SOLUTION BRIEF

Security and Networking for Healthcare Emergency Response

Executive Summary

When healthcare organizations need to deploy emergency services outside of established facilities to respond to specific needs like field diagnosis or testing, it is critical to ensure secure and reliable networking. Implementing a secure emergency deployment plan is essential to scale vital operations in the face of adversity.

To enable proper emergency response and business continuity, employees in temporary or remote locations must have secure access to medical information and devices. While infrastructure, capacity, and coverage requirements vary from hospitals to clinics and everything in between, security, reliability, and manageability must be consistent with enterprise controls. It can be very difficult to successfully deploy cybersecurity solutions across all of these environments, as most solutions are built for one environment. As such, they do not scale well from the data center or cloud to a remote mobile site.

Fortinet offers an integrated solution to support remote or emergency deployment. FortiGate next-generation firewalls (NGFWs) have built-in support for IPsec virtual private networks (VPNs), enabling remote providers to connect securely to the company network. Fortinet access points (APs) provide outdoor, weather-resistant connectivity with cellular or wired connection. With secure endpoint connectivity provided by FortiClient, organizations can securely support remote telemedicine and maintain business continuity.

Highlights:

Quick and Easy Deployment
- Preconfigured
- User or field-engineer deployed
- Zero-touch deployment

Flexible Management and Scalability
- Cloud and/or local device OS
- Built-in monitoring and reporting
- Add services when needed—monitoring, security, etc.

Low Cost Without Compromise
- Consistent user experience
- Cost-effective

Temporary Healthcare Sites Require Secure Networking

Whether healthcare staff is at a hospital or a remote clinic, quick access and a consistent experience are required. Staff members need seamless access to centralized medical records, local and remote clinical applications, and many other resources. Secure mobility between locations requires sophisticated identity management integrated with a comprehensive security solution. But remote care delivery must still make economic sense, and the cost and complexity of provisioning and maintaining secure Wi-Fi access and VPN connectivity at remote sites is often a barrier.

Fortinet Solves Remote Healthcare Challenges

For small or temporary sites, FortiWiFi UTM appliances combine an entry-level FortiGate with a full-featured AP. This network in a box is equipped with a VPN and comprehensive security suite. A full range of APs is available to provide ample options for high-density indoor coverage. And, ruggedized outdoor models can be deployed in even the most extreme conditions.

Fortinet's comprehensive solution delivers:

Ease of deployment

An entire wireless infrastructure can be deployed quickly and easily, without additional hardware, and without sacrificing security. Deployed APs are registered to FortiCloud and immediately adopt the organization's defined security policies. This seamless security posture ensures that all clinical locations are properly secured at deployment, leaving no unplanned security gaps.

Security threat management

Comprehensive protection against wireless protocol and RF attacks, malware, keyloggers, viruses, and zero-day attacks is required at user entry points to the network. The closer security is to the end-user, the better they and the network are protected.

Up-to-date protection

Cutting-edge automated network protection updates from Fortinet's accomplished security research team, FortiGuard Labs, assures some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and other threats.

Application control

Complete application visibility and precision control of the network, with signatures for over 4,000 applications, lets hospitals and clinics prioritize, throttle, or block applications at a group, user, or device level.

Unified management

The same (or different) policies can be administered to both wired and wireless networks. Single-pane-of-glass management of security and networking saves time and resources.

Deployment Details

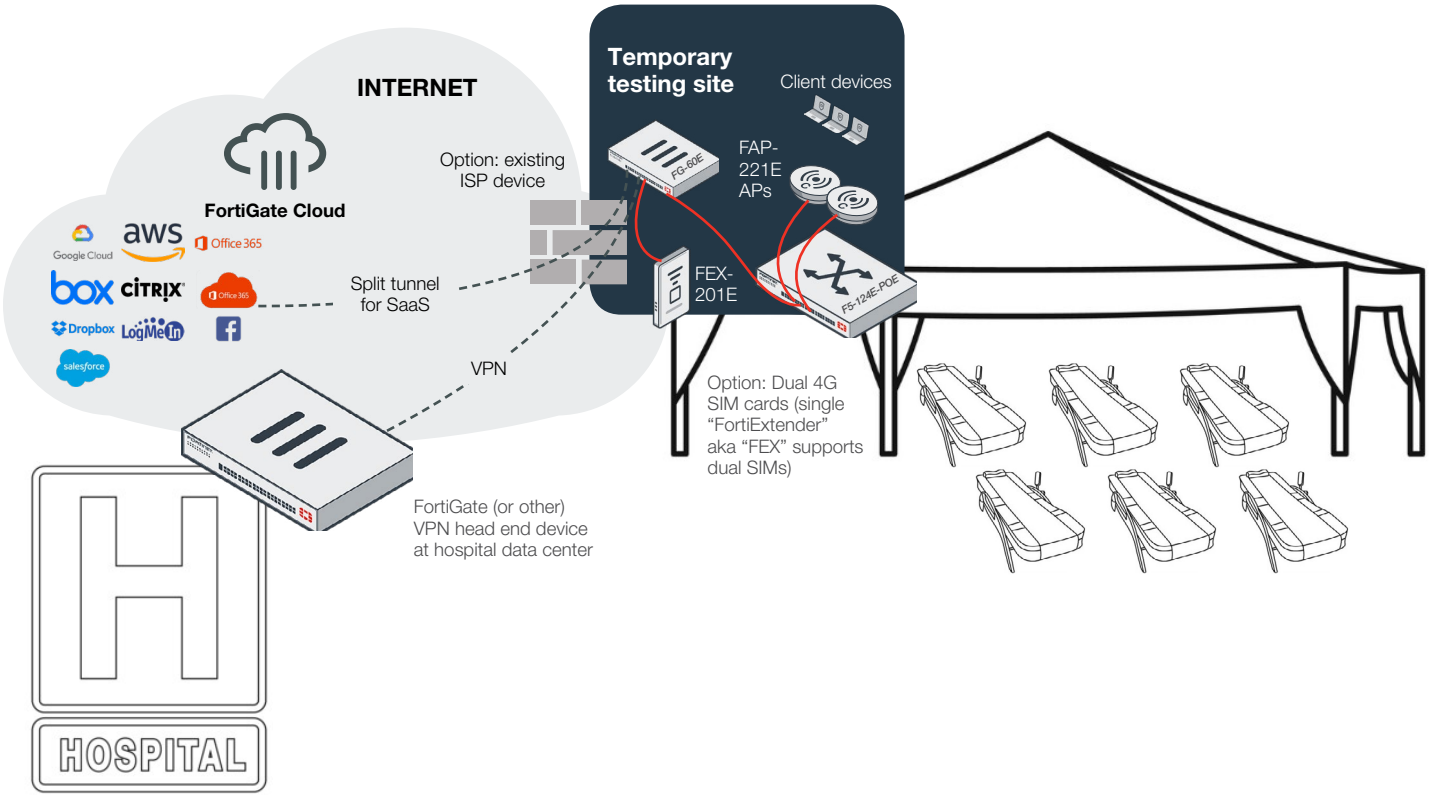

Figure 1: Mobile pandemic testing/triage site deployment.

Automated provisioning enables fast and easy deployment:

1. The first step is for the FortiExtender to power up and establish a data link to a mobile phone tower. Next, FortiGate at the mobile site should power up to initialize.
2. As part of powering up, the FortiGate will query the FortiGate Cloud. The FortiGate Cloud can be preconfigured by Fortinet to recognize each FortiGate calling and assign it to the appropriate customer. At that point, either a configuration is pushed from FortiGate Cloud or the FortiGate is directed to the appropriate FortiManager designated by the customer to get the right configuration.
3. A VPN tunnel is established from the mobile site to the hospital system headquarters. A split tunnel permits direct, secure access to Software-as-a-Service (SaaS) applications from the mobile site.

Quickly Deploy Secure Healthcare Services with Fortinet

Fortinet delivers a fast, scalable, cost-effective solution for small or temporary healthcare sites that enables the same high-performance security and networking that large hospitals depend on. There are four primary components in this solution:

- **FortiGate.** 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.
- **FortiSwitch.** FortiSwitch switches deliver a secure Ethernet solution that can be easily managed from a FortiGate or via the cloud.
- **FortiAP.** FortiAP access points deliver secure, wireless access that can be easily managed from a FortiGate or via the cloud.
- **FortiExtender.** FortiExtender is an LTE connectivity appliance that can provide a primary or secondary wide-area network (WAN) link to a FortiGate using the data network of mobile phone providers.

These components integrate into the Fortinet Security Fabric to ensure consistent policy enforcement and faster response to threats. Integration also makes it easy to add more security controls such as endpoint protection or access authentication at any time.

April 1, 2020 6:26 AM

633042-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Healthcare Emergency Response\sb-security-and-networking-for-healthcare-emergency-response-V1-412020-519AM