Customer Situation

A Judicial Department of a northwestern U.S. state set out to establish a disaster recovery plan to ensure business continuity for the state's judicial system in the case of a major catastrophe. For their back-up data center, the Judicial Department chose a hardened joint military and civilian site, which was aimed at integrating state and federal resources into a single "readiness" center.

The new site is located several miles from the existing Judicial Department data center and connected via a municipally-owned fiber network. The new facility provides the Judicial Department with both physical security and environmental security for their servers and storage devices with features such as redundant network paths, earthquake resistant racks and fireproof server facilities. These measures assure the department's judicial proceedings, case file information and other electronic court-related documents remain available in times of a natural or man-made disaster, or terrorist attack.

In order for the Judicial Department's data to reach the new site, it has to be sent beyond their own physical network. To prevent the accidental or malicious loss of vital records and personally identifiable information, the Judicial Department decided to protect this information by encrypting all data transmissions to and from the new disaster recovery site. The Judicial Department also needed to relocate some of their servers from the existing data center to the new readiness center and bring them back online with the encryption in place. All of this was to be accomplished without server reconfiguration or interruption of the judicial system's daily business.

CASE STUDY

Disaster Recovery

State Judicial Department encrypts traffic between courthouse and recovery site

Solution Requirements

The Judicial Department requires instant access to records, cases and other information stored on their servers. This means that as the Judicial Department migrated to the new data center, they could not take the network down. The encryption solution had to be deployable without disrupting network applications, compromising the speed of their gigabit links or impacting the users in any way.

They also required a flexible encryption solution that could adjust to future changes in the network infrastructure. They wanted to migrate resources at their own pace without changes to the equipment that could force "cut-over" timelines or operational windows to work around.

Lastly, the encryption solution needed to integrate into their existing Layer 2 infrastructure that connected the two facilities, but also be capable of accommodating a move to an IP infrastructure in the future without appliance upgrades, massive reconfigurations or re-architecting of the network.

The Judicial Department needed a scalable encryption solution that was quick and easy to install, simple to manage and did not compromise their network performance. The Judicial Department had already received the budget for this project, but the project had to be completed by the end of the current fiscal year. They needed to select a vendor and implement the solution in a relatively short time frame in order to meet both budget and facility move-in deadlines.

The Bidding Process

The Judicial Department summarized their technical requirements into a formal and public Request for Quotation (RFQ). However, most encryption vendors could meet only a few of the requirements. More specifically, only one vendor offered deployment flexibility that allowed a smooth and transparent data center move without time-consuming and complex network architecture changes. In addition, only that one vendor offered a single platform with the ability to adjust to future changes and modifications being considered for the Judicial Department's network infrastructure.

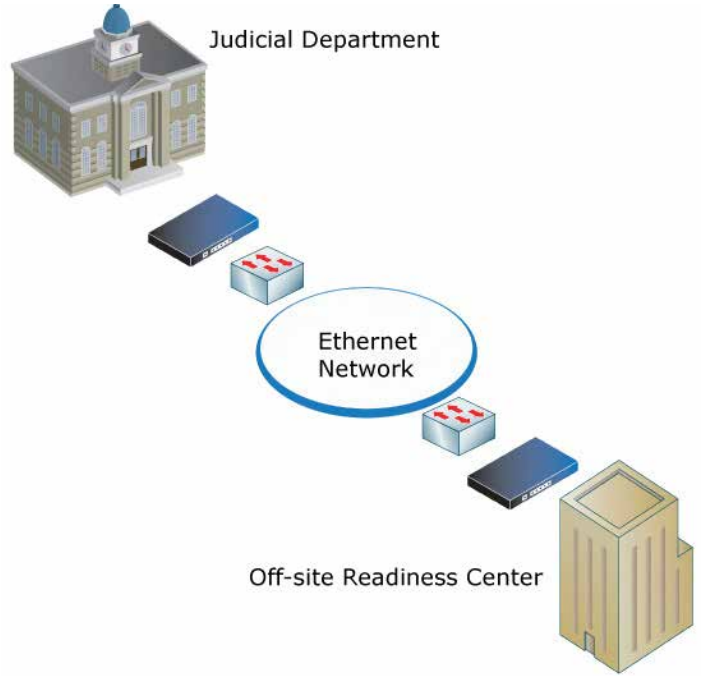
Certes Networks' network encryption solution offered all of the capabilities and flexibility required for this deployment. With its transparent nature and capability of being deployed into either Layer 2 or Layer 3 networks, it was a natural fit. Only one bid was received that could satisfy all the current and future requirements for the Judicial Department's encryption needs; the one with Certes Networks' encryption solution.

Installation

Before they began the actual migration of data, the Judicial Department wanted the readiness center to be fully functional. Once the servers were physically moved and the new data center was ready for the encryption solution, the gear was brought in. The morning was spent training the Judicial Department's IT personnel on the configuration, operation and management of the new appliances. By the end of the day, the IT staff had the encryption solution configured, installed and deployed with basic security policies. Over the course of the next few weeks, the Judicial Department continued to fine-tune their security policies and maximize their application performance.

In order to meet their high availability requirements, the Judicial Department deployed redundant encryption appliances in both of the data centers. This high availability option allows for the standby and hot failover to a secondary encryption appliance, guaranteeing that the data will continue to be protected and available in the rare event of an encryption appliance or network infrastructure failure.

In the case of this Judicial Department's deployment, the centralized management point was established in the IT department office, which is not in either data center. With this feature, the network administrator does not have to leave their desk to change security policies or add additional encryption into the network. Everything can be managed remotely from the administrator's desktop.



The Judicial Department deployed a Certes Networks encryption solution to protect their data as it travels between the Courthouse and the off-site Disaster Recovery center.

Results

By deploying the Certes Networks encryption solution, the Judicial Department met all of their requirements. They completed the installation and migration within their budget and time frame. This solution gives them the flexibility to expand their encryption in the future with ease. It was quick and easy to install and it did not compromise their network performance or impact their end users.

Certes Networks also enables the Judicial Department to migrate at any time to an IP networking infrastructure without affecting their current security infrastructure. The encryption appliances will continue to provide high-speed, low latency encryption on either network infrastructure. The Judicial Department now ensures the confidentiality and integrity of their data as it moves between their data centers with a solution that delivers the flexibility, transparency and manageability they require.

About Certes Networks

Certes Networks protects data in motion. The company's award-winning CryptoFlow® Solutions safeguard data traffic in physical, virtual and Cloud environments, enabling secure connectivity over any infrastructure without compromising network device or application performance. Companies around the world rely on network encryption products from Certes Networks to protect data, accelerate application deployment, simplify network projects, reduce compliance costs, and improve the return on investment in IT infrastructure.

For more information visit **CertesNetworks.com**

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

V2-08-25-2015