USE CASE: REGIONAL BANK

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

SITUATION ANALYSIS

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.

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 tele-communications 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 Provable Security™ delivered through the Certes Layer 4 solution would meet all of the customer's requirements. Prior Certes technology had already been approved for deployment on other customers' MPLS networks.

SOLUTION

Certes Networks Provable Security™

To help network security team to achieve their goal of keeping the regional bank's data safe, the team must begin to think of data security as a measurable contribution to the organizations.

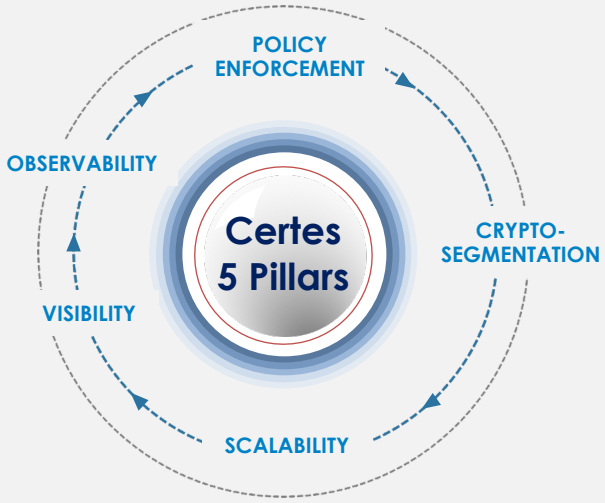
Certes Networks Provable Security™ introduces a new way to think about data security and the effectiveness of your security strategy based on the Certes Five Pillars, key performance indicators (KPIs) that are ***quantifiable, measurable and outcomes driven.***

How We Deliver on Provable Security

Certes Networks Provable Security™ is supported and interconnected by the Certes Five Pillars. Each pillar is a KPI that measures the value that the security strategy delivers to an organization as a whole.

The Certes Layer 4 technology solution delivers on these KPIs and is able to quantify security's role to build, modify and measure a security strategy that aligns and protects the needs of the regional bank while mitigating risk.

CERTES NETWORKS PROVABLE SECURITY™



Quantifiable, Measurable and Outcomes Driven

The Certes Five Pillars

PILLAR ONE: POLICY ENFORCEMENT

Certes Networks Provable Security™ starts with the premise that policy enforcement is only as good as the policy defined and how that policy is enforced

While threats are virtually infinite, data access is finite and measurable. Therefore, by allowing policy enforcement at a level of granularity that quickly eliminates risk, security can, in fact, be manageable, measurable, outcomes driven and ultimately, provable.

PILLAR TWO: CRYPTO-SEGMENTATION

Crypto-segmentation, removes the implicit trust and helps prohibit lateral movements in the network. Crypto-segmentation creates small zones by which organizations can separate applications and workloads to secure fine-grained policies individually. But one challenge created by this approach is gaining visibility into just how many available pathways exists. The ability to visualize these thousands of potential paths between applications, workloads and data sources is essential.

PILLAR THREE: SCALABILITY

Scalability refers to the ability to implement secure data protection technology that is independent of your applications and network infrastructure.

The Certes Layer 4 solution is a simple and scalable, end-to-end encryption management solution that is interoperable and integrates easily into any existing network whether Legacy network, 3rd party network or multiple sites in different locations -- all without having to move, disrupt or replace your current network infrastructure.

PILLAR FOUR: VISIBILITY

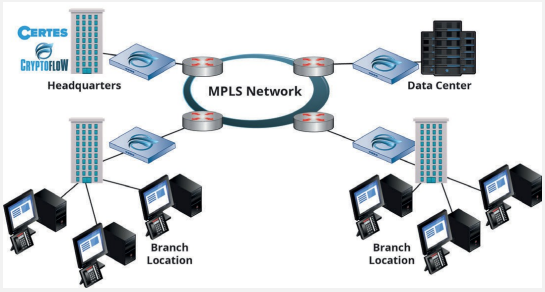
The Certes Layer 4 solution encrypts data in transit and allows for secure masked encryption of only the payload, and not the entire network data packet, independent of applications and network with no changes to routers, switches and firewalls. With standard IPsec encryption there is no visibility of data at Layer 3 and Layer 4.

By applying the Certes Layer 4 solution, network visibility and operational functionality are maintained providing security for data in transit.

PILLAR FIVE: OBSERVABILITY

Certes Observability is a mandatory key performance indicator and completes the Five Pillars of Certes Networks Provable Security™ in order to quantify and measure a security strategy that aligns with the business needs of an organization while mitigating risk.

Certes Observability is the Policy Enforcement Engine that provides visual proof that your security strategy is effective. It enables greater insight into the overall reliability, impact and success of systems, their workload and behavior. Real-time solutions are now observable via a global view of the network environment.



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

"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.

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.

CERTES NETWORKS

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@certesnetorks.com

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