

CASE STUDY

# Dominican Republic Bank Achieves High Availability and Security of Its Network

In 2015, the development fund FONDESA—an NGO focused on educational loans—created the brand new Banco de Ahorro y Crédito FONDESA (BANFONDESA) to offer a broad portfolio of financial services. Today, BANFONDESA serves a host of clients in the Dominican Republic—from micro-entrepreneurs to small rural producers, low-income families, and urban and rural labor groups. With 59 branches across the country, the organization covers close to 70% of the Dominican territory, reaching approximately 300,000 customers with products such as savings accounts, fixed-term deposits, and loans.

To support its growth, the bank inherited part of FONDESA's network and communications infrastructure. The company started securing its digital operations with two FortiGate Next-Generation Firewalls (NGFWs) in its main data center and at its headquarters, through which all internet traffic from the 59 branches was routed.

However, BANFONDESA realized it could save costs by integrating its communications and security infrastructure. In addition, the bank required unified management of the entire network to simplify administration. After analyzing several options on the market, the company ultimately chose the Fortinet Security Fabric as the foundation for building its unified networking and security platform.

By deploying Fortinet solutions, the bank achieved a few key goals: unifying management of network and security technologies, improving control of branches' voice and data communications, and providing better support for high availability of communications. "Security controls and attack detection were improved. Having a unified platform with Fortinet allows us to have a more streamlined administration and to speed up the process of updates and incident reports," says Junior Méndez, BANFONDESA's Technology Manager.

## Highly Available and Cost-effective Infrastructure

BANFONDESA's network infrastructure lacked high availability. When problems occurred, sites could be disconnected, while the IT team had to travel to manually deal with the problems. BANFONDESA first decided to install a FortiGate NGFW at each site, together with FortiSwitch secure Ethernet switches and FortiAP access points. The optimization of Wi-Fi connectivity at its offices was key to business development, as several processes depended on connectivity and communications.

In addition, the bank deployed a high-availability communications network using Fortinet Secure software-defined wide-area networking (SD-WAN), providing the support its operations needed. BANFONDESA also acquired a backup internet link at each location, using different vendors and technologies. This reduced overhead from having traffic centralized at the data center; internet providers charged more for data center links than for distributed links across branches. Today, if an internet provider fails, BANFONDESA's network responds automatically to provide availability and redundancy, regardless of location.



*"Security controls and attack detection were improved. Having a unified platform with Fortinet allows us to have a more streamlined administration and to speed up the process of updates and incident reports."*

– Junior Méndez, Technology Manager, BANFONDESA

## Details

**Customer:** Banco de Ahorro y Crédito Fondesa (BANFONDESA)

**Industry:** Financial Services

**Location:** Dominican Republic

**Number of Secure SD-WAN**

**Locations:** 59

## Business Impact

- High availability of communications network for 59 remote offices
- Centralized management and broad network visibility
- Cost savings in communications infrastructure management

Along with the FortiGate NGFWs, both Fortinet Secure SD-WAN and LAN Edge infrastructures deliver all the external and internal traffic routing for the branches. The solution also helps BANFONDESA manage network segmentation, enabling the IT team to allocate resources on a more granular level.

## Security as the Centerpiece of the Business Ecosystem

In its early days, BANFONDESA's branches were linked with devices that did not offer security. Branches experienced several security intrusion attempts—many of which could not be adequately addressed at the endpoint level. “We chose Fortinet because its complete solution ecosystem addressed our requirement to acquire additional tools to support our business growth without changing the infrastructure,” explains Méndez.

Within the Fortinet Security Fabric, the company added several Fortinet solutions to extend protection to endpoints and users, alongside shielding traffic to the bank's applications and services. BANFONDESA uses FortiAuthenticator to enforce an identity-driven access policy within the company's network, working closely with FortiToken to manage two-factor authentication. In addition, the FortiMail solution adds a layer of protection to prevent, detect, and respond to email-based threats, while FortiWeb protects web applications from potential breaches.

BANFONDESA also integrated additional Fortinet solutions into its security environment. The FortiSIEM security information and event management solution has helped the bank identify threats, correlate them, and set up alerts that enable the bank to act immediately in case of security events. Likewise, FortiNAC network access control has extended visibility, control, and automated response for everything that connects to the network, providing a clear view to support regulatory certifications and security best practices that require financial services organizations to establish and maintain an accurate inventory of all connected devices.

## Centralized Control for Easier Management

Given all these tools, the bank needed an efficient way to manage its resources. It uses the FortiManager network management solution to centrally control its entire network ecosystem. “The implementation of Fortinet's solutions allowed us to obtain significant cost savings in communications, considering an 11-month forecast for the return on the investment made,” highlights Méndez. By having a single administration tool, the entity has also simplified several processes, such as applying unified security policies that immediately affect every single device.

With FortiAnalyzer, the financial institution added real-time incident logging and reporting. Now, the bank can react instantly—or even automatically—to incoming threats.

BANFONDESA's choice of Fortinet as a technological partner has been crucial in supporting its business growth. The company is already planning upcoming sites, which will all have a Fortinet Security Fabric-based network and security infrastructure. “Fortinet addresses having dispersed tools from multiple vendors. For companies like us, Fortinet is the answer,” concludes Méndez.

## Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken
- FortiMail
- FortiWeb
- FortiSIEM
- FortiNAC

*“The implementation of Fortinet's solutions allowed us to obtain significant cost savings in communications, considering an 11-month forecast for the return on the investment made.”*

– Junior Méndez, Technology Manager, BANFONDESA



[www.fortinet.com](https://www.fortinet.com)

Copyright © 2022 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.