USE CASE: DISASTER RECOVERY

State Judicial Department encrypts traffic between courthouse and recovery site

SITUATION ANALYSIS

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, including a terrorist attack.

In order for the Judicial Department's data to reach the new site, data had to traverse 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.

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 render their network inoperable.

The encryption solution had to be deployable without disrupting applications or network infrastructure nor compromise functionality or performance.

RFP 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 service provider offered deployment flexibility that did not

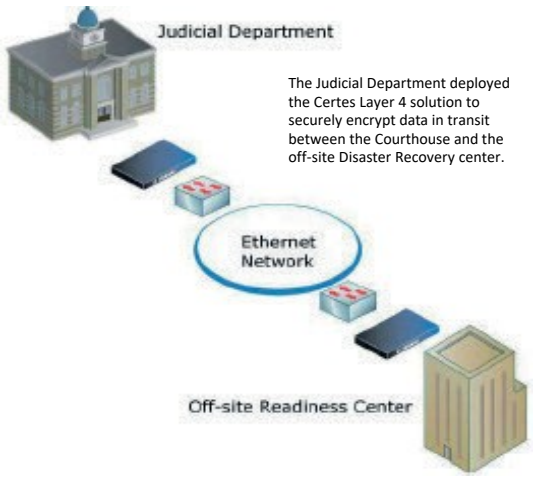
require any changes or disruption to network operations. In addition, only one service provider offered a single, scalable platform to scale for future upgrades and modifications.

The Certes Layer 4 solution offered all of the capabilities and flexibility required for this deployment. This encryption management solution is network agnostic, can be easily integrated into and fully interoperable with any network, and can be deployed at either Layer 2, 3 or 4.

Only the Certes Networks bid could satisfy all the current and future requirements for the Judicial Department's encryption needs and, therefore, was selected to implement the Certes Layer 4 solution.

IMPLEMENTATION

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 Certes Layer 4 solution, the Certes Enforcement Points (encryption appliances) and key management system were implemented.



The Judicial Department deployed the Certes Layer 4 solution to securely encrypt data in transit between the Courthouse and the off-site Disaster Recovery center.

The IT team was then trained on the configuration, operation and management of the new appliances. By the end of the day, the IT staff had the Certes Layer 4 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 failover to a secondary encryption appliance, guaranteeing data will continue to be protected and available in the event of an encryption appliance or network infrastructure failure.

The centralized management point was established in the IT department office, which is not in either data center, so that remote management was possible, thus decreasing additional resources.

RESULTS

By deploying the Certes Layer 4 solution, the Judicial Department met all of their requirements. They completed the installation and migration on budget on on time. This solution gave them the scalability to expand their network in the future and installation was quick and uncomplicated with zero impact to network performance.

The Judicial Department is able to migrate at any time to an IP networking infrastructure without affecting their current infrastructure. The Certes 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 in transit with a simple, scalable and uncomplicated solution.

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.