QBurst | A High AI-Q™ Company

Scalable Web Portal for Unified Office Security Management

Empowering a global security leader with a centralized cloud console to orchestrate services, monitor logs, and manage Customer Premise Equipment (CPE) at scale.

Overview

We engineered a multi-tiered security portal using Java and Spring to manage front-end functions for a massive fleet of 5,000+ CPEs.

- Developed a high-performance Central Controller API to synchronize service configurations between the cloud infrastructure and on-site hardware.
- Achieved full compliance with OWASP Top 10 security standards, ensuring the portal itself remains as impenetrable as the services it manages.

Client Profile

A decade-long pioneer in information security, this client offers an integrated services framework to help global enterprises actively monitor and prevent risk. Their solutions protect critical infrastructure for hundreds of customers through a blend of cutting-edge hardware and managed software services.

Challenges: Orchestrating Security Across Borders

Managing a distributed security network required moving beyond fragmented legacy systems:

- **Scaling Demands:** The portal needed to support up to 5,000 CPEs, with each unit serving between 50 and 500 individual users.
- **Complex Role Hierarchy:** Different access levels were required for Sales Managers, Client Admins, and Customer Account Owners to prevent unauthorized configuration changes.
- **Hardware-Software Sync:** Ensuring real-time synchronization between the cloud-based management console and the physical CPE controllers at customer sites.

- **Log Inundation:** The need for a threaded, high-efficiency log analysis engine to parse service logs (Firewall, VPN, IPS/IDS) and generate actionable reports.

QBurst Solution: Multi-Tiered Security Orchestration

We developed a scalable, multi-tiered architecture that separates user interaction from backend logic and hardware communication. The solution was built using Spring Security for robust authentication and Hibernate for efficient data management.

The technical framework consists of four integrated components.

- **Security Portal:** A feature-rich console where customers can subscribe/unsubscribe to services and manage VPN, Firewall, and Proxy configurations via a ticket-based Service Desk.
- **Central Controller API:** Built as a dedicated communication layer between the CPEs and the portal, utilizing Quartz Scheduler for critical backend synchronization jobs.
- **CPE Web App:** A localized application facilitating LDAP-based identity management and user authentication directly at the customer site.
- **Log Analysis Engine:** A threaded Java application using regular expressions and pattern matching to parse raw logs from CPEs into readable, graphical reports for the portal dashboard.

Key Features and Technical Highlights

- **Customizable Widget Dashboard:** An aesthetically appealing interface that allows users to monitor real-time security metrics.
- **Automated Alerting:** Integrated SMS and Email gateways to notify administrators and users of security incidents or configuration changes.
- **Service Desk Integration:** A built-in system for customers to raise service requests, which client admins can then "tune" directly within the portal.
- **CPE Health Monitoring:** The controller continuously verifies that all configured services (IPS, IDS, VPN) are functional and reports status back to the cloud.

- **Universal Compatibility:** A responsive design that ensures seamless performance across all major browsers (Chrome, Firefox, IE).

Impact

- **Enterprise-Grade Scalability:** The portal successfully scales to handle 5,000+ CPEs and millions of end-user data requests.
- **Operational Efficiency:** Centralizing management into a single access point reduced the complexity of providing security services across 30 countries.
- **Hardened Security:** The platform passed all rigorous internal security assessments and adheres to OWASP Top 10 best practices for web application safety.
- **Improved Customer Retention:** The intuitive UI and self-service subscription model empowered customers, leading to a better user experience and reduced administrative support tickets.
- **Proactive Risk Management:** Real-time log analysis and notifications allow the client and their customers to mitigate threats before they escalate.