

Customer Situation

This Southeastern U.S. Regional Bank is an independent financial institution focusing on consumer finance in general, and on real estate and cash loans in particular. Since the early 1940's, they have been providing sound financial advice and services for families and individuals based on Benjamin Franklin's "common folk" ideals. The Regional Bank currently operates more than 250 branch offices in the Southeastern United States and they are continuing to expand throughout the region.

From its very beginning, the Regional Bank has, as part of their corporate mission statement, adhered to "industry best practices" in order to pursue a healthy financial position for itself and its customers. With the recent reports of security breaches and data theft within the industry, as well as the increasing government and industry regulations, the Regional Bank recognized a need to proactively protect their customers' personal identifiable information.

With this in mind, the Regional Bank began looking for ways to protect their customers' personal and financial information as it traversed their network. They were particularly interested in finding a way to add data protection without impacting performance or re-architecting their network.

CASE STUDY

Regional Bank

Bank deploys group encryption to encrypt VoIP and data between 250 locations



Solution Requirements

The Regional Bank operates a fully meshed topology with 250 sites over a converged MPLS backbone. Traditional data applications, Voice over IP telephony and distance-based training are utilized at every location. The IT staff required any proposed solution to be:

- Transparent to network applications and performance
- Interoperable with the existing MPLS infrastructure
- Centrally configurable and manageable
- Capable of generating a report for auditors to prove their customers' information is secure

In addition to the technical requirements, the Bank asked for a very aggressive roll-out schedule. Since the fourth quarter is typically the busiest time of the year for this Regional Bank, the entire solution needed to be deployed, installed and operating by the end of the third quarter, which left only a 60-day window for the complete installation.

Deployment

The Regional Bank turned to their telecommunication service provider for a solution. The service provider knew that in order to meet the Regional Bank's strict performance and technical requirements, a novel solution was required. Traditional VPN encryption solutions would make it nearly impossible to manage 250 fully meshed sites and would degrade network performance, disrupting latency-sensitive applications such as VoIP.

The service provider's security team had the solution. Having deployed it successfully with other accounts, they knew Certes Networks' group encryption solution would meet all of the customer's requirements and had already been approved for deployment on other customers' MPLS networks.

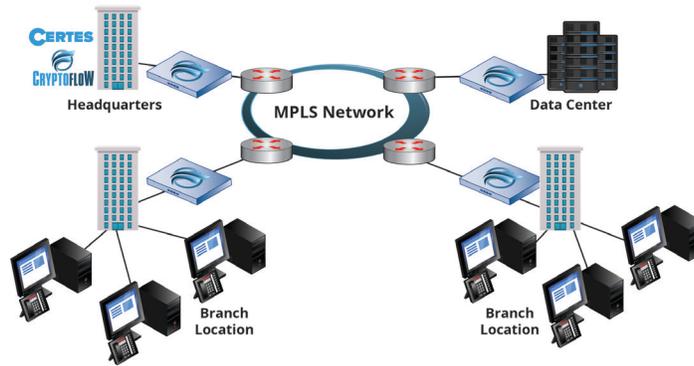
CASE STUDY: REGIONAL BANK

Certes Network's policy and key management solution offered the Regional Bank a unique approach to network encryption with capabilities that no other company could match, including:

- **Simple Tunnel-less Encryption** - A unique approach that greatly simplifies the implementation of network-wide encryption. With tunnel-less encryption, network performance is maintained and no network changes are required.
- **Strong Protection of Customer Information** - Protects converged voice, video and data using industry standard AES 256-bit encryption.
- **Microsecond latency** - Optimizes encryption with latency that is measured in mere microseconds. This means that even the most latency sensitive applications such as Voice and Video over IP do not suffer performance degradation.
- **Centralized Management** - A centralized management portal where security administrators can manage security policies, encryption key distribution and appliance configurations.

The security team decided to implement Certes Networks' group encryption solution, which met every one of the Regional Bank's requirements. In order for the deployment to be completed before the beginning of Q4 business, the service provider needed to stage, ship, deploy and activate the entire encryption solution at all 250 fully meshed sites within 60 days.

The solution called for the deployment of one 100 Mbps encryption appliance at each of the Regional Bank's branch offices, as well as at the HQ office.



Security policies are defined and then encryption keys are dynamically distributed to all 250 encryptors.

Results

The deployment was completely shipped, installed and running at all 250 sites in less than 45 days. Each of the design and performance requirements were met—on time and above expectations.

With their entire network now encrypted, the Regional Bank is proactively protecting their customer data and VoIP communications. By grouping their endpoints and sharing encryption keys with those endpoints, the Regional Bank is able to treat this fully meshed, 250 site network as one group. This drastically reduces the management complexity and eliminates the performance issues typically associated with traditional encryption.

The Regional Bank has set the bar with their determination to provide the highest level of data protection for their customers' personal and financial information.

“

We are very pleased with the simplicity and effectiveness of the group encryption solution deployed by the service provider.

”

— Director of IT
at the Regional Bank.

About Certes Networks

Certes Networks' solutions safeguard enterprise data communications to ensure privacy compliance and block the top data breach attack vectors. Banks, financial institutions, healthcare organizations, governments and other companies in nearly 100 countries rely on Certes' security and compliance solutions to protect their sensitive networked applications. The solutions feature unique Layer 4 "stealth encryption" technology that automatically encrypts data communications and enables enterprises to adopt modern Zero Trust security protection.

For more information visit CertesNetworks.com

CERTES

Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East
and Africa Sales
emea@certesnetworks.com