CASE STUDY

Growing Healthcare Provider Inspects Encrypted Traffic at Scale

Recoletas
Grupo Hospitalario

Grupo Recoletas is one of the most important private hospital groups in Spain and a healthcare leader within the Castilla y León region. Headquartered in the city of Valladolid, it offers excellent medical teams and comprehensive facilities dedicated to the sole objective of providing the best and most complete hospital service to patients. Grupo Recoletas specializes in the management of high-technology healthcare resources across seven hospitals, 11 medical centers, five institutes, and four diagnostic centers.

Encryption Inspection Without a Performance Penalty

Josep Bardallo has been the CIO and CISO at Grupo Recoletas for five years, with a team of 15 IT staff. In that time, the organization has rapidly grown with new acquisitions.

With the emergence of compliance regulations that stipulated the encryption of patient information and medical records and images—specifically the EU's General Data Protection Regulation (GDPR) and Spain's Organic Law 3/2018, as of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)—Bardallo and his team were given the mandate to ensure that traffic containing the aforementioned data was encrypted. At the same time, with 80% of traffic encrypted using secure sockets layer (SSL) or transport layer security (TLS) encryption, Bardallo and his team required a solution that would enable them to inspect all network traffic without the performance degradation that typically occurs with SSL/TLS inspection.

"We specifically wanted a firewall solution that could handle our growing volumes of encrypted network traffic," Bardallo says. "While we have multiple systems that generate patient data that must be encrypted, our SAP and medical imaging systems are big drivers when it comes to our encrypted volumes. They are also critical systems for us."

To find the right solution, Bardallo needed to demonstrate return on investment (ROI)—which is a core business focus for Grupo Recoletas. "ROI is more than simply cost for us," he says. "It also involves aspects such as scalability and ease of deployment and management."

"We needed an affordable way to inspect SSL/TLS traffic without slowing down our network. Corsa and Fortinet virtual technologies are helping us do exactly that, even as our business expands."

– Josep Bardallo, CIO, Grupo Recoletas

Details

Customer: Grupo Recoletas

Industry: Healthcare

Location: Valladolid, Spain (EU)

Business Impact

- Reduced deployment time to minutes versus days, saving over €43,000 Euros in labor per site
- Delivered 3x to 4x lower solution cost without reducing performance
- Achieves regulatory compliance by inspecting 100% of SSL/TLS encrypted traffic

Corsa and Fortinet Deliver a Scalable, High-performance Solution

Bardallo and his team understood from experience that implementing next-generation firewall (NGFW) devices can be a complex process, with multiple factors affecting the overall performance of the solution. In the past, they had seen a trade-off between security effectiveness and network performance. Therefore, Bardallo's criteria for evaluating a new solution included:

- Confirmation that security protections did not adversely impact network performance
- Testing SSL/TLS capabilities and assurance that they would only pay for the inspection capacity they needed on a subscription basis
- Evaluation of virtualization for simplicity, flexibility, and ease of use

While Grupo Recoletas evaluated a couple of different solution options, Bardallo and his team ultimately settled on a joint solution from Corsa Security and Fortinet. "It offered the best price-performance ratio by far," he says. The integrated solution Fortinet and Corsa presented to Grupo Recoletas is comprised of two main elements (in addition to the solution's host Dell EMC Server):

Solutions

- FortiGate VM
- FortiManager VM
- FortiAnalyzer VM
- Corsa Turnkey Network Security Virtualization Platform

Fortinet Partner

- Corsa Solutions

Fortinet Security Fabric

For this instance, the Fortinet Security Fabric architecture would include FortiGate VM virtual NGFWs and Fabric Management Center (FMC) solutions.

- **FortiGate VM.** FortiGate virtual appliances offer complete NGFW protection with full SSL/TLS inspection capabilities. They feature all the security and networking services common to traditional hardware-based FortiGate devices—including antivirus, web filtering, application control, and intrusion prevention (IPS).
- **Fabric Management Center (FMC).** As part of the FMC, FortiManager and FortiAnalyzer enable network and security teams to simplify operations. They offer flexible deployment options, including VM instances—which was a perfect fit for Grupo Recoletas' needs.

Corsa Red Armor Network Security Virtualization Platform (NSVP)

Corsa's platform would include hardware for load balancing as well as software management.

- **Corsa Security Orchestrator.** Software that provides a cloud-like user experience for managing virtualized network security infrastructures. It provisions and manages the virtual network security appliances and the associated server, network, and load-balancing functions. It pushes the necessary initial configuration to the virtual appliances that allows them to be seamlessly integrated into the centralized firewall policy manager (FortiManager).
- **Corsa Security Services Load Balancer.** A transparent in-line load balancer that distributes traffic to all virtual appliances.

While the Corsa physical appliance is installed on-premises in the data center, FortiGate VM can be deployed as needed across Grupo Recoletas' private cloud. Virtual instances of FortiManager (automation-driven network management) and FortiAnalyzer (analytics-powered security and log management) are key security elements used by the healthcare provider's network operations team.

"One of the facets of the joint solution that we really liked involved the ability to deploy it without making any changes to our network," Bardallo says. "Corsa and Fortinet technologies took care of the virtualization complexity with a tightly integrated platform, thus eliminating the need to do any DevOps work." Carolyn Raab, the chief product officer at Corsa, elaborates: "As part of our turnkey network security virtualization platform, FortiGate VMs offer our customers scalable protection that helps them demonstrate immediate ROI."

To meet Grupo's requirements, Corsa, a Fabric-Ready Partner in the Open Fabric Ecosystem, leveraged the underlying open architecture of the Security Fabric to seamlessly integrate with Fortinet virtual NGFW instances and FMC solutions. By removing silos and facilitating openness and seamless integrations, the Open Fabric Ecosystem enabled Corsa and Fortinet to jointly deliver the solution integrations as a single, cohesive system to meet Grupo Recoletas' business and security requirements.

In terms of setup costs, Corsa and Fortinet solution deployment can be done in minutes versus days of setup for a physical big-box appliance solution per location. Across 23 total sites, that amounts to an approximate difference of less than two hours (at five minutes per virtual deployment) versus 23 days (at one day per onsite physical solution deployment). When multiplied by the labor costs of an average network engineer in Spain, this timesaving equates to an immediate capital expenditure (CapEx) savings of over €1,900 Euros (~$2,100 USD) per site, or a total of €43,700 Euros ($48,300 USD).[1]

Scalability was also an important consideration for Bardallo. "We were able to demonstrate that network throughput performance was not impacted when decryption and other next-generation security features were enabled," he says. "We can scale inspection capacity for any amount of traffic."

> *"Corsa and Fortinet technologies took care of the virtualization complexity with a tightly integrated platform, thus eliminating the need to do any DevOps work."*
>
> *– Josep Bardallo, CIO, Grupo Recoletas*

Solution Evaluation Under Real-world Conditions

Grupo Recoletas started with deployment at a single site to test the solution's performance before rolling out to other sites in 2020. The team evaluated the performance of the Corsa and Fortinet joint solution in the following areas:

Platform installation. The platform was installed within an hour and did not require any network topology changes to Grupo Recoletas' network. The result: Traffic into the platform exactly matched traffic out of the platform with zero degradation in throughput performance and no packets dropped.

Create and load balance all traffic to a virtual NGFW cluster. Using a cluster of four FortiGate VM virtual appliances, traffic was load balanced and a policy was configured to "implicitly accept all" traffic. This created a baseline of understanding for the data path performance of the platform. The result: The load balancer performed very well, providing a good equilibrium of new and concurrent sessions over all FortiGate VM NGFWs.

Application control and full SSL/TLS inspection with exemptions. All traffic into the platform was decrypted as necessary, inspected, and categorized by application. The result: All traffic into the platform exactly matched traffic out of the platform with zero degradation in throughput performance and no packets dropped.

Additional NGFW services were activated and tested with full SSL/TLS inspection enabled. Throughout these tests, the FortiGate VM NGFW behaved the same as a traditional hardware-based firewall, but with the added ability to conveniently monitor the VMs from the infrastructure perspective and the ability to scale to high capacity going forward. VMs were created and removed ad hoc to verify the ability to scale up and down dynamically.

Reducing Risk While Enabling New Lines of Business

Bardallo and the Grupo Recoletas team were very satisfied with the results of their single-site evaluation across all their critical areas of interest and are busy working to roll it out across the organization's other sites.

Effective, comprehensive protection

The joint Corsa and Fortinet solution immediately reduced risk of a security breach hidden within encrypted traffic. Grupo Recoletas is now able to inspect 100% of network traffic while operating its network without performance degradation. "The virtualization capabilities proved to be push-button," Bardallo says. "After the platform was installed, there was no further need to engage with any element of hardware."

Grupo Recoletas engineers can use FortiManager in a simple, intuitive, and out-of-the-box manner for centralized visibility of all deployed VMs. FortiAnalyzer real-time monitors were leveraged to get the status of each VM and also get reports on traffic throughput, inspection rate, CPU utilization, and memory utilization. In addition, statistics from the Corsa virtualization platform provide insights into the network and compute infrastructure for both individual VM health and overall inspection capacity health to ensure that protection is never compromised and network performance is maintained.

Seamless scalability

Corsa's scale-out approach to turnkey virtualization offers simplicity, flexibility, and ease of use. Scale is particularly important for the organization's expanding needs. Grupo Recoletas has more than doubled in size in recent years and will be adding another two or three medical centers in 2020. Their current plan is to deploy two VMs for each location. The Recoletas team has not yet decided if they want to manage inspection centrally (routing traffic through the main data center where the Corsa virtualization platform performs inspection on-premises) or in a decentralized architecture, where inspection happens at each of the 23 site locations.

The Corsa/Fortinet solution offers the ability to avoid doing refreshes to accommodate traffic demand increases with additional hospitals and increasing traffic flows. As traffic increases, Recoletas can meet inspection demands by adding more VM licenses to scale inspection as needed. This results in a fast time to market when securing new acquisitions while future-proofing the organization's overall network capacity for years to come—even as encrypted traffic becomes more prevalent.

Realizing significant ROI

The joint Corsa and Fortinet solution offers outstanding TCO to Grupo Recoletas due to benefits of using virtualization for inspection. "As part of our Corsa turnkey network security virtualization platform, FortiGate VMs offer our customers scalable protection that helps them demonstrate immediate ROI," says Raab. For comparable inspection capabilities, Grupo Recoletas would have needed to buy much larger NGFWs from other vendors. The cost of the combined solution was 3x to 4x less expensive than competing "big-box" appliances, which were needed due to degradation of inspection at scale.

Also, budgeting for 100% inspection protection does not rely on complicated five-year network usage models, as with other competing solutions. Recoletas would not be tied in to paying for more bandwidth than they currently needed over an extended contract period in order to anticipate future needs. With these metrics in hand, Bardallo was able to fulfill the business requirement of demonstrating the ROI of the Corsa/Fortinet solution over alternatives to executive management.

Encryption Inspection Designed for Secure, Scalable Growth

With high-performance protection, dynamic scalability, and exceptional value, the Corsa platform, including the Fortinet VM-based solutions, addresses all the key requirements for Grupo Recoletas' encryption inspection needs across a distributed healthcare infrastructure. "We're responsible for keeping our patients' private information safe and secure at all times," Bardallo says. "Corsa and Fortinet are a big part of how we do that going forward as we expand the Corsa turnkey network security virtualization platform across our other facilities."

[1] "Average Network Engineer Salary in Spain," PayScale, accessed February 3, 2020.

FORTINET

www.fortinet.com

February 20, 2020 11:38 AM

592175-0-0-EN

D:\Fortinet\Work\2020\February\022020\cs-grupo-recoletas