SONICWALL

Securing Esports in K-12 and Higher Education

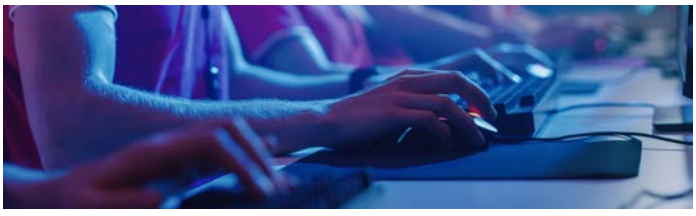
Overview

Online games were once discouraged in schools for fear of distracting students from their studies. More recently, schools have started to introduce clubs and intra-mural competitions as the benefits of esports, such as increased academic and social engagement and strengthened teamwork and collaboration, are being realized. Some colleges and universities even offer scholarships for athletes.

Apart from attitude changes, there also has been technological advances in esports. Games played on single-player consoles have evolved to multi-player tournaments streamed to different campuses. School clubs and tournament organizers offering the games must ensure a safe digital environment for the players and spectators.

Challenges

There are many considerations towards establishing a secure environment for esports and online games in schools. Game servers may be on-premises or hosted in public clouds. Players may be students on-campus or guests from other schools. In addition, hackers may try to disrupt games or steal critical information. The following are some of the challenges faced by institutions offering esports programs:



Deploying Low Latency Networks with High Security

Security is a top consideration whether students are playing Rocket League[1] on hand-held Nintendo[2] Switches in school clubs or battling at a League of Legends[3] regular-season competition. Threat actors can launch ransomware or network intrusion attacks to disrupt gameplay.

In addition to security, network latency is a major concern. A millisecond delay can turn a winning game into a losing one which in turn can result in dropped ratings that may impact championship titles and scholarships. As a result, institutions must implement High Availability and high-performing networks that complement the protection against attacks that target players, game servers or streaming platforms.

Strong Protection for PII and Game Assets

Regardless of whether players and spectators are students or guests, institutions and school clubs may incur reputation damage if they fail to secure the personally identifiable information (PII) of all parties involved. Schools must also protect account-related details such as IP addresses, login credentials, game strategies and data.

[1]Rocket League is a property and trademark of Psyonix LLC.
[2]Nintendo is a property and trademark of Nintendo, Ltd.
[3]League of Legends is a property and trademark of Riot Games, Inc.

SOLUTION BRIEF

Large Attack Surface Area

With high prestige and rewards at stake, cyberattacks have been launched to affect game outcomes. Threats such as distributed denial of service (DDoS) attacks disrupt communications and networks. Some games contain hidden malware, and these malware games, when downloaded or accessed, result in information theft and damaged files. Malware games, when downloaded or accessed, result in information theft and damaged files. Phishing sites deceive victims into sharing account credentials.

Solution

SonicWall provides comprehensive security to minimize risks and maintain a safe esports and gaming environment.

Secure Networks

SonicWall's next-generation firewalls (NGFWs) block cyberattacks while delivering high performance, availability and reliability. Built-in DNS filtering blocks access to malicious domains in phishing attacks while Content Filtering Services (CFS) allow for the elimination of inappropriate and illegal web content, as required. In addition, Intrusion Prevention Services (IPS) detect and prevent malicious traffic without impacting performance and Wi-Fi 6 capabilities further increase speed, security and efficiency. High availability (HA) firewall devices provide the uptime that meets your organization's needs.

Secure Access

SonicWall's NextGen VPN secures access to a broad range of applications and devices, including cloud-based applications, mobile devices and IoT devices, which are all critical elements in esports programs. Secure Mobile Access (SMA) provides access to trusted devices and authorized users. Cloud App Security (CAS) protects against account takeovers, insider threats and compromised credentials.

Advanced Threat Protection

Our Capture Advanced Threat Protection (ATP) sandbox blocks zero-day attacks at the gateway while our patented Real-Time Deep Memory Inspection (RTDMI™) discovers hidden threats even in encryption. Capture Security Center (CSC) provides centralized control and visualization across network and endpoint security operations.

Benefits

With SonicWall cybersecurity solutions that protect campus networks and student assets, institutions with esports programs are empowered to:

- Foster engagement and increase student participation
- Build trust with players and community
- Maintain operational continuity throughout the campus

Summary

Esports provide scholarship opportunities, recognition and positive social health to students. To foster a safe and conducive environment for esports programs, institutions must secure campus networks and access while preventing PII thefts and disruptive cyber attacks. SonicWall delivers strong cybersecurity protection with the network performance, availability and reliability that esports organizations and schools need to maintain their competitive edge.

Esports in Schools Use case

Depending on the size of the institution, school or district, IT might deploy a SonicWall NSsp, NSa or TZ firewall. Large institutions may include NSv, a virtual firewall, for microsegmentation, allowing granular control over applications and workloads. For schools, the firewall is connected to a SonicWall Switch which in turn is connected via site-to-site VPN to other deployed firewalls in the district or distributed campuses with Secure Mobile Access (SMA) for remote or at-home players. The firewall can be centrally managed along with other firewalls, connected switches and access points using our Network Security Manager (NSM). DNS and reputation-based content filter rules – administered via NSMs centralized dashboard – provide ease-of-management in preventing student access to harmful websites or inappropriate content while Capture Client extends security to remote or at-home faculty devices.

Schools can use a TZ or NSa firewall and SonicWall Switch to connect to IP phones, cameras, and other smart devices. Alternatively, SonicWall access points, integrated with Wi-Fi 6 for increased connectivity, speed and security, can be connected to the SonicWall Switch and managed via the cloud using Wireless Network Manager or NSM.

Cloud App Security protects SaaS productivity platforms. Capture Security Center adds single-pane-of-glass governance to your entire security platform. Network Access Control (NAC) minimizes security risks by ensuring only authorized and authenticated students, teachers, staff and guests are allowed access to the campus WLAN.

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL