

CASE STUDY

Leading Latin American Airline Saves 50% in Connectivity Costs in Its National and Metropolitan Network With Fortinet Secure SD-WAN

In 2020, the global COVID-19 pandemic severely impacted the travel and tourism industry. Airlines were particularly hard hit and had to reduce their operations, in some cases by 100%. While waiting for commercial activity to resume, many airlines took the opportunity to optimize their infrastructure.

Copa Airlines, one of the most dominant airlines in Latin America, also faced this challenging time. Copa Airlines serves 31 countries in the Americas, from Canada to Argentina. Before the pandemic, the company was operating approximately 300 flights daily to over 80 destinations; the operation remains with a smaller volume compared to the capacity offered prior to the pandemic.

The situation compelled Copa Airlines to find new ways to reduce costs to protect its cash flow. Following an analysis by the airline's Technology Infrastructure team, the company undertook an aggressive plan to obtain multiple financial savings.

Part of Copa Airlines' staff is based at the head office in Panama, where the team oversees key functions such as customer service, flight operations, fleet maintenance, finance, technology, and training. The employees at its main airport hub and primary hangar for aircraft maintenance are located at the Tocumen International Airport in Panama City.

Building the Foundation With Strong Security and Cloud Benefits

Several years ago, Copa Airlines began updating its network platform with two main objectives: developing a secure network and offering dedicated connectivity to critical business functions.

The airline implemented FortiGate next-generation firewalls (NGFWs) at its facilities in Panama to protect the organization from internal and external threats. As a result, it achieved a resilient network that supports the users in the country. They leveraged FortiManager for central policy management and FortiAnalyzer for Fortinet Security Fabric analytics and automation.

This Fortinet solution facilitated the company's ambitious growth plans: The IT team can quickly and easily add Fortinet products to protect new network segments, applications, and business functions. The team was also able to configure the new FortiGate NGFWs remotely, which due to the pandemic, required easy deployment. Since all the FortiGate firewalls are centrally managed and are integral components of the Fortinet Security Fabric, they have consistent network security policies across the network, so they can avoid business disruptions while protecting the company from advanced threats.



"We needed a cost-efficient, secure, and scalable solution. The FortiGate equipment enabled us to develop a secure SD-WAN model that came with a 50% cost savings in national and metropolitan connectivity. The Fortinet Secure SD-WAN solution brought us reliable, redundant, and seamless connectivity, as well as centralized management and secure network traffic."

- Hugo Aquino, Director of Infrastructure Services and Technology Operations, Copa Airlines

Details

Customer: Copa Airlines

Industry: Transportation

Location: Panama

Business Impact

- 50% reduction in connectivity costs in its national and metropolitan network by shifting from MPLS to SD-WAN
- Improved operational efficiencies through centralized visibility and control over the entire network security infrastructure

As part of its modernization strategy, Copa Airlines integrated its data center with Microsoft Azure and Amazon AWS. Securing a multi-cloud environment was also a priority, since most of its employees use cloud applications. The company evaluated several vendors and found that Fortinet offered what it was looking for, including the connectors to integrate with its hybrid IT architecture. “The FortiGate NGFW allowed us to meet all our security needs. In fact, it even exceeded them, thanks to the integrated networking-specific features,” says Gilberto Añino, technology infrastructure manager at Copa Airlines.

Fortinet Secure SD-WAN for a Reliable, Cost-effective, and Seamless Connection

The modernization process was not limited to security issues. The team also wanted to move all of Panama’s metropolitan wide-area network (WAN) connectivity from multiprotocol label switching (MPLS) networks to the internet, by means of a secure, scalable, and cost-effective software-defined WAN (SD-WAN) solution. This step was envisioned as a forward-looking initiative. However, the pandemic forced a sudden acceleration of pace.

In an environment of multiple sanitary restrictions, which caused the closure of the airspace of several countries in the region, the Technological Infrastructure team of Copa Airlines focused on planning the migration to SD-WAN. “We did a hardware inventory and realized that the installed FortiGate devices could support this solution,” Añino explains. “The consulting from the Fortinet team was crucial, and their availability to do the necessary tests gave us the peace of mind that it was going to work. The results surprised us.”

The company leveraged the installed equipment to make a networkwide modification and set up the Fortinet Secure SD-WAN solution in all of its locations in Panama. “We needed a cost-efficient, secure, and scalable solution,” adds Hugo Aquino, director of Infrastructure Services and Technology Operations at Copa Airlines. “The FortiGate equipment enabled us to develop a secure SD-WAN model with a 50% cost savings in national and metropolitan connectivity. The Fortinet Secure SD-WAN solution brought us reliable, redundant, and seamless connectivity, as well as centralized management and secure network traffic.”

The cost reduction was the most obvious result of the implementation. Monthly internet service provider (ISP) costs fell, a welcome relief for Copa Airlines during the pandemic. The Fortinet Secure SD-WAN solution also brought Copa Airlines other advantages, such as greater control over internet links and overall superior network visibility.

Furthermore, Fortinet Secure SD-WAN technology enhances the scalability of the airline’s network. “If tomorrow we want to connect another ISP, we can do it without any inconvenience, regardless of the technology,” added Añino. “We assigned protocols and aggregated the necessary links to make it work. Prior to this development, we had to depend on a provider to ensure the connection. With Fortinet, we do not depend on a third party for connectivity and can guarantee a continuously reliable and available connection.”

Business Impact (contd.)

- Improved business resilience and scalability by eliminating dependence on single internet provider, ensuring reliable WAN access to applications
- Enhanced security posture through more robust threat mitigation and the ability to avoid lateral spread of threats

Solutions

- Fortinet Secure SD-WAN
- FortiGate
- FortiManager
- FortiAnalyzer

“If tomorrow we want to connect another ISP, we can do it without any inconvenience, regardless of the technology. With Fortinet, we do not depend on a third party for connectivity and can guarantee a reliable connection that is always available.”

- Gilberto Añino, Technology Infrastructure Manager, Copa Airlines

Before, the company had to manually join the various links at a single point and create a network bridge between them. This involved a high level of technical and operational complexity, in addition to the risk that modifying one link could affect another. Now, the Fortinet Secure SD-WAN solution, with its application awareness and WAN route optimization, makes everything seamless and automatic.

In the event of an outage on a primary WAN link, Fortinet Secure SD-WAN automatically reroutes traffic to the next best link, so users do not experience any service disruption. This gives Copa Airlines the resiliency it needs to support its most critical applications, such as its new website and reservation system, which require high availability and a secure treatment of customer information. The Copa Airlines IT team is confident that the Fortinet Secure SD-WAN solution—and the rest of its Fortinet Security Fabric—have the capacity to support these and other critical business needs at all times.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.