CASE STUDY

Northern European Bank's Transformation to Agile and Responsive Cloud-based Application and Service Delivery

For more than a century, this company has been a major force in banking, helping millions of customers, both individual and commercial, to realize their ambitions—locally as well as internationally.

To maintain growth at the forefront of such a competitive domain for so long has required continual innovation and transformation in the products and services delivered as well as in the very structure of the organization itself.

One of the most significant and challenging of these transformations in recent years has been the expanding role of IT within the bank. From a comparatively small group supporting the business through its maintenance of infrastructure and resources, the IT group has grown into a major new revenue center through its successful use of digital innovations such as cloud computing and software-defined networking (SDN).

A New Cloud-based Data Center

Central to the bank's digital transformation was the creation of a new cloud-based data center to replace the legacy mainframe systems on which they had relied for so long (and indeed on which much of the banking sector still relies today).

To achieve the performance and agility necessary to win market share in today's highly competitive financial services sector, the bank realized it would need to create a pool of IT and IS resources with on-demand availability. This in turn would require the ability to rapidly adapt and reconfigure the network infrastructure in response to the evolving requirements of new applications and services.

To do this, they would need to leverage the principles of SDN in which some of the traditionally fixed structures of the network would be replaced with virtual equivalents that could be automatically "spun up" and configured in real time, from a central location, under software control.

At the same time, to ensure maximum security and future-proofing, they were determined not to put all their technological eggs into a single vendor's basket. This meant building an open, application programming interface (API)-based ecosystem in which network elements could be combined into a holistic, tightly integrated infrastructure of secure, high-performance connectivity.

"… Delivery to support the needs of Line of Businesses/ developers drained our resources but with the use of API and automation a lot of the drudgery has now been eliminated for the benefit of the business."

Details

Customer: Major Northern European Bank

Industry: Banking

Location: Northern Europe

Business Impact

- Enabled the creation of new services and revenue streams
- Increased business agility through automated service deployment and configuration
- Enhanced security and reduced the burden of compliance

Technology Choices

In selecting the technological components for the new data-center infrastructure, there were three essential criteria:

1. **A robust and open API**
   To provide the level of service agility demanded by the business, they developed a self-service portal through which new services could be created, launched, and updated in real time. This in turn necessitated granular API access to all the key components of the network infrastructure, as well as to the multitude of application microservices from which the final applications would be built.
2. **Performance**
   To support the necessary segmentation of microservices, each with its own security and quality-of-service (QoS) requirements, and to allow the network to scale smoothly to meet future as well as current demands, performance would be paramount.
3. **Price**
   Although the investment would ultimately generate new revenue streams and increase the productivity of the bank's costly and expanding development team, the new data center would nevertheless need to show an appropriate return on initial investment.

Solutions

- FortiGate
- FortiManager VM
- FortiAnalyzer VM
- FortiAuthenticator

"Before … it would typically take a number of weeks to launch each new service and the process could be very frustrating. Now, we can be operational in a matter of hours."

After extensive research and testing, the bank chose the Fortinet Security Fabric approach, including **FortiGate next-generation firewalls (NGFWs)** with management, analytics, automation through the Fortinet Management Center (FortiManager, FortiAnalyzer), and authentication provided through FortiAuthenticator. Key to this decision was the availability of a prebuilt security fabric connector for the chosen SDN framework of switches and infrastructure controller.

The pairing of these technologies provides the bank with an ability to microsegment the service delivery environment, supporting the application of highly specific, security-related services to individual modules and traffic flows. The combined solution streamlines traffic to supported FortiGate appliances and can automatically assign security policies to individual data-center workloads.

For the initial rollout of the new data-center, 42 FortiGate NGFWs have been deployed, simplifying network complexity and providing visibility into applications, users, and networks. The FortiGate appliances combine dedicated, purpose-built security processors with threat-intelligence services from FortiGuard Labs to deliver top-rated security and high-performance threat protection. With automated, policy-based responses, FortiGate and the Fabric Management Center can accelerate time to resolution for any security incident from small to large.

The Fabric Management Center (FortiManager and FortiAnalyzer) provides the bank with powerful, simplified network orchestration, automation, and response, with granular device and role-based administration across the entire data center.

FortiAuthenticator further strengthens the bank's access security for members of the DevOps team by simplifying and centralizing the management and storage of user identity information and enabling a range of single sign-on (SSO) methods.

Automated Operations, Orchestration, and Response

The consequences of a large-scale data breach can be devastating to any modern organization, but within the banking sector it can be an order of magnitude more serious. As the complexity and sophistication of the threat landscape increases, the task of preventing such breaches becomes ever more challenging. And while this is true even for relatively static network topologies, the challenges are multiplied when moving to a dynamic cloud-based environment.

Automated workflows and orchestration—from detection, to protection, to response—were an essential requirement for this bank and therefore a major advantage of the Fortinet solution.

The automation of network operations afforded by the Fortinet Security Fabric helps the bank's DevOps team to focus on time to market, improving operational efficiencies through zero-touch provisioning, and generating real-time insights into issues such as spikes, scaling, and priority routing of traffic. Automation of security operations reduces risk through proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.

The solution has also helped the bank meet their compliance requirements through automated audits, tracking, and ongoing reporting.

As a result, the new data center has revolutionized operations and service. According to the bank's global head of network technology spokesperson, "Before the new data center came online, it would typically take a number of weeks to launch each new service and the process could be very frustrating. Now, we can be operational in a matter of hours. This not only opens up new business opportunities, but greatly increases the productivity of our expanding development group. In fact, it is from this enhanced productivity that we have seen the most significant returns on our investment so far."

July 20, 2020 9:10 PM

732861-0-0-EN

D:\Fortinet\Case Study\Red Case Study\Northern European Bank\cs-FA-northern-european-bank-7202020