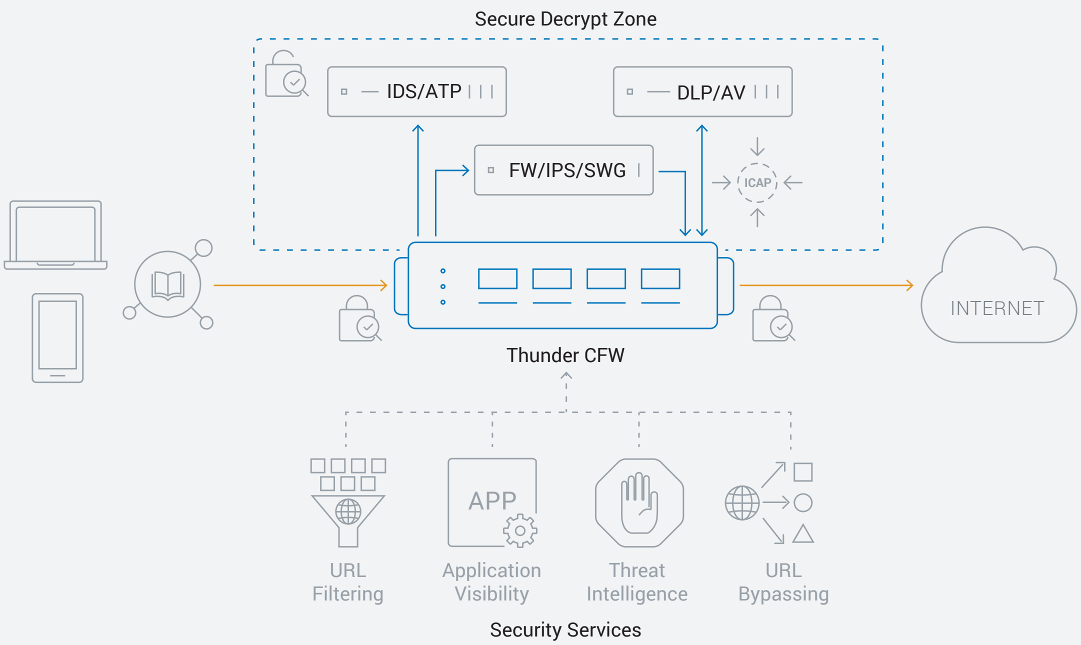

Figure 2: Thunder CFW augments existing security devices and provides advanced services to enforce CIPA and enhance overall network security

- Gain visibility into application traffic based on connection rates and bandwidth usage, using the **Application Visibility and Control service**. This service can be used to identify web applications that students are accessing and then, based on school/library policies, administrators can block access to either specific websites and applications or certain types of content on a website—e.g., disabling video streaming on YouTube and Facebook while allowing access to the websites' textual content, etc.
- Blocking traffic to known web categories like adult content, gambling, etc. as well as specific domains, using the URL Filtering service. The **URL Filtering service** can be very helpful in enforcing CIPA rules since it leverages web categorization and enables administrators to restrict access to known malicious and harmful content on the Internet.
- Selectively bypass traffic based on web categories while decrypting and monitoring the rest, with the URL Bypassing service. The **URL Bypassing service** leverages web categorization and provides 83 web categories based on which traffic can be separated and bypassed. These web categories include over 600 million known domains that can be used to define separate web access policies for different user groups.
- Selectively bypass traffic based on different **Active Directory groups** within a school. For example, SSL/TLS traffic for the faculty remains encrypted while traffic for students is intercepted and decrypted.
- Block access to known malicious sources on the Internet using the **Threat Intelligence service**. Traffic from known bad actors and other categories, including known botnet participants who are accessing school services, can be dropped and blacklisted. With approximately 48 million known entries, it provides an effective defense with multiple security research groups supplying threat intelligence feeds.
- Ensure that students can't disable additional safety features like Safe Search on search engines with powerful and customizable **A10 aFleX® rules**.

SOLUTION COMPONENTS

A10 Thunder CFW delivers comprehensive network security, combining state-of-the-art decryption, world-class threat intelligence and advanced content filtering to provide a surefire solution for CIPA compliance. The Thunder CFW device is installed inline on the network perimeter, intercepting and decrypting traffic and sending it in clear text to other security devices installed in the network. This ensures that any malicious traffic that may be hidden by SSL/TLS encryption can be identified and blocked.

SUMMARY

Deep visibility into encrypted traffic enables administrators to monitor network activities, minimize access to violent and malicious materials and potentially save lives. Thunder CFW not only protects students from exposure to threats and harmful content on the Internet, but also ensures that security infrastructures operate at peak performance while inspecting encrypted traffic. With Thunder CFW, school districts can easily enforce CIPA standards for students while maintaining privacy for faculty and authorized personnel.

NEXT STEPS

For more information about Thunder CFW, visit a10networks.com/cfw.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-SB-19194-EN-01 DEC 2018