CASE STUDY

Major European Bank Reengineers Itself to Enhance Quality, Efficiency, and Security

As part of the parent company of a major European banking conglomerate, this organization is tasked with the development and deployment of the group's extensive application portfolio.

With an ongoing focus to improve the quality and efficiency of service delivery, a recent initiative for the applications team has been the migration away from the bank's legacy data centers to a cloud-centric environment. The transition presented the team with the opportunity to overhaul the IT infrastructure and to simultaneously implement a dramatically enhanced security architecture.

A cornerstone of the reengineered environment has been the selection of the Cisco Application Centric Infrastructure (ACI). Cisco ACI utilizes an architecture based on software-defined networking (SDN) principles to reduce total cost of ownership, automate IT and IS tasks, and to accelerate data-center application deployments.

The addition of the Fortinet FortiGate Connector for ACI to the Cisco solution has enabled the bank to leverage the automated security provisioning and protection capabilities of the industry-leading range of FortiGate next-generation firewalls (NGFWs). The combination facilitates the application of enterprise security policies in a highly granular manner that was not achievable with the legacy monolithic environment.

Benefits of the Cloud

The adoption of a cloud-based infrastructure enables the bank to create a pool of IT and IS resources with on-demand availability: Each component is able to be dynamically allocated to individual tenants and deallocated when no longer required. The Cisco ACI and FortiGate Connector pairing provides the ability to micro-segment the bank's environment, supporting the application of highly specific, security-related services to individual modules and traffic flows.

The FortiGate Connector facilitates the tight integration of multiple FortiGate 3000D enterprise firewalls with ACI and the bank's Cisco Application Policy Infrastructure Controller (APIC). The APIC cluster spans two physical data centers that together provide cloud services to the entire infrastructure.

> *"The Cisco and Fortinet partnership is key for the bank: We now have the ability to finely tune our environment and to accurately impose security policies in a distributed and highly granular manner. Using much less effort, we can roll out a wide portfolio of services that are significantly more secure, have higher performance, and better flexibility than ever before."*
>
> *– Senior Network and Data Center Engineer, Major European Bank*

Details

Customer: Major European Bank

Industry: Financial Services

Location: Europe

Aggregate and Automate

FortiGate NGFWs are deployed in the production environment resource pool for both Layer 2 (transparent—"GoThrough" mode) and Layer 3 (routed—"GoTo" mode) traffic flows between a highly configurable combination of application components, each set known as an endpoint group (EPG). Once defined, EPGs can be individually mapped to network resources, creating the ability to apply specific security characteristics using tailored policies and rules at logical application boundaries.

Using attribute-based logic, each EPG can be configured to automatically react to pre-defined events and circumstances: For example, instantly isolating individual infrastructure components when a specific set of conditions is encountered.

EPGs utilize microsegmentation to provide control and flexibility across policy definitions. The same approach is further leveraged to create partitions that span combinations of virtual and physical domains to provide even greater operational flexibility, control, and visibility.

Groups of security policies are placed into libraries for future reuse, giving the bank's developers the ability to rapidly construct a customized set of highly granular security requirements that can be used throughout the complete application development/deployment life cycle.

Business Impact

- Substantial elevation of enterprise-wide security posture
- Enhanced efficiency, pace, and quality-of-service delivery operations
- Highly tailored security policies rapidly deployable throughout application development life cycle
- Visibility into physical and virtual application workloads

Solutions

- FortiGate 3000D
- Cisco Application Centric Infrastructure
- FortiGate Connector for Cisco ACI

In-depth Analysis

As the Cisco Application Centric Infrastructure only utilizes stateless access control lists (ACLs), analysis would primarily have been focused on the contents of packet headers. The addition of FortiGate enterprise firewalls provides the ability to conduct "stateful" inspection, enabling an in-depth examination of multiple packet parameters, including source, destination, and payload. Not all internal traffic is required to pass through a firewall, and the ability of FortiGate to perform stateful inspections enables the determination of the appropriate routing and levels of scrutiny to apply.

Fortinet Security Fabric Delivers

Each model in the FortiGate range comes equipped with the Fortinet FortiOS network security operating system to provide deep visibility and cross-platform control. A FortiGuard Labs subscription service also is included with the enterprise firewall, ensuring that all devices are continually protected against malware with the most up-to-date security intelligence. All of the Fortinet components are unified within the Fortinet Security Fabric, an intelligent framework that provides broad, powerful, and automated security capabilities able to span the bank's entire attack surface.

24/7 Benefits

An always-present challenge for the bank's team is that maintaining continual application availability is a mission-critical imperative, dictating that any changes—including the conversion to cloud and SDN-based models—must not have any impact on daily operations. The FortiGate integration with Cisco ACI delivers—through the use of service insertion and chaining—the necessary reliability, security, and multi-tenancy characteristics to avoid such disruptions.

The reengineered architecture has provided the bank with multiple benefits spread across many areas, including development, operational, and financial disciplines. A company senior network and data center engineer comments, "The Cisco and Fortinet partnership is key for the bank: We now have the ability to finely tune our environment and to accurately impose security policies in a distributed and highly granular manner. Using much less effort, we can roll out a wide portfolio of services that are significantly more secure, have higher performance, and better flexibility than ever before."

FORTINET®

www.fortinet.com