BLACK BOX

CASE STUDY
CYBERSECURITY

Strengthening Cybersecurity for a Leading Philippines Contact Center through Advanced Firewall Technology

Overview

A major contact center organization in the Philippines needed to upgrade its cybersecurity infrastructure. The company handles inbound customer service, technical support, outbound sales, and market research, thus processing massive amounts of sensitive client data every day. Their existing unified threat management (UTM) device at Manila headquarters had reached its limits. The legacy solution simply wasn't keeping pace with current security demands. They needed something more powerful and flexible to protect operations and keep service running smoothly.

They partnered with Black Box, where the experts deployed a next-generation firewall (NGFW) solution that provides advanced perimeter protection, centralized visibility, and real-time threat intelligence, all without disrupting their existing IT setup.

AT A GLANCE

CHALLENGES

- Outdated perimeter defenses couldn't keep up with evolving cyber threats
- The existing unified threat management (UTM) system at the Manila site wasn't scalable and lacked granular control
- There was limited visibility into user activity and network traffic patterns
- The organization needed to boost data security and compliance without sacrificing operational efficiency

SOLUTIONS

- Deployed a Fortinet Next-Generation Firewall (NGFW) with integrated log analyzer
- Separated internal and external networks for better protection
- Implemented centralized user authentication and policy-driven access control
- Added comprehensive gateway-level threat detection, real-time reporting, and bandwidth optimization

RESULTS

- Achieved stronger perimeter security with simpler policy management
- Gained centralized visibility and control across the organization
- Optimized bandwidth utilization and provided secure VPN access for remote users
- Streamlined administration and cut down management complexity

BENEFITS

- Better protection against modern cyber threats
- Improved performance through intelligent traffic management
- Simplified, policy-based security operations
- Built a trusted, scalable security architecture that supports future growth
- Established an enduring partnership that ensures continuous protection and compliance

Challenges

The organization's operations relied heavily on secure, high-performance networks to support continuous customer interactions and maintain data integrity. As cyber threats grew more sophisticated, their legacy UTM device no longer provided adequate visibility or control. IT administrators were unable to monitor network activity effectively or enforce the access policies the environment demanded.

Here's the reality: thousands of users log in simultaneously across different departments and client accounts. Without adequate safeguards, data exposure and compliance violations were legitimate concerns. The network lacked automated threat response and detailed traffic analysis, putting operations at risk. Remote access and VPN demands kept growing, too, making security management even harder. They needed an enterprise-grade solution that offered complete visibility, centralized policy enforcement, and solid protection, without disrupting system performance. Scalability and simplicity were critical for supporting future expansion and technology upgrades.

Solutions

Black Box conducted a detailed assessment of the existing infrastructure and recommended a comprehensive Fortinet Next-Generation Firewall (NGFW) solution, designed to strengthen perimeter security while integrating seamlessly with current systems.

The new configuration separates internal and external networks clearly, which strengthens perimeter defenses and reduces vulnerabilities. An integrated Fortinet log analyzer captures and correlates network events so that the team gets real-time visibility into user activity, security alerts, and bandwidth usage. Centralized authentication and policy-based access give administrators full control over user permissions and network behavior.

The NGFW offers layered gateway protection against malware, phishing, and intrusion attempts, while secure VPN services ensure safe remote access for authorized users. The solution also optimizes bandwidth by prioritizing legitimate traffic and blocking unauthorized data transfers automatically. Black Box's consultative approach ensured the NGFW deployment worked smoothly with existing systems, ensuring minimal disruption and maximum security gains.

Results

The Fortinet NGFW changed everything about how this organization handles cybersecurity. Network visibility improved dramatically, allowing IT teams to monitor user behavior, identify anomalies, and address threats before they cause damage. The centralized dashboard simplified policy management and reduced the workload significantly. Bandwidth utilization became much more efficient, keeping performance consistent across all departments. Remote users got secure, authenticated VPN access. Automated threat prevention reduced downtime and increased overall resilience. Together, these changes strengthened compliance readiness, stabilized operations, and created a reliable foundation for future digital transformation projects.

Why Black Box?

The contact center selected Black Box for its proven expertise in enterprise cybersecurity, consultative approach, and ability to deliver scalable, future-ready solutions. Through its partnership with Fortinet, Black Box enabled the organization to meet immediate security needs while aligning with long-term strategic objectives.

By combining technical precision with proactive support, Black Box delivered results that exceeded expectations. The contact center's network became easier to manage, governance practices were strengthened, and trust was reinforced across all levels of the business.

This project highlights how Black Box empowers contact centers to safeguard critical data, maintain operational continuity, and remain resilient in an increasingly connected and dynamic digital environment.