

USE CASE: NATIONAL BANK

Customer uses VLAN-based Ethernet encryption to maintain network performance

SITUATION ANALYSIS

A large National Bank, headquartered in Ankara, Turkey, is the country's seventh largest bank and the fourth largest network with 586 branches nationwide. Because it process millions of financial transactions every week, this National Bank understood the cost savings offered by utilizing Metro Ethernet.

They decided to take advantage of the cost savings and increased bandwidth offered by Metro Ethernet by migrating from their leased line and ATM infrastructure. However, they were very concerned about the protection of their data and the innate vulnerabilities of a Metro Ethernet infrastructure.

The National Bank decided not to move forward with their migration unless a solution was found to mitigate these security vulnerabilities.

THE BIDDING PROCESS

The National Bank held initial meetings with four vendors, two offering IPsec-based solutions, and two offering Ethernet encryption solutions. Due to the performance issues and additional complexities of an IPsec-based solution, they immediately eliminated two proposals.

SOLUTION REQUIREMENTS

The National Bank recognized the need for a network-level data encryption solution. They needed a solution that worked native to a Layer 2 infrastructure and was capable of encryption based on VLAN ID. This ability would enable them to choose which data streams would be encrypted and which would be transmitted in the clear.

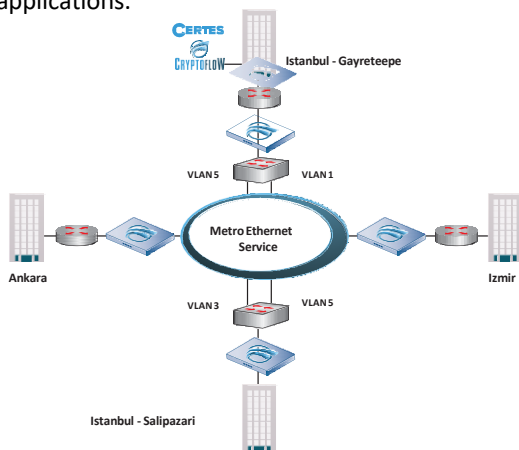
The solution also needed to work with their custom hub & spoke topology, support point-to-multipoint applications and offer an automated encryption key manager for their multicast applications.

The National Bank decided on a phased transition to Metro Ethernet and required an encryption solution capable of accommodating their rollout schedule, without adding complexity or time-consuming configurations. They started with four back-up lines to ensure the deployment would proceed as planned. Once those lines were up and fully functioning with the encryption, they would begin a staggered deployment to 22 other nodes. In addition, the National Bank also required the solution to support point-to-multipoint encryption and have an automated encryption key manager for their multicast applications.

Most importantly, the solution could not impact their Quality of Service (QoS) applications, nor could it add more than a few microseconds of latency to their overall network performance.

At the request of the National Bank, the two vendors with Ethernet encryption solutions were brought in for further testing. Once the initial testing was complete a Request For Proposal (RFP) was released detailing the requirements. The first vendor proposed a strict point-to-point implementation at each node. The National Bank recognized the operational complexity involved in this type of deployment and knew this solution would be difficult to manage. It was evident this approach would not work with their secure multicast applications and did not fit with their overall large-scale deployment strategy.

Certes Networks proposed their policy and key management solution and low-latency encryption appliances to protect the National Bank's sensitive data. This approach to policy and key management offered the flexibility to meet all of the customer requirements, including a simple deployment roadmap and the ability to encrypt multicast traffic without compromising network performance or applications.



With Certes Networks, the National Bank is able to keep their existing Ethernet architecture and VLAN separation, while encrypting customer data throughout the network.

DEPLOYMENT

The National Bank was eager to implement the encryption solution and continue with their network transition. However, they were not willing to take any chances with their data by rushing through the installation and deployment process. On the first day, the first phase of the initial deployment was staged for testing. The National Bank's network team was impressed with the simple installation and easy deployment of the encryption solution.

Because of the success of the initial deployment, the National Bank decided to immediately move forward and encrypt a link from Istanbul to Ankara. Early in day two, the National Bank was sending and receiving encrypted traffic between the two sites.

The remaining encryption appliances were deployed into the remaining initial sites just as smoothly. The National Bank was able to centrally configure the appliances, generate security policies and encryption keys, and then deploy them into the network. Within a matter of days, the National Bank was sending and receiving encrypted network traffic from four sites, without performance degradation or adverse effect to their QoS.

RESULTS

With the successful installation of the Certes Networks Layer 4 solution, the National Bank is realizing the anticipated cost savings of Metro Ethernet while maintaining the highest level of data security available. This encryption infrastructure provides the National Bank with top functionality with zero impact to performance enabling them to utilize existing multicast services while encrypting data in transit. The National Bank is currently working on the next phase of the overall deployment of new Metro Ethernet sites.



Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.