SOLUTION BRIEF

Protecting Next-Generation 911 and First-Responder Systems

Executive Summary

Cybercriminals are increasingly targeting emergency response networks throughout the United States. The risk to first-responder and next-generation 911 (NG911) systems posed by advanced malware and denial-of-service (DoS) attacks highlights the critical need for state and municipal governments to secure their emergency response networks. Fortinet can help governments modernize their networking and security infrastructure while mitigating the risks of cyberattacks and system breaches.

Increasing Attacks Against First-Responder and 911 Systems

Cyberattacks against emergency dispatch systems continue to cause extremely dangerous problems for city, county, and even national call centers. Recent attacks include New York (Suffolk County),[2] Texas (Fort Worth),[3] and a nearly daylong outage of the nation's new 988 mental health helpline.[4] The New York Times remarked about the Suffolk County attack: "It is a situation that experts say not only reveals the county's vulnerability but also presents an ominous warning for a nation unprepared for crippling online threats."[5] To make matters worse, these incidents are poised to multiply as 911 networks transition to NG911 systems—enabling voice, video, text, and data to be received via IT networks.

A recent cyberattack shut down 911 systems in Suffolk County, New York—reducing employees to using pencil and paper while leveraging outside first-responder resources from New York City.[1]

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. now has over 5,700 primary and secondary public safety answering points (PSAPs), each of which operates differently and typically provides service at the county level.[6] 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 also makes technology modernization more challenging.

NG911 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 NG911 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, NG911 systems are typically self-contained, proprietary solutions that communicate with text control centers (TCCs) via the Message Session Relay Protocol (MSRP). MSRP facilitates large-scale instant messaging, including transferring large files such as video and images within NG911 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 NG911, public safety agencies must adopt cybersecurity designed to protect MSRP.

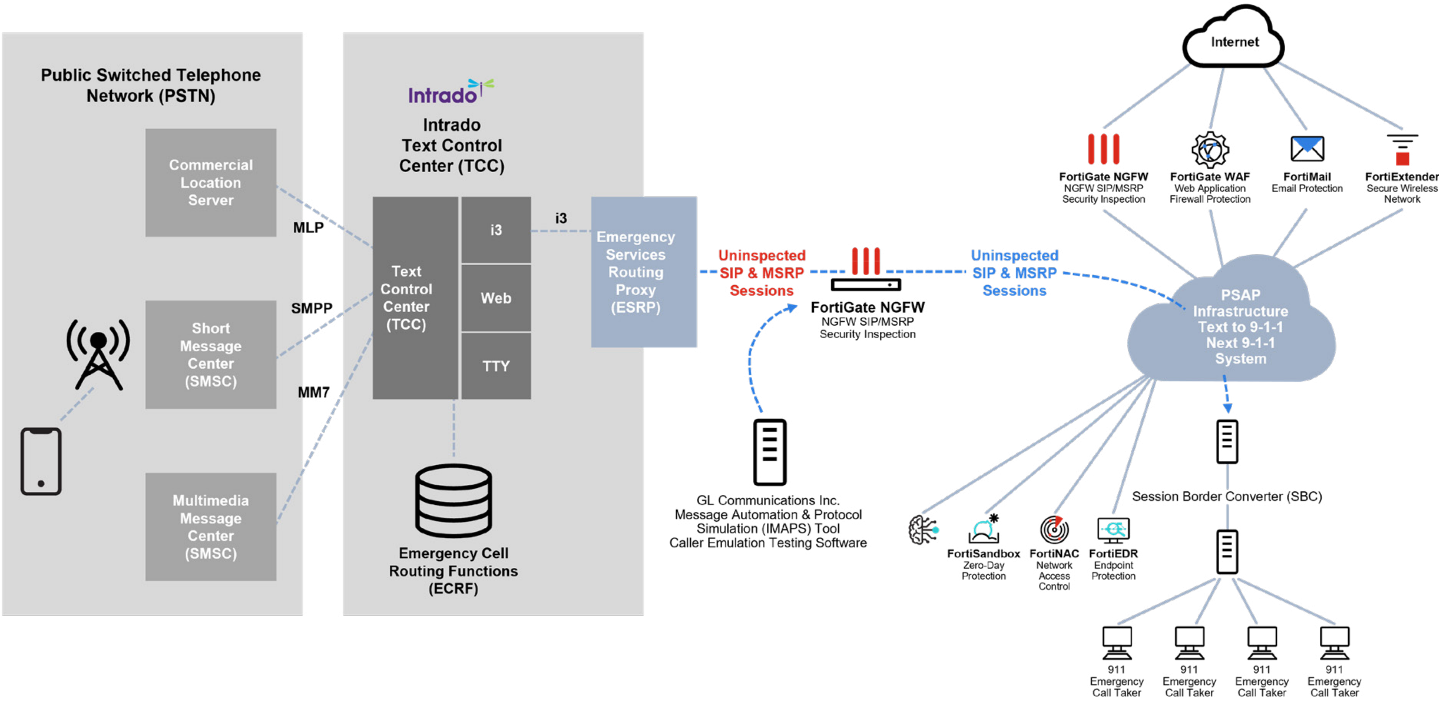
Public Switched Telephone Network (PSTN)
Commercial Location Server
Short Message Center (SMSC)
Multimedia Message Center (SMSC)
MLP
SMPP
MM7
Intrado
Intrado Text Control Center (TCC)
Text Control Center (TCC)
i3
Web
TTY
i3
Emergency Cell Routing Functions (ECRF)
Emergency Services Routing Proxy (ESRP)
Uninspected SIP & MSRP Sessions
FortiGate NGFW
NGFW SIP/MSRP Security Inspection
Uninspected SIP & MSRP Sessions
GL Communications Inc.
Message Automation & Protocol Simulation (IMAPS) Tool
Caller Emulation Testing Software
Internet
FortiGate NGFW
NGFW SIP/MSRP Security Inspection
FortiGate WAF
Web Application Firewall Protection
FortiMail
Email Protection
FortiExtender
Secure Wireless Network
PSAP Infrastructure Text to 9-1-1 Next 9-1-1 System
FortiSandbox
Zero-Day Protection
FortiNAC
Network Access Control
FortiEDR
Endpoint Protection
Session Border Converter (SBC)
911 Emergency Call Taker
911 Emergency Call Taker
911 Emergency Call Taker
911 Emergency Call Taker

Figure 1: NG911 infrastructure diagram.

The Advantage of an MSRP-Focused Security Solution

The best way to protect NG911 is to perform security inspections on MSRP messages before they enter the system. Public safety agencies need cybersecurity that features an MSRP decoder to do this. This critical functionality inspects MSRP traffic for threats and helps coordinate security reinforcement. PSAPs also need advanced threat detection capabilities. 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 malicious traffic.

For example, automated DoS attacks can generate MSRP messages much faster than a human can type, which can overwhelm NG911 systems and block actual emergency calls from getting through. Adding an MSRP protocol decoder tracks the rate of MSRP messages coming into the NG911 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 (example: malware) and inspect for embedded malicious URLs.

The risk of cyberattacks looms large for NG911 implementation because transitional systems that still include some legacy technologies have a very broad attack service—which increases vulnerability to threats like ransomware.[7]

This solution bolsters security by creating redundancy and ensuring PSAPs have no single point of failure. An MSRP decoder also makes PSAPs more resilient. 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 insufficient to protect these critical systems on its own.

Enter the Fortinet Security Fabric for NG911 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 its many benefits, the **Fortinet Security Fabric** includes MSRP decoding capabilities such as:

- 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

Building AI/ML security into NG911

The Fortinet Security Fabric comprises integrated security solutions sharing real-time information to protect the network infrastructure. Depending on the specific needs of the NG911 deployment, Security 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 NG911 environment starts with **FortiGate Next-Generation Firewalls (NGFWs)**. FortiGate NGFWs filter network traffic to protect an organization from external threats. While maintaining all the features of a stateful firewall—such as packet filtering, virtual private network (VPN) support, network monitoring, and IP mapping features—FortiGate NGFWs also possess deeper inspection capabilities that give them a superior ability to identify attacks, malware, and other threats.

As the threat landscape continues to develop rapidly, traditional firewalls fall further behind and put your organization at risk. FortiGate NGFWs not only block malware but also include paths for future updates, allowing them to evolve with the landscape and keep the network secure as new threats arise. Specific FortiGate benefits include:

- **Application control:** Fortinet has one of the largest applications databases to safeguard your organization from risky applications and allows you visibility to and control over 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 malware, spyware, or risky content downloads.
- **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 on the FortiGate allows text messages to be decoded in transit and analyzed for malicious content.

Securing SIP for NG911 Environments

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

- **Whitelisting/blacklisting:** FortiGate can whitelist and blacklist specific mobile device numbers (MDNs) for new SIP sessions.
- **Advanced Voice over Internet Protocol (VoIP) protection:** The FortiOS SIP application-level gateway (ALG) protects VoIP (SIP and session description protocol [SDP]) services in unified communication and next-generation networks (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 countermeasures and 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 overloading 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 a DoS attack or a flash crowd can cause.
  - **Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) pinholing:** RTP pinholing only forwards RTP/RTCP packets that conform to the particular session description of the associated SIP dialogue. If a SIP dialogue is finished, FortiOS automatically closes the pinhole. RTP/RTCP pinholing is supported by FortiASIC acceleration and achieves high-packet throughput at low jitter and delay.
  - **Stateful SIP dialogue tracking**: FortiOS tracks SIP message sequences and prevents unwanted SIP messages unrelated to a particular SIP dialogue. For instance, FortiOS can detect malicious SIP BYE messages that do not conform with the associated context of the SIP dialogue.
  - **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. But to securely pass through the FortiGate, this encrypted signaling traffic must first be unencrypted and inspected. FortiOS intercepts, unencrypts, and inspects these SIP packets, and allowed packets are then re-encrypted and forwarded to their destination.

The Cybersecurity and Infrastructure Security Agency (CISA) has received funding to deliver a cyber-resilient 911 ecosystem and to ensure small-scale NG911 systems align with National Institute of Standards and Technology (NIST) cybersecurity standards.[8]

  - **Inspecting SIP on multiple ports:** FortiOS can detect and inspect SIP and SDP user datagram protocol (UDP) and TCP sessions as well as 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 standby FortiGate device. FortiOS dynamically updates the context on the standby unit with SIP- and RTP-related data. This enables the standby unit to take over stable voice calls in case of an active unit's planned or unplanned outage or failover.
- **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 redirecting 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 showing particular SIP-related attacks or syntax violations with SIP messages or logs summarizing 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 application-layer gateway follows the configured NAT addresses in the firewall's 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.

Connections to the network (both physical and wireless) also need to be secured in NG911 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 to 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 NG911 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 industry's largest and most accomplished security research and analyst teams—which studies every critical area of the threat landscape, including malware and botnets, mobile, and zero-day vulnerabilities.

Leveraging FirstNet wireless WAN for reliable PSAP broadband

When it comes to delivering public safety and emergency services, PSAPs are the heart of emergency operations. These locations receive NG911 emergency communications from landline phones, mobile phones, VoIP, and Text-to-911. The PSAP also dispatches alerts and warnings to residents via broadcast communications. Most importantly, these locations dispatch emergency requests to first responders through computer-aided dispatch (CAD) over broadband and FirstNet Cellular.

Fortinet offers secure FirstNet cellular gateways via **FortiExtender**, a 5G/LTE wireless WAN gateway fully integrated with the Fortinet Security Fabric. By deploying FortiExtender alongside FortiGate as the PSAP CAD, your emergency communications and dispatch will be fully protected by a variety of AI/ML security capabilities that leverage FortiGuard threat intelligence. Fortinet converges essential networking services like SD-WAN, switching, wireless, and FirstNet on a single FortiOS operating system and delivered via a single management dashboard.

Wireless communications are protected without much oversight or manual effort because Fortinet automatically protects the PSAP from known and unknown threats.

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 NG911 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 and 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 NG911 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.

[1] "Suffolk County Asks NYPD for Help After Hack Cripples 911 Call Center and Police HQ," September 19, 2022.

[2] "Suffolk County Asks NYPD for Help After Hack Cripples 911 Call Center and Police HQ," September 19, 2022.

[3] "MedStar 911 dispatch, patient care reporting systems disrupted after cyberattack, officials say," WFAA, October 20, 2022.

[4] "Feds say cyberattack caused suicide helpline's outage," Associated Press, February 3, 2023.

[5] "How a Cyberattack Plunged a Long Island County Into the 1990s," The New York Times, November 28, 2022.

[6] "9-1-1 Statistics," NENA, accessed March 23, 2023.

[7] "NYC says it's on track to launch next-generation 911 system by 2024," StateScoop, December 29, 2022.

[8] "Cybersecurity and Infrastructure Security Agency Budget Overview—Fiscal Year 2024," U.S. Department of Homeland Security, March 2023.

www.fortinet.com

April 25, 2023 11:26 AM
777920-A-0-EN