

Cisco SAFE Security Architecture for Schools: More Effective and Efficient Security

Cisco SAFE Security Architecture for Schools is an online security reference architecture that provides detailed security design and implementation guidelines for K-12 schools. As part of an overarching Cisco Service Ready Architecture for Schools initiative, Cisco SAFE Security Architecture for Schools helps build a secure and reliable school network infrastructure to support 21st-century education.

The Need for Security Architecture

Schools are transitioning from classroom teaching to full Internet-based education and learning. Students, teachers, and staff are embracing new technologies and tools in a fast-changing and media-rich learning environment. This transition brings new and complex challenges. Without adequate security protection, for instance, schools may be threatened by harmful content and theft of personal identity information and student records, as well as the abuse of internal application and network resources. Regulatory and industry compliance requirements add further reasons to improve security. For instance, schools need to comply with the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA) if they accept federal funding.

In the past, schools depended on perimeter security tools such as firewalls for protection. Today, these point products alone are no longer adequate to support and secure a dynamic education environment in which students, parents, teachers, and guests are increasingly sharing both information and the network infrastructure. In addition, many schools are confronted with limited staff and inadequate security infrastructure as they attempt to protect their critical resources and services. A holistic security architecture is needed to help schools secure their infrastructure and resources effectively and efficiently.

Cisco SAFE Security Architecture for Schools

Cisco SAFE Security Architecture for Schools advocates a defense-in-depth approach to security. It addresses the security of the entire school infrastructure, demonstrating the importance of integrating security with each component, including networking devices, endpoints, databases, web, and email, so that collectively they can strengthen the overall school environment with protection, visibility, and controls.

The design uses a modular approach to provide detailed guidelines for various parts of the school network. The entire design contains an Internet-facing network that is typically managed at the school district level. The network then extends to the data center and individual school sites. The overall security architecture has the following components:

- **Network foundation protection:** The network is the foundation for communications and collaborations. Securing networking devices (such as routers and switches) is vital to ensure the availability and integrity of the school network infrastructure. Cisco switching and routing platforms provide numerous security capabilities, including spanning-tree protection, Layer 2 attack prevention, antispoofing, and Cisco IOS[®] firewalls. Cisco Security Design Guide for Schools provides guidance on how to design and configure networking devices securely, plus other best practices such as policies for controlling administrative access and handling change management.
- **Internet perimeter protection:** The Internet is a tremendous source of information and collaborative capability for the education community. However, schools need to take great care to protect students and staff from certain harmful content on the Internet. In addition, they need to defend against remote attackers who use the Internet to steal sensitive information such as personal data and identity information. Cisco offers a

comprehensive set of solutions for schools to protect their Internet connectivity as well as their internal resources and users. Cisco Adaptive Security Appliance (ASA) is a powerful and versatile solution to defend against Internet-based network attacks. In addition to its firewalling capabilities, Cisco ASA can be expanded to support an intrusion prevention system (IPS) and virtual private networks (VPNs). Cisco IronPort™ email security delivers a highly efficient solution to fight spam and email-based malware. Cisco IronPort web security provides not only URL filtering but also advanced capabilities to fight botnet traffic, malware, and spyware. Cisco SAFE Security Architecture for Schools provides details on designing and implementing Internet firewall, web, and email security.

- **Network access security and control:** Protecting a school's internal network and critical resources from unauthorized users and from unsecured laptops and other mobile devices is a major component in securing the school infrastructure. Shielding the infrastructure from network infections is another major consideration. Cisco offers a number of solutions to help schools achieve these goals, including Cisco Network Admission Control (NAC) and Cisco Identity-Based Networking Services (IBNS). These solutions provide user authentication and role-based access for students and staff at school sites and the district office. Cisco NAC also provides enforcement of device-level security policies and remediation services, and Cisco IBNS concentrates on authentication and authorization based on the IEEE 802.1X standard as well as web-based authentication methods. Cisco SAFE Security Architecture for Schools focuses on recommendations for configuring and deploying network access control for schools.
- **Endpoint protection:** Cisco SAFE Security Architecture for Schools provides recommendations for protecting servers and other school-controlled systems from viruses, malware, botnets, and other malicious software.
- **Cisco Video Surveillance:** IP-based video surveillance systems are deployed throughout the school district to monitor and analyze activity at all school premises with the intention to prevent and deter safety incidents. The video surveillance system provides first responders and school staff real-time information, vital to determine the appropriate and timely response to safety incidents.
- **Cisco Unified Communications Services and Alerting:** Cisco SAFE Security Architecture for Schools takes advantage of IP-based telephony, video, digital signage and conferencing services to facilitate the agile response to safety and security incidents. Cisco Unified Communications systems are therefore deployed throughout the school premises.
- **Professional services:** Cisco and partners can help plan, build, and run networks that follow Cisco SAFE Security Architecture for Schools to meet the unique needs of education customers, including regulatory compliance and protection from online and physical security threats.

Cisco Validated Design

Cisco SAFE Security Architecture for Schools is a Cisco Validated Design. This means that the architecture is supported by in-depth design, testing, validation, and documentation. This design helps schools by reducing their time and effort in designing and implementing a highly efficient and secure school network.

- Validated designs, based on best practices and real-world testing and validation, help schools by removing much of the guesswork that has traditionally gone into securing a network infrastructure. Schools can avoid mistakes and system errors that may occur due to trial-and-error attempts to create a secure environment.
- Detailed, step-by-step architectural and platform-specific guidance reduces the time and effort required for the school IT staff to design, deploy, and implement a secure network.
- Collaboration between security components and the network infrastructure not only creates stronger security, but also helps ensure better network availability and support for key educational and business applications and services.
- A systems approach and the ability to enforce security policies provide a foundation for compliance with laws such as CIPA and FERPA.

Conclusion

Cisco SAFE Security Architecture for Schools helps schools strengthen their online security by delivering a systematic and comprehensive architectural design. The detailed knowledge and recommendations save effort, cost, and time for schools as they improve their protection for the school infrastructure and resources.

For more information, please visit <http://www.cisco.com/go/designzone>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)