SOLUTION BRIEF

Secure Remote Access for Students, Faculty, and Staff at Scale

Executive Summary

Schools and universities face a number of different potential emergency situations, such as illness, flood, hurricanes, and power outages. Implementing a virtual learning plan for your campus or district is essential to ensuring your systems are capable of conducting classes and lessons while maintaining the minimum days requirement for public K-12 school districts in the face of adversity.

The ability to support students, faculty, and staff with the secure access and appropriate web filtering to study and work remotely is essential to ensuring continuity and security.

For Fortinet customers, our solution includes integrated support for remote access. FortiGate next-generation firewalls (NGFWs) have built-in support for virtual private networks (VPNs), enabling remote students and employees to connect securely to the school or campus network when necessary or required. With secure connectivity, provided by FortiClient, schools and universities can support both cloud-based eLearning and remote work with options to split the traffic as needed and only require a secure connection to the school or university when accessing data in those environments. The majority of education customers may have no requirement to connect directly to the school or university.

The ability to securely support a remote learning policy is an essential component of any continuity and disaster recovery plan. A campus may be incapable of sustaining normal courses and activities onsite, due to a power outage or similar event, or illness or flooding may make it unsafe for students and staff to travel onsite. In the case of K-12, all remote students are still required to be filtered for Children's Internet Protection Act (CIPA) compliance. You could be subject to costly audits at a later date for failing to provide filtering.

In these scenarios, a school must still be capable of supporting secure and filtered remote connectivity. For Fortinet customers, their existing technology deployment already contains this functionality. FortiGate NGFWs have integrated support for IPsec and SSL VPNs, enabling secure connectivity for partners, students, and faculty and staff working from any location.

Securing Remote Users with FortiGate NGFWs

Fortinet solutions are designed to be easy to use from initial purchase through end of life. FortiGate NGFWs include zero-touch deployment functionality. This enables appliances deployed at remote sites, to ensure educational continuity and support for virtual learning through automated setup.

The IPsec and SSL VPN integrated into every FortiGate NGFW offers an extremely flexible deployment model. Remote students and staff can either take advantage of a clientless experience or gain access to additional features through the FortiClient endpoint solution.

Initiatives that issue laptops to students have shown significant positive impact on student test scores in English/language arts, writing, math, and science.[1]

Google for Education and similar services ease administration for teachers, provide new and innovative ways to engage students, and provide students with creative problem-solving skills.[2]

Google for Education and similar services can provide a paperless classroom with easy accessibility, and can help K-12 students transition to other learning management systems used in higher education.[3]

Findings show that eLearning increases retention rates 25% to 60% while retention rates of face-to-face training are only 8% to 10%.[4]

The Fortinet Security Fabric takes advantage of a common Fortinet operating system and an open application programming interface (API) environment to create a broad, integrated, and automated security architecture. With the Fortinet Security Fabric, all devices, including those deployed remotely to support remote learning and work, can be monitored and managed from a single pane of glass. From a FortiGate NGFW or a FortiManager centralized management platform deployed in the main campus, the network and security team can achieve full visibility into all connected devices, regardless of their deployment situation.

In the event of a natural disaster or other event that disrupts normal operations, an organization must be capable of rapidly transitioning to a fully remote online education system. Table 1 shows the number of concurrent VPN users that each model of the FortiGate NGFW can support.

Beyond offering encryption of data in transit, via an IPsec or SSL VPN and FortiClient, Fortinet solutions offer a number of other features that can help an organization to secure its remote workforce. These features include:

- **Data loss prevention (DLP).** FortiGate and FortiWiFi provide DLP functionality for remote workers, which is essential for teleworking executives with frequent access to sensitive company data.
- **Endpoint security.** FortiEDR provides advanced threat protection for remote workers' computers including automated remediation.
- **Advanced threat protection.** FortiSandbox offers analysis of malware and other suspicious content within a sandboxed environment before it reaches its destination.
- **Wireless connectivity.** FortiAPs provide secure wireless access at remote work locations with full integration and configuration management in a single pane of glass.
- **Device access management.** FortiNAC is able to enforce bring-your-own-device (BYOD) policies even over remote VPN connections, allowing the school to control what types of devices can connect and what access they receive.
- **Telephony.** FortiFone is a secure, Voice over IP (VoIP) telephony solution, whose traffic is secured, managed, and monitored by a FortiGate NGFW.
- **Software-defined wide-area network (SD-WAN).** Secure SD-WAN functionality integrated into every FortiGate NGFW provides direct-to-internet connectivity for cloud-based resources and optimization of VoIP and video traffic.

Model	Concurrent SSL VPN Users	Concurrent IPsec VPN Users	Managed FortiAPs (Tunnel Mode)
100E	500	10,000	32
100F	500	16,000	64
300E	5,000	50,000	256
500E	10,000	50,000	256
600E	10,000	50,000	512
1100E	10,000	100,000	2,048
2000E	30,000	100,000	2,048
All Larger Models*	30,000	200,000	2,048
*3300E supports 1,024 Tunnel Mode APs			

Table 1: Number of concurrent VPN connections supported by various models of FortiGate NGFWs.

Use Cases for Fortinet Products Supporting Remote Education, Teaching, and Work

Not every student or employee in education institutions requires the same level of access to resources when learning and working remotely. Fortinet provides tailored solutions for every remote student, teacher, and administrator:

1. **Student.** Most students and teachers will primarily require access to a learning management system, generally provided via the cloud. They might also require access to email, internet, teleconferencing, and file sharing from home. This includes access to Software-as-a-Service (SaaS) services in the cloud, such as Google for Education, and online teleconferencing such as Google Hangouts, Microsoft Teams, and Zoom.

Students, teachers, and IT administrators can connect using FortiGate integrated SSL VPN client software or via the FortiClient endpoint security solution. They may also require authentication to Google for Education or Microsoft AD.

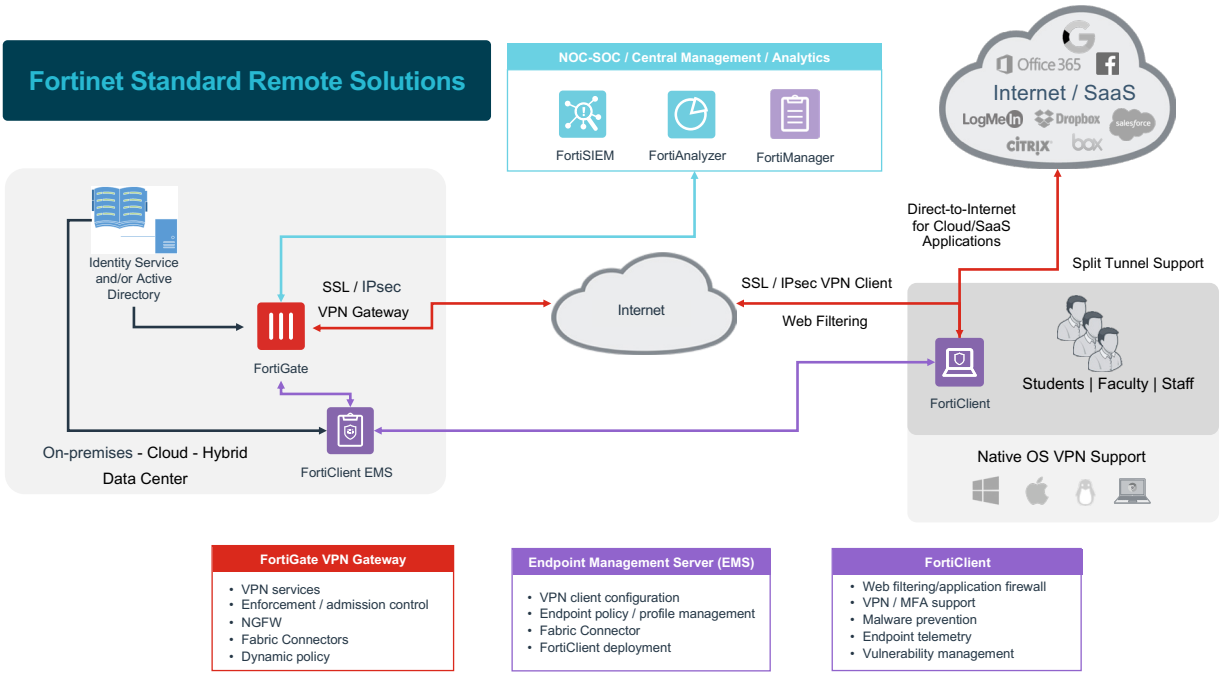

Figure 1: Fortinet solution deployment for standard students, faculty, and staff.

The Fortinet Security Fabric solution FortiAuthenticator provides single sign-on (SSO) to Google and Microsoft environments and allows for multi-factor authentication (MFA). The split tunnel capabilities of the FortiClient allow for the most flexible deployment while maintaining web filtering and security for all traffic. Even when connecting directly to the internet, web-filtering and malware policies are enforced and auditable. This includes SSO capabilities with Microsoft and Google.

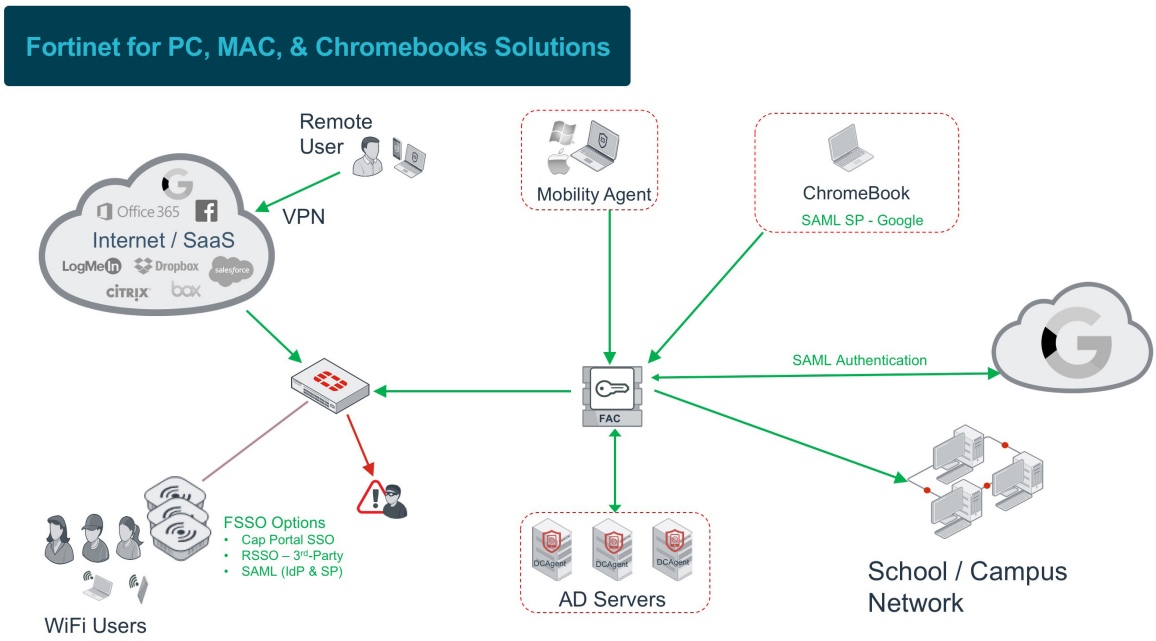

Figure 2: Fortinet SSO solution deployment for Microsoft and Google with FAC (FortiAuthenticator).

2. **Advanced administrators, and faculty and staff.** These users require access to a learning management system, generally provided via the cloud. Staff users may require access to function-specific capabilities (HR, administration, etc.) from their remote worksite. Faculty and staff can also connect to the organization using the FortiGate integrated IPsec or SSL VPN client or via the FortiClient endpoint solution. Secure SD-WAN capabilities integrated into every FortiGate NGFW enable secure, direct-to-internet access to SaaS resources.

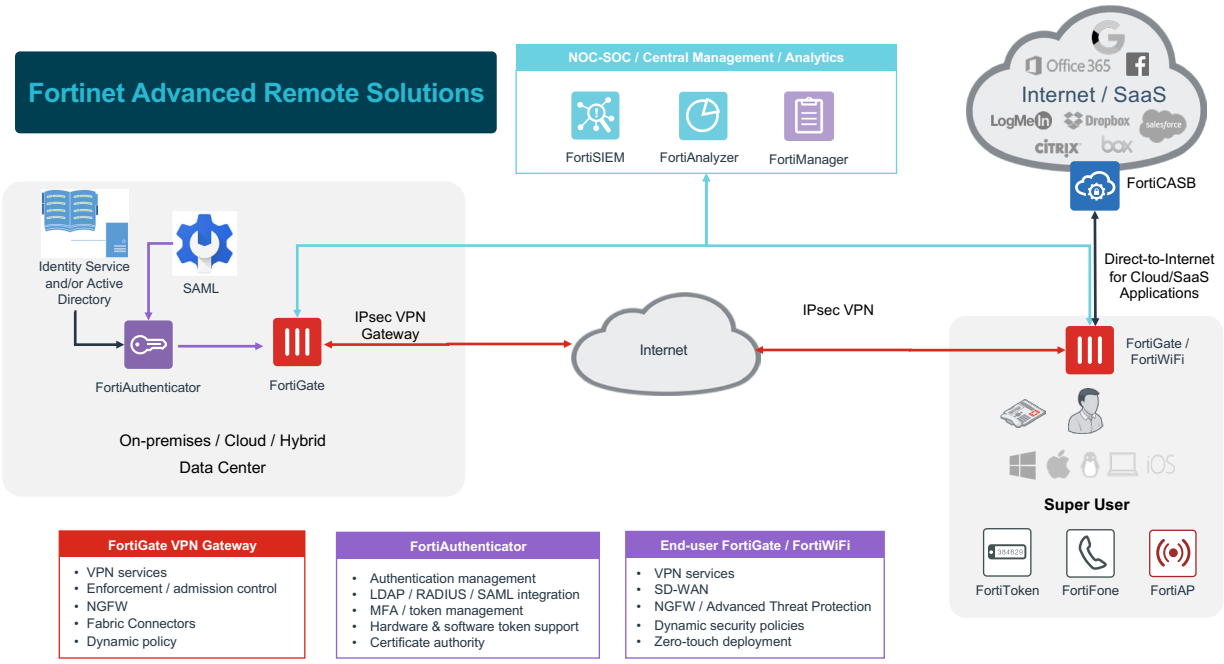

Figure 2: Fortinet SSO solution deployment for Microsoft and Google with FAC (FortiAuthenticator).

Achieve Full Security Integration with Fortinet Solutions

The Fortinet Security Fabric enables seamless integration of an organization's remote workforce and student body. All Fortinet solutions are connected via the Fortinet Security Fabric, enabling single-pane-of-glass visibility, configuration, and monitoring. A number of Fabric connectors, an API environment, DevOps community support, and a large extended Security Fabric ecosystem enable integration with over 250 third-party solutions as well.

This is essential when an organization is preparing a business continuity plan, since a school may be forced to transition over to a fully remote workforce with little or no notice. Single-pane-of-glass visibility and management of an organization's security architecture ensures that support for telecommuting does not jeopardize an organization's cybersecurity.

Fortinet offers a number of solutions capable of supporting and securing a remote workforce. These solutions are available via flexible procurement options:

- **Bring-your-own-license (BYOL).** Licenses purchased from a Fortinet channel partner for different products are transferrable across platforms though the BYOL program.
- **Pay-as-you-go (PAYG).** Fortinet solutions like FortiGate NGFW and FortiWeb Cloud web application firewalls (WAF)-as-a-Service can be consumed using a PAYG on-demand usage model from the Amazon Web Services (AWS) and Google Cloud Marketplaces.

The following solutions are part of the Fortinet Security Fabric and support secure telework:

- **FortiClient.** FortiClient strengthens endpoint security through integrated visibility, control, and proactive defense and enables organizations to discover, monitor, and assess endpoint risks in real time.
- **FortiGate (BYOL, PAYG).** FortiGate NGFWs utilize purpose-built cybersecurity processors to deliver top-rated protection, end-to-end visibility and centralized control, as well as high-performance inspection of clear-texted and encrypted traffic.
- **FortiWiFi.** FortiWiFi wireless gateways combine the security benefits of FortiGate NGFWs with a wireless access point, providing an integrated network and security solution for teleworkers.

- **FortiFone.** FortiFone provides unified voice communications with VoIP connectivity that is secured and managed via FortiGate NGFWs. The FortiFone soft client interface allows users to make or receive calls, access voicemail, check call history, and search the organization's directory right from a mobile device.
- **FortiToken.** FortiToken confirms the identity of users by adding a second factor to the authentication process through physical and mobile application-based tokens.
- **FortiAuthenticator.** FortiAuthenticator provides centralized authentication services including single sign-on services, certificate management, and guest management.
- **FortiAP.** FortiAP delivers secure, wireless access to distributed enterprises and remote workers and can be easily managed as a physical appliance or via the cloud.
- **FortiWeb Cloud (BYOL, PAYG).** Fortinet WAFs protect hosted web applications from both known vulnerabilities and zero-day threats using multilayered and correlated detection methods.
- **FortiManager (BYOL).** FortiManager provides single-pane-of-glass management and policy controls across the extended enterprise for insight into networkwide, traffic-based threats. This includes features to contain advanced attacks as well as scalability to manage up to 10,000 Fortinet devices.
- **FortiAnalyzer (BYOL).** FortiAnalyzer provides analytics-powered cybersecurity and log management to enable improved threat detection and breach prevention.
- **FortiSandbox (BYOL, PAYG).** Fortinet sandboxing solutions offer a powerful combination of advanced detection, automated mitigation, actionable insight, and flexible deployment to stop targeted attacks and subsequent data loss.

A Secure Foundation Ensures Education Continuity

Preparing for learning and operational continuity and disaster recovery is vital for school districts and universities. An important component of this is the ability to support a fully remote classroom and workforce with little or no notice.

When developing virtual learning continuity plans, it is essential to ensure that the school or university has the resources in place to secure remote students and staff. Fortinet solutions are easily deployable and configurable and enable any school district or university to maintain full security visibility and control regardless of their deployment environment.

[1] Leo Doran and Benjamin Herold, "1-to-1 Laptop Initiatives Boost Student Scores, Study Finds," Education Week, May 17, 2016.
[2] "Helping K-12 educators make a greater impact," Google for Education.
[3] Matthew Lynch, "10 Benefits of Google Classroom Integration," The Tech Edvocate, September 4, 2018.
[4] Karla Gutierrez, "Facts and Stats That Reveal The Power Of eLearning," SHIFT eLearning, April 7, 2016.

FORTINET

www.fortinet.com

March 26, 2020 10:52 AM
623285-0-0-EN
Map:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2020:SB-Secure-Remote-Access-for-Student:sb-security-remote-access-for-student Folder:sb-security-remote-access-for-student-032620-1052am