

# SITUATION ANALYSIS

Columbia County Sheriff's Office is a law enforcement agency based in the State of Florida.

Their data network is comprised of six sites connected over a carrier provided MPLS backbone. The MPLS network delivered Service Level Agreement (SLA) on prioritization of delay sensitive traffic to ensure high quality voice over IP and video over IP traffic. Also required was support for multicast applications in use on the Sheriffs Office network.

The six locations consist of:

- Central Administration
- Data Center
- The County Jail
- Dispatch
- The Courthouse
- The Task Force

Each location other than the Central Administration site is unmanned in terms of IT skills and requires an engineer callout on any issues at each site.

# **CUSTOMER REQUIREMENTS**

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) division enforces a security policy that specifies that all Criminal Justice Information (CJI) in transit should be encrypted when it moves across data network connectivity that sits outside of a trusted location, meaning when wide area connectivity such as MPLS, VPLS, SD-WAN, Dark Fiber, Metro-E, Microwave or Long range WiFi is used. Being a Law Enforcement agency, Columbia County Sheriffs office requires access to CJI, which is shared from one location to another. Therefore it must comply with the CJIS Security Policy.

In addition to deploying an encryption technology, the CJIS Security Policy states that the standard to be deployed must be FIPS-140-2 certified encryption.

### IN ADDITION, RECOMMENDATIONS ARE MADE THAT:

An encryption key management control process should ensure only authorized users have access to encryption keys. The most practical way to meet this recommendation was to ensure that encryption keys were owned and managed by the Sheriff's Office.

### **FINAL CHALLENGES**

The final challenge for the Sheriff's office was that any standard encryption solution would;

- Remove the ability for the carrier to see the Quality of Service (QoS) markings on the data traffic that allows them to prioritize delay sensitive traffic needed to meet their SLA.
- Introduce delay to network traffic
- Not support multicast applications
- Require infrastructure and configuration changes to the existing network
- Require additional costs for licenses on the firewalls, routers or switches

# THE SOLUTION

Certes' High Assurance Encryption Overlay was deployed utilizing Certes Layer 4 patented encryption. A single instance of the Crypto Flow Net Creator Orchestration platform was deployed at the Administration/Data Center as a virtual machine to enable centralized management for all deployed enforcement points.

At each site a Certes Enforcement Point (CEP) was deployed. The process was simple in terms of planning and execution as the following three step process was used:

The Certes physical appliance which would run as an enforcement point was deployed at each location behind the WAN router. This was a simple task of unplugging the LAN connection and Inserting the Certes device during a schedule d change window.

A management IP address was configured on each CEP device, and the device was added to the Orchestration platform. Each enforcement point was adopted, a policy was created to encrypt all traffic between sites using an Easy-Mesh layer 4 policy, and the policy was pushed to the enforcement points.

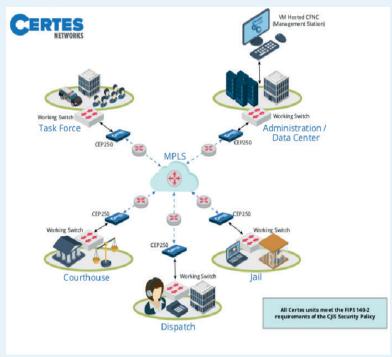
Once the CEP's were deployed over a period of one week (across all 6 locations), the adding of the devices and the pushing of a policy to encrypt the required data took less than an hour, creating a very happy customer.

In addition to the technical deployment, the Sheriffs Office was also provided with all the supporting documentation for inclusion within their CJIS Audit Documentation Set which would enable them to provide evidence to a CJIS auditor that technology controls were deployed In accordance with the requirements of the CJIS Security Policy.

# **KEY BENEFITS**

- Quick and easy deployment enabling the Sheriffs Office to quickly react to and meet the requirements of the CJIS Security Policy.
- The Sheriffs Office retains ownership and control of all encryption keys and can automatically rotate (change) the keys in use every hour with Zero Impact to traffic and with Zero touches required.
- Certes Patented Layer 4 Encryption is an 'Overlay and fully transparent to the network and Service Provider, resulting in no impact to SLA's, traffic performance or multicast application traffic.
- Subscription based pricing with low cost of entry but fully scalable and upgradeable to meet future requirements.





# CERTES' INTERVIEW WITH WAYNE CRAIG, DIRECTOR OF IT AT COLUMBIA COUNTY SHERIFF'S OFFICE, REGARDING THE COUNTY'S CJIS AUDIT CHALLENGES.

What was the key challenge you had when it came to ensuring your department's compliance with the CJIS Security Policy?

A key challenge was meeting the requirements to encrypt Criminal justice Information In translt. ACJIS audit was scheduled to take place within the next month and we did not have a solution In place. Traffic was being transmitted across our network unencrypted.

Were you actively looking at solutions prior to the <u>audit?</u>

Our team had been looking at options but did not find anything suitable. All of the options that met the FIPS 140-2 certification requirement were either:

- 1. Too expensive (like many small-medium sizes counties, our budget is limited!)
- Too complicated to Implement as our County's IT department did not have adequate resources in place to take on an implementation on top of their demanding workload.
- Too long to implement in order to meet the audit timescales.

Why did you choose Certes as your CJIS solution?

Certes proposed a solution that was affordable and was within the county's budget. I attended an on-line product demonstration and was able to determine that Certes' solution was easy to implement and It would be possible to do so within a matter of days. This was very helpful as it meant that the County could have a solution in place prior to the pending CJIS audit which was due to take place Imminently.

The County was also Impressed that we would not need to take on additional resources for ongoing management of encryption keys. Other solutions we looked at would require the County's IT team to take on additional staff to do this. This was not the case with Certes solution' - we were very impressed with the fact that key management was automated, needing minimal resource.

## How did the implementation go?

Like any implementation, we had to blend the solution in with our infrastructure. Certes' provide great support in ensuring that everything was connected the way it should be.

What is the current status with your network and CJIS compliance?

Our network is operating exactly the same after the Implementation of Certes equipment as It did beforehand - there have been no issues. We have had confirmation from the FDLE auditor that our solution to encrypt CJI in transit meets the requirements of the CJIS Security Policy.



**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