

SOLUTION BRIEF

Improving VoIP Quality and Survivability With Fortinet Secure SD-WAN

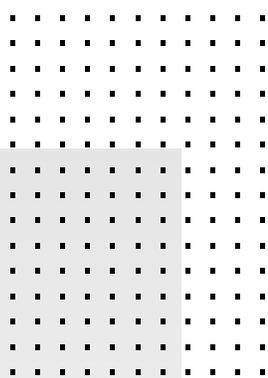
Executive Summary

Many organizations are still connecting wide-area networks (WANs) with legacy multiprotocol label switching (MPLS) and a hub-and-spoke architecture. Until a few years ago, this was standard. However, digital transformation (DX) is quickly changing that model. The rapid rise in pure Voice over Internet Protocol (VoIP) applications, as well as business collaboration apps, has put additional strain on the WAN. Variations in the quality of the underlying circuits, as well as network congestion, can affect the quality of voice calls, and in more severe instances, drop the call outright. A new approach to networking is needed to keep up with new technologies.

SD-WAN addresses today's challenges by fundamentally changing the way organizations architect and implement WAN. Its combination of intelligent path selection, WAN remediation, and application identification has redefined what is possible in a WAN. It not only lowers costs but also adds functionality. With SD-WAN, VoIP traffic can dynamically utilize the best-performing link, recover from packet loss, and survive blackouts and brownouts in links. Fortinet Secure SD-WAN goes above and beyond by offering ASIC-accelerated performance, a comprehensive application identification database (supporting over 5,000 applications), unmatched WAN scaling, and the industry's most robust security.

Barriers to Great VoIP Quality of Experience

In VoIP, the analog voice signal is digitized via a codec and converted into IP packets. The IP packets are then sent along to their intended destinations. As such, the underlying network can have a huge impact on the perceived quality of the call. Lost packets or large variations in delay (jitter) can cause garbled audio or even the entire call to drop. Network congestion when the voice traffic is competing with other applications over the same amount of bandwidth can also lead to lower-quality audio. Finally, an overburdened branch router can, at times, have a negative effect on voice traffic. This is often an overlooked area when troubleshooting VoIP-related issues.



“The global VoIP market size is projected to reach \$105660 million by 2028, from \$85330 million in 2020, at a CAGR of 3.1% during 2021–2027.”¹

Fortinet Secure SD-WAN for Superior VoIP

Fortinet Secure SD-WAN utilizes an array of technologies to address the above issues and improve VoIP quality and survivability.

Path failover involves moving flows from an underperforming transport to a better-performing transport. One key element of SD-WAN for VoIP is VoIP survivability. Fortinet Secure SD-WAN can, in real time, detect a drop in link quality and immediately move the voice call to a better-performing link. In fact, there are multiple application-steering strategies where the behavior of when and where to failover can be defined.

Active-passive path performance measurements refer to the constant polling and measurements of branch-to-application traffic for service-level agreement (SLA) enforcement. One advantage of Fortinet Secure SD-WAN as it relates to link health measurements is the flexibility to choose per-application measurement targets rather than a one-size-fits-all approach. This allows organizations to more accurately measure branch-to-voice applications whether the voice service is hosted internally (using a solution such as [FortiVoice](#)) or from an external provider, such as RingCentral. Fortinet Secure SD-WAN uses active probing methods combined with passively measured metrics derived from actual voice data. This guides intelligent decisions on whether a specific link is the best-performing path for VoIP traffic.

Furthermore, Fortinet Secure SD-WAN can select the best available path for voice applications based on mean opinion score (MOS). It is a way of representing the quality of the voice call as experienced by the end user. VoIP quality can be divided into levels based on MOS scoring: Excellent = 4.3–5.0, Good = 4.0–4.3, Fair = 3.6–4.0, Poor = 3.1–3.6, Bad = 2.6–1.0. This allows voice calls to fail over to a better path in the event the MOS score drops below a certain threshold.

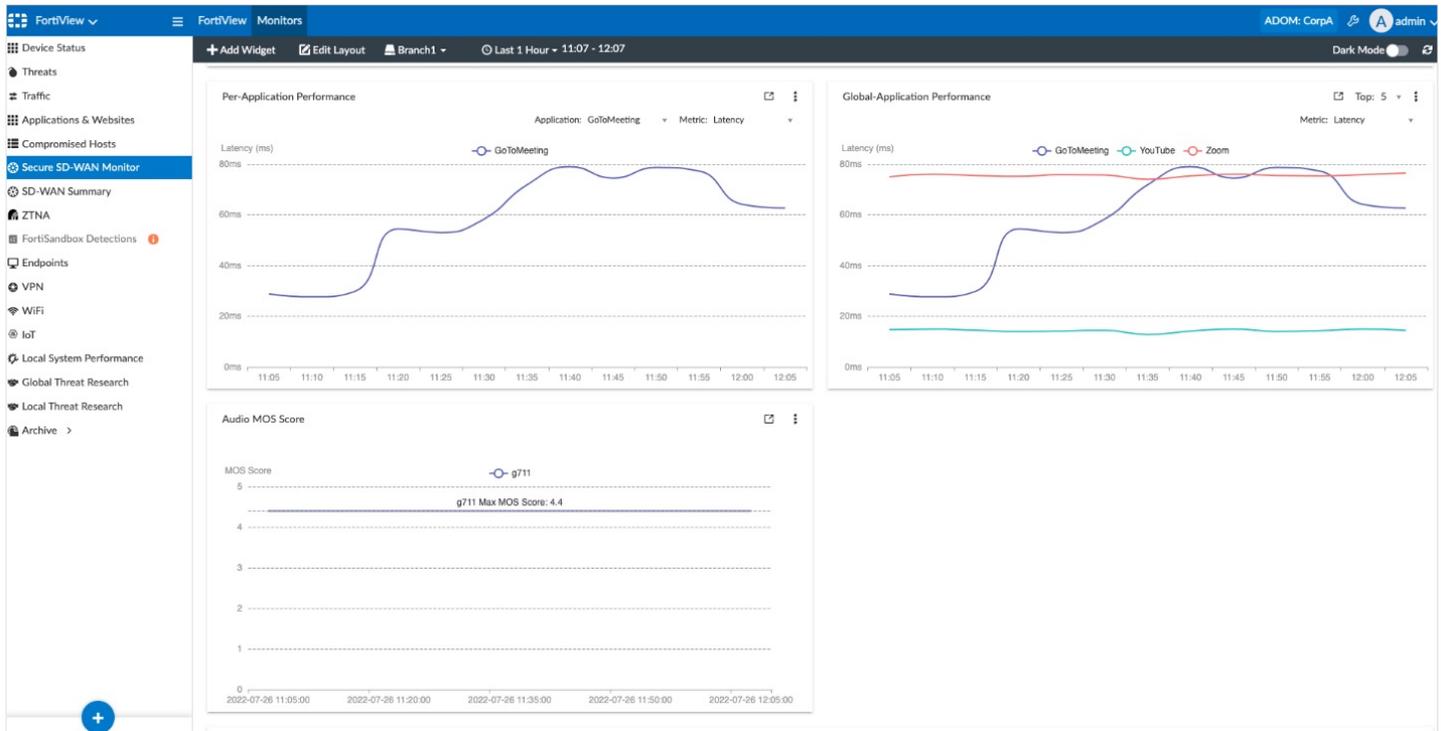


Figure 1. Analytics for application performance and MOS score

WAN remediation includes technologies such as forward error correction (FEC) and packet duplication to help overcome lost packets and transmission errors to improve call quality. FEC works by adding redundant data (parity bits) along with the original payload to correct errors in transmission. Calculations are done at the receiving FortiGate on the payload and redundant data to restore any packets that may have been lost or malformed during transmission. Fortinet Secure SD-WAN features adaptive forward error correction where the amount of redundant data dynamically adjusts according to how much packet loss is observed. This allows for optimal bandwidth use when FEC is enabled. Packet duplication, on the other hand, sends a duplicate copy of the original voice traffic across multiple SD-WAN tunnels. The mirrored traffic is then compared on the receiving FortiGate to accurately restore the original voice packets. Both of these features are often used to improve the quality of experience (QoE) for voice traffic.

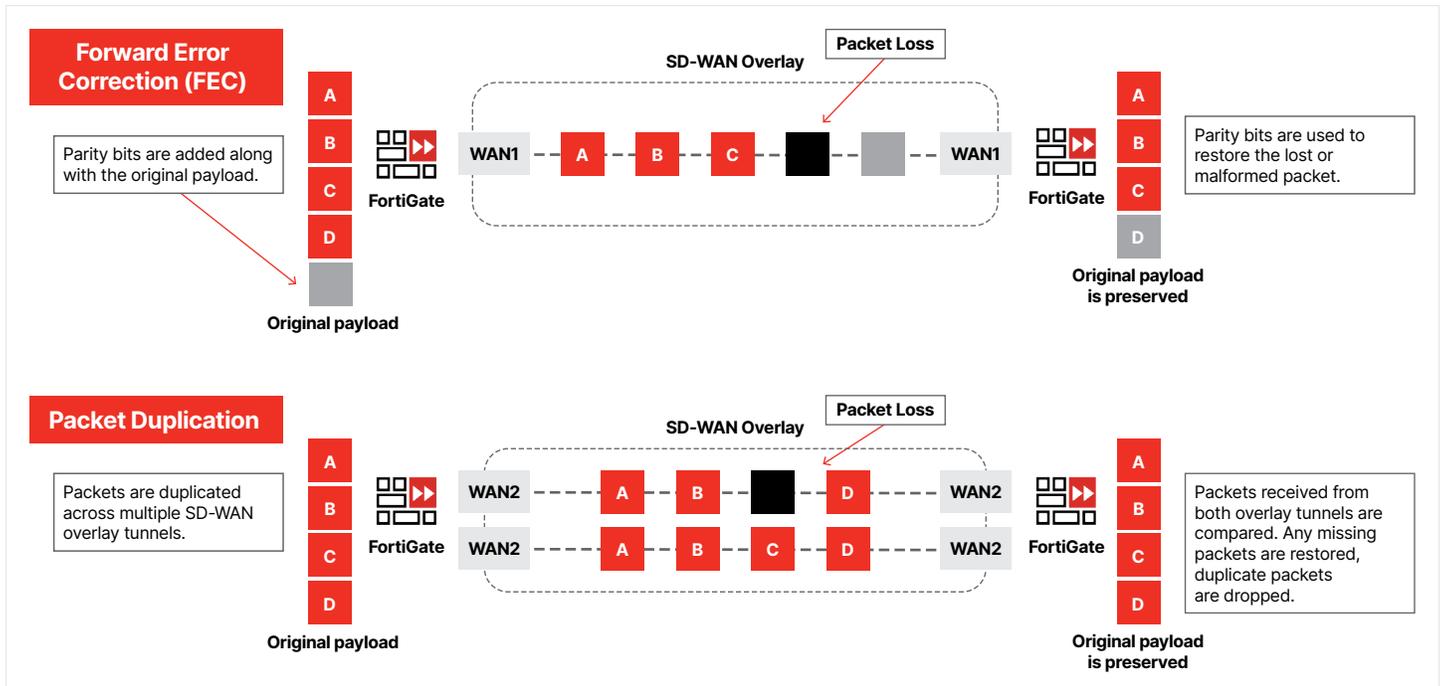


Figure 2. Forward error correction and packet duplication

Quality of service (QoS) is determined through voice and video traffic prioritization. Bandwidth is finite, and with digital transformation, there are more applications than ever that compete for the same bandwidth. Sometimes it is necessary to prioritize how traffic is distributed based on business needs. The Fortinet Secure SD-WAN QoS feature can police, shape, and queue network traffic at each location. Adjustments can be made automatically depending on available bandwidth at certain times of the day. Traffic shaping can be applied to specific application flows, such as for voice traffic.



Best Practices

Before best practices are outlined, it's important to point out that the goals of many SD-WAN deployments are to ensure voice survivability and voice quality.

Voice survivability

Voice survivability in general means that the call does not drop when there are adverse conditions with the underlying network (an outage or excessive packet loss). Whether the call is hosted internally via a PBX or other VoIP system such as [FortiVoice](#) or externally from a cloud service, the recommendation is to configure SD-WAN rules to utilize overlay SD-WAN VPN tunnels for voice traffic. This allows the voice traffic from the various paths to share the same egress IP address so that the existing voice session can persist, even in the event of a failover. To take it a step further, use MOS as failover criteria in SD-WAN rules for the most accurate voice failover.

Voice quality

From a voice quality perspective, WAN remediation techniques (FEC and packet duplication) require that the voice traffic go over an SD-WAN overlay tunnel. Both ends of a tunnel need to agree on the parameters for these features to function correctly. When leveraged correctly, these features can seamlessly provide top-notch voice quality even when the underlay transport is having issues. Traffic shaping is another feature that is commonly used to give voice a higher priority and guarantee a certain amount of bandwidth for voice traffic.

Summary

The digitization of voice is one of the key elements of the ongoing digital transformation movement and a huge driver for SD-WAN growth. Organizations leverage VoIP for its flexibility and cost savings. This aligns with the fundamental characteristics of SD-WAN. Fortinet Secure SD-WAN empowers networks with the features, security, and performance for a robust and resilient VoIP infrastructure and improved QoE.

¹ [“VoIP Market Size to Reach 3.1% CAGR and USD 105660 Million by 2028, Offer Growth Opportunities to the Top Vendors, Types, Applications,”](#) TheExpressWire, March 28, 2022.



www.fortinet.com