SOLUTION BRIEF

Protecting NextGen 911 Systems with the Fortinet Security Fabric

Executive Summary

Cyber criminals are increasingly targeting emergency response networks throughout the United States. The risk to Next Generation (NextGen) 911 systems posed by advanced malware and denial-of-service (DoS) attacks highlights the critical need for local governments to secure emergency response networks. The Fortinet Security Fabric can help governments modernize their infrastructure while mitigating the risks of cyberattacks and system breaches.

Attacks Against 911 Emergency Systems Are Increasing

In the last three years, there have been more than 40 cyberattacks across the U.S. specifically targeting 911 dispatch centers.[1] This includes the widely publicized hack of Baltimore's 911 system, which caused a temporary disruption that forced call center support staff to manually manage emergency calls.[2] To make matters worse, these incidents are poised to multiply as traditional 911 networks transition to NextGen 911 systems, which enable voice, video, text, and data to be received via IT networks.

Even though the same three-digit number (911) can be dialed anywhere in the U.S. when someone needs help, the underlying infrastructure of the country's 911 network is currently a patchwork of disparate systems. The U.S. has 5,700 separate state and local public safety answering points (PSAPs), each of which operates differently and typically provides service at the county level.[4] Traditional PSAPs rely on legacy technologies, which function as closed internal networks that have few interconnections with other systems. This reduces the attack surface, but it also makes technology modernization more challenging.

In Tennessee, a ransomware attack demanding 2,000 BTC shut down an entire 911 dispatch system—disrupting normal operations for three days as the system was rebuilt.[3]

NextGen 911 systems use Internet Protocol (IP)-based networks to enhance the response capabilities of call centers and public safety agencies. They enable PSAPs to perform call transfer and data sharing and allow them to accept calls from mobile, text, and voice applications. But NextGen 911 systems also come with increased security risks, including outages due to DoS attacks that overrun the service provider or infrastructure. Other security threats include malware, ransomware, and spoofing, which involves an unauthorized device disguising itself as an authorized device.

As shown in Figure 1, NextGen 911 systems are typically self-contained, proprietary solutions that communicate with text control centers (TCCs) via the Message Session Relay Protocol (MSRP). The MSRP is used to facilitate large-scale instant messaging—including transferring large files such as video and images within NextGen 911 systems. But TCCs cannot perform security inspections on MSRP messages, which may contain malicious URLs, malware attachments, and other security threats.

To address the critical threats targeting NextGen 911, public safety agencies need to adopt cybersecurity that is designed to protect MSRP.

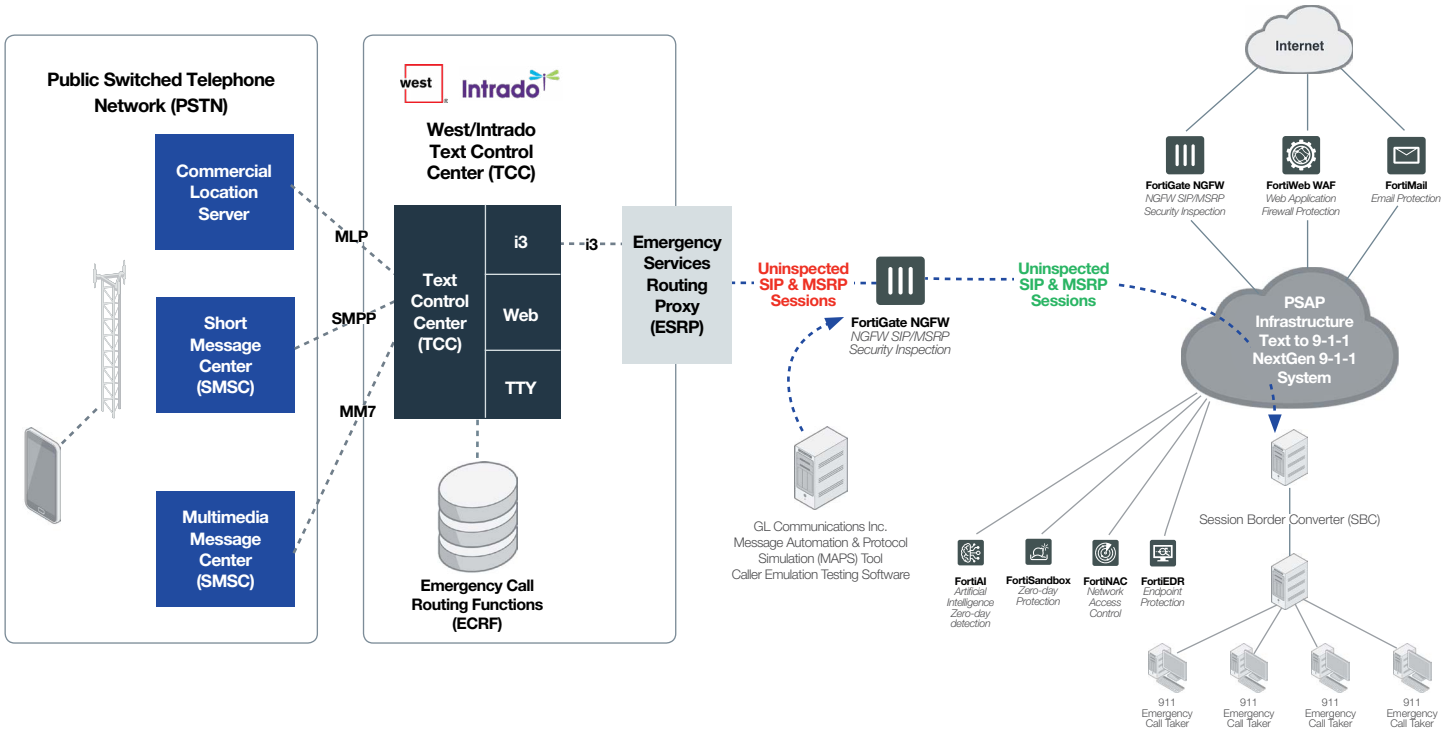

Figure 1: NextGen 911 infrastructure diagram.

The Advantage of an MSRP-focused Security Solution

The best way to protect NextGen 911 is to perform security inspections on MSRP messages before they enter these systems. To do this, public safety agencies need cybersecurity that features an **MSRP decoder**. This critical functionality inspects MSRP traffic for threats and helps coordinate security reinforcement. PSAPs need advanced threat detection capabilities, and an MSRP protocol decoder can provide this by applying existing intrusion prevention system (IPS) signature sets to MSRP traffic to surface known threats and block this malicious traffic.

For example, automated DoS attacks can generate MSRP messages much faster than a human can type, which can overwhelm NextGen 911 systems and block actual emergency calls from getting through. The addition of an MSRP protocol decoder tracks the rate of MSRP messages coming into the NextGen 911 system. Cybersecurity defenses can then alert administrators that there is a problem—or if a certain threshold is reached, automated actions can be triggered, such as dropping those messages. An MSRP decoder also can inspect text messages or images for hidden security threats (e.g., malware) and inspect for embedded malicious URLs.

This solution bolsters security by creating redundancy and ensuring PSAPs have no single point of failure. An MSRP decoder also makes PSAPs more resilient because it can be scaled to support increases in traffic growth associated with multimedia messages, while giving them access to threat intelligence and insights they can use to combat future security threats.

As of this writing, an MSRP decoder is something that most point security solutions on the market cannot offer and it is not enough on its own to protect these critical systems.

The extrapolated results of a recent simulation indicate that 200,000 bots would be able to overwhelm the 911 systems of the entire United States.[5]

NextGen 911 systems are susceptible to man-in-the-middle attacks, DoS attacks, and unauthorized network access. They are also vulnerable to insider threats, attacks from malicious applications, and unauthorized data access.[6]

Enter the Fortinet Security Fabric for NextGen 911 Infrastructure

Rather than adopting several different point solutions with narrow capabilities, local governments need an integrated cybersecurity platform with products that automate key processes using artificial intelligence (AI) and machine learning (ML). Among many benefits, the **Fortinet Security Fabric** includes MSRP decoding capabilities.

Fortinet secure MSRP communication features include:

- Rate limiting for MSRP messages
- Message rate control on Session Initiation Protocol (SIP) and MSRP based on mobile device number (MDN)
- Text message inspection for malware-based attacks like cross-site scripting (XSS) and SQL injection
- Inspection for embedded malicious URLs
- Inspection for embedded malicious files
- Applying existing IPS signature sets to MSRP traffic
- Detection and flagging of repeated MSRP messages

Key Fortinet Solutions for NextGen 911

The Fortinet Security Fabric is comprised of integrated security solutions that share information in real time to protect network infrastructure. Depending on the specific needs of the NextGen 911 deployment, the Fortinet Fabric-connected solutions ensure continuous, end-to-end protection and real-time threat intelligence sharing to repel coordinated, multipronged attacks across the entire infrastructure.

Securing any NextGen 911 environment starts with the **FortiGate next-generation firewall (NGFW)**. Next-generation firewalls filter network traffic to protect an organization from external threats. Maintaining features of stateful firewalls such as packet filtering, virtual private network (VPN) support, network monitoring, and IP mapping features, NGFWs also possess deeper inspection capabilities that give them a superior ability to identify attacks, malware, and other threats. NGFWs provide organizations with application control, intrusion prevention, and advanced visibility across the network. As the threat landscape continues to develop rapidly, traditional firewalls fall further behind and put your organization at risk. NGFWs not only block malware but also include paths for future updates, giving them the flexibility to evolve with the landscape and keep the network secure as new threats arise. Benefits of FortiGate include:

- **Application Control:** Fortinet boasts one of the largest applications databases to safeguard your organization from risky applications, and allows you visibility and control of applications running in your network.
- **Intrusion Prevention:** Stop unwanted attempts to access your network that target vulnerabilities and configuration gaps. Fortinet blocks over 10 million intrusion attempts per minute.
- **Web Filtering:** Protect your organization by blocking access to malicious, hacked, or inappropriate websites with FortiGuard Web Filtering. Web filtering is the first line of defense against web-based attacks. Malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.
- **Advanced Threat Protection:** Stop malicious files and payloads moving into your network with FortiGuard's leading advanced malware, antivirus, and sandboxing capabilities.
- **Text Message Protection:** MSRP inspection is done on the FortiGate, which allows text messages to be decoded in transit and analyzed for malicious content.

FortiGates also include a number of benefits specific to security for Session Initiated Protocol (SIP):

- **Whitelisting/Blacklisting:** FortiGates have the ability to whitelist and/or blacklist specific Mobile Device Numbers (MDNs) for new SIP sessions.
- **Advanced Voice over IP protection:** The FortiOS SIP Application Level Gateway (ALG) protects Voice over IP (SIP and session description protocol [SDP]) services in Unified Communication and next-generation network (NGN)/IP multimedia systems (IMS) networks with the following advanced VoIP defense mechanisms.
- **Deep SIP message inspection (also called deep SIP header inspection):** Verifies SIP and SDP header syntax and protects SIP servers from potential SIP Fuzzing attacks. When a violation is detected, FortiOS can impose counter measures and can also send automatic SIP response messages to offload processing from the SIP server.
- **SIP message rate limiting:** Allows rate limiting of SIP messages per SIP request method. This prevents a SIP server from overload or from DoS attacks using particular SIP methods. For example, FortiOS can protect SIP servers from a flood of SIP REGISTER or INVITE messages, which can be caused by a DoS attack or a flash crowd.

The Department of Homeland Security (DHS) recommends that public safety agencies look for NextGen 911 protection that adheres to the NIST Cybersecurity Framework's risk-based approach to improving the security of critical infrastructure.[7]

- **Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) pin holing:** RTP pin holing only forwards RTP/RTCP packets that conform to the particular session description of the associated SIP dialog. If a SIP dialog is finished, FortiOS automatically closes the pinhole. RTP/RTCP pin holing is supported by FortiASIC acceleration and achieves high packet throughput at low jitter and delay.
- **Stateful SIP dialog tracking:** FortiOS tracks SIP message sequences and prevents unwanted SIP messages that are not related to a particular SIP dialog. For instance, FortiOS can detect malicious SIP BYE messages that do not conform with the associated context of the SIP dialog.
- **Inspecting SIP over Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (secure SIP):** Some SIP phones and SIP servers use SSL or TLS to encrypt SIP signaling traffic. To allow SIP over SSL/TLS calls to pass through the FortiGate unit, the encrypted signaling traffic has to be unencrypted and inspected. FortiOS intercepts and unencrypts and inspects the SIP packets. Allowed packets are then re-encrypted and forwarded to their destination.
- **Inspecting SIP on multiple ports:** FortiOS can detect and inspect SIP and SDP user datagram protocol (UDP) and TCP sessions and SIP SSL sessions and you can configure the ports that the SIP ALG monitors for these sessions. In addition, you can configure two different ports for SIP UDP sessions and two different ports for SIP TCP sessions. The port configuration can be changed without affecting other parts of the SIP configuration.
- **Carrier-grade protection:** To protect VoIP infrastructure in carrier networks, FortiOS complies with typical carrier requirements for availability and robustness.
- **High availability:** FortiOS supports a hot failover configuration with an active and a standby FortiGate device. FortiOS dynamically updates the context on the standby unit with SIP and RTP related data. This enables the standby unit to takeover stable voice calls in case of a planned or unplanned outage or failover of the active unit.
- **Geographical redundancy of SIP servers:** In FortiOS SIP server cluster configurations the active and standby units can be deployed in different geographical locations. This configuration prevents a total outage of a SIP server infrastructure if one location goes offline. FortiOS supports the detection of SIP server outages (loss of heartbeats) and a redirect of SIP messages to the redundant SIP server location.
- **Logging and Reporting:** FortiOS can log call related information internally or to an external SYSLOG or FortiAnalyzer unit. This includes event logs that show particular SIP-related attacks or syntax violations with SIP messages or logs that summarize call statistics.

- **Network Address Translation (NAT)/Network Address and Port Translation (NAPT):** FortiOS performs configurable network address translation for IP addresses in the SIP and SDP header. The SIP ALG follows the configured NAT addresses in firewall virtual IPs and changes SIP header IP addresses accordingly. RTP NAT is controlled by SIP/SDP and the firewall policy. This allows translating an unlimited number of IP addresses without adding specific RTP policies.
- **Header manipulation:** FortiOS SIP and SDP header manipulation supports SIP NAT through FortiGate units configured as NAT firewalls.

A **FortiSandbox** inspects traffic and safely detects malicious content (such as malware) before it can exploit the network. FortiSandbox can be added as a physical appliance for closed deployments or via the cloud for those that allow it. The new Fortinet FortiAI artificial intelligence analysis solution can work in tandem with FortiSandbox to offer additional protection against emerging attack variants and zero-day threats.

There is often also an email and/or web server within NextGen 911 environments so that communications can be sent to emergency centers via public-facing email or webpage form. **FortiMail** and **FortiWeb** solutions can be integrated with FortiSandbox to help protect against malicious content from those sources.

The infrastructure itself also needs specific defenses in place to repel access-based attacks. **FortiNAC** (network access control) and **FortiEDR** (endpoint detection and response) solutions help secure threat exposures via users and connected devices.

- **FortiNAC:** The proliferation of Internet-of-Things (IoT) devices has made it necessary for organizations to improve their visibility into what is attached to their networks. They need to know every device and every user accessing their networks. IoT devices enable digital transformation initiatives and improve efficiency, flexibility, and optimization. However, they are inherently untrustworthy, with designs that prioritize low cost over security. FortiNAC provides the network visibility to see everything connected to the network, as well as the ability to control those devices and users, including dynamic, automated responses.
- **FortiEDR:** Advanced attacks can take just minutes, if not seconds, to compromise the endpoints. First-generation EDR tools simply cannot keep pace. They require manual triage and responses that are not only too slow for fast moving threats but also generate a huge volume of indicators that burden already overstretched security teams. Further, legacy EDR tools drive up the cost of security operations and can slow processes, negatively impacting business. FortiEDR delivers advanced, real-time threat protection for endpoints both pre- and post-infection. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR helps organizations stop breaches in real time automatically and efficiently, without overwhelming security teams with a slew of false alarms or disrupting business operations.

Connections to the network (both physical and wireless) also need to be secured in NextGen 911 environments. **FortiAP** protects wireless access points and **FortiSwitch** secures Ethernet connectivity throughout the infrastructure with seamless, low-cost deployment.

Many 911 centers still rely on archaic private branch exchange (PBX) phone systems and T1/TDM technology that has been around for 25-30 years or more. The cost effectiveness of a **FortiVoice** solution can help these organizations migrate to Voice over IP/Session Initiation Protocol (VoIP/SIP) systems where competing solutions may be too cost prohibitive.

The Fortinet Security Fabric unifies all these parts of the NextGen 911 security infrastructure, shares both local and global threat information, and then automates responses in real time. The Fortinet approach applies the latest intelligence from **FortiGuard Labs**—one of the largest and most accomplished security research and analyst teams in the industry—which studies every critical area of the threat landscape including malware, botnets, mobile, and zero-day vulnerabilities.

A Unified Approach To Protecting Emergency Services

Cybersecurity has become an essential aspect of public safety, and adopting the right security solutions can empower local governments with the capabilities they need to render potentially lifesaving aid to constituents when they need it most. As more localities transition to NextGen 911 systems, they need a cybersecurity partner that understands the challenges and specific requirements of their IT infrastructures.

With the Fortinet Security Fabric, local governments get a security platform that provides end-to-end visibility and offers unique features like MSRP protection, as well as proactive detection and prevention response capabilities mapped to NIST Framework standards. Using this approach, PSAPs can also scale their IT infrastructure as new data sources emerge that need to be routed through NextGen 911 systems.

The Fortinet approach to advanced MSRP-focused security makes 911 networks more resilient, especially as they modernize to deliver more robust and responsive services.

A Unified Approach To Protecting Emergency Services

Cybersecurity has become an essential aspect of public safety, and adopting the right security solutions can empower local governments with the capabilities they need to render potentially lifesaving aid to constituents when they need it most. As more localities transition to NextGen 911 systems, they need a cybersecurity partner that understands the challenges and specific requirements of their IT infrastructures.

With the Fortinet Security Fabric, local governments get a security platform that provides end-to-end visibility and offers unique features like MSRP protection, as well as proactive detection and prevention response capabilities mapped to NIST Framework standards. Using this approach, PSAPs can also scale their IT infrastructure as new data sources emerge that need to be routed through NextGen 911 systems.

The Fortinet approach to advanced MSRP-focused security makes 911 networks more resilient, especially as they modernize to deliver more robust and responsive services.

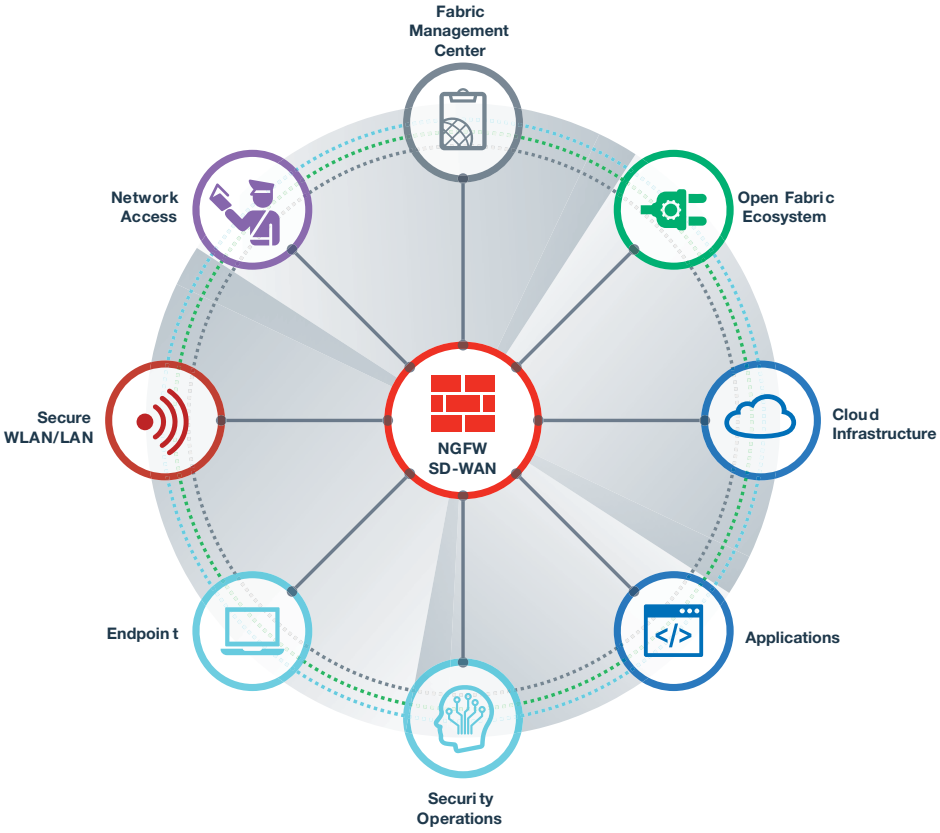

Figure 2: A Fortinet Security Fabric deployment for securing NextGen 911 infrastructure.

[1] Dan Retzer, "911 dispatch centers can take multiple steps to combat cyberattacks," Urgent Communications, November 15, 2019.

[2] "Baltimore's 911 emergency system hit by cyberattack," NBC News, March 28, 2018.

[3] John Schuppe, "Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?," NBC News, April 3, 2018.

[4] Jill C. Gallagher, "Next Generation 911 Technologies: Select Issues for Congress," Congressional Research Service, July 9, 2018.

[5] Byron Mühlberg, "Next Generation 911 Systems Vulnerable to DDoS Attacks," CPO Magazine, March 27, 2020.

[6] Phil Goldstein, "The Cybersecurity Needed for NG911 Systems," StateTech, October 31, 2019.

[7] Ibid.

October 24, 2020 3:10 AM

777920-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\BOFU - Securing NG911 Solution\[UPDATE - 10162020]\sb-FA-protecting-nextgen-911-systems-10162020\sb-FA-protecting-nextgen-911-systems-10162020