



*iPolicy Networks' Intrusion Prevention Firewall are helping state and local government achieve stronger security and regulatory compliance through integrated networks security solutions.*

Case Study

**EXECUTIVE SUMMARY**

**Industry:**  
**State Government**

**Environment:**  
Utah's Department of Alcoholic Beverage Control (UDABC) manages all licensing, distribution, and oversees 37 retail liquor stores and is thus responsible for protecting sensitive credit card data. The agency's 1000 BaseT network is connected by T1s to 37 remote sites.

- Key Business Challenge:**
- Customer credit card data at possible risk.
  - Additional security needed to support compliance requirements.
  - No pre-patch shield in place when testing patches.
  - Reporting tools tedious to use
  - Can't afford to disrupt business operations with a complex security solution deployment

- Key Business Solution:**
- Installed iPolicy's Intrusion Prevention Firewall with intrusion detection and prevention, Layer 3-7 deep inspection stateful firewall & URL/content filtering.
  - Comprehensive security solution detects & prevents network attacks
  - Pre-patch shield protects against vulnerabilities while waiting for and/or testing patches.
  - Graphical reporting tools take just minutes instead of hours to use
  - iPolicy solution deployed and operational in under four hours

**Key Business Benefit:**  
Utah's Department of Alcoholic Beverage Control runs a network with enterprise-level security measures, equipping the agency with strong tools to prevent network attacks & theft of customers' credit card data.

**iPolicy Networks' Intrusion Prevention Firewall protects a progressive state agency's sensitive customer data.**

**Background**

The State of Utah is one of 18 states that take a proactive stance on promoting moderate, rather than excessive, use of alcohol. To achieve this, Utah's Department of Alcoholic Beverage Control (UDABC) is largely responsible for all licensing, distribution, and sales of alcoholic beverages. While full liquor service is available in licensed restaurants, banquet and catering facilities, airport lounges, and private clubs, patrons purchase packaged liquor, wine, and heavy beer in State Liquor Stores and Package Agencies..

Today, the UDABC runs 37 retail shops throughout the state. As with any retail operation, customers often pay for their purchases with credit cards. The UDABC takes the responsibility of protecting its customers' financial information as seriously as it does maintaining the sensible use of alcohol.

**Key Challenge**

With so much sensitive data at stake, the UDABC's Technical Support Specialist Supervisor, Kevin Perry, wanted peace of mind that the right security measures were in place to protect the agency's network from hackers and viruses. Rather than rely solely on the firewall that all Utah state agency networks reside behind, Kevin wanted to install an extra measure to protect private customer data: a solid perimeter of security surrounding the UDABC network.

Additionally, as a retail operation the UDABC needed to adhere to certain compliance regulations that other state agencies did not; specifically, the PCI Data Security Standard compliance mandate required by all major credit card companies. Using VISA's CISP standard as its framework, PCI Data Security Standard compliance is meant to protect cardholder data. Merchants that are not compliant can face hefty fines. However, implementing the PCI Data Security Standard requirements – from installing data encryption software to developing complex security monitoring policies – is not an overnight process.

What Kevin Perry wanted to find was a comprehensive network security system that would serve as permanent protection of the UDABC's network, while providing the heightened level of security required for CISP/PCI compliance. Because time was of the essence, it was critical the chosen security system could be deployed in a matter of hours, not days, without disrupting network operations – a requirement that Perry was uncertain a sophisticated security technology could meet.

**"We couldn't afford to interrupt our daily operations, and were delighted find that iPolicy's security products could be deployed in just a matter of hours. Couple that with the great price point and ease of use, and you have a truly impressive security solution"**

Kevin Perry, Technical Support Specialist Supervisor  
State of Utah's Department of Alcoholic Beverage Control

### Additional Issues

Like other organizations running Windows-based networks, the UDABC depends on Microsoft patches to ward off the latest viruses. But patches can cause the breakdown of other network systems, and what's more, IT staff can't always test a patch in time to assure it won't cause network interruption. This posed the UDABC with the problem of how to keep its network guarded any time a patch was being tested.

Additionally, from a management perspective, the previous security reporting tools were hardly efficient. Kevin Perry's team had to sift through page after page of log items to identify the kinds of attacks that were coming in. In fact, this four to five-hour process was so time consuming and tedious, it was generally limited to a weekly basis.

### Solution

The UDABC evaluated three security solutions, and soon realized the first two would not meet their strict requirements to have a fully operational security infrastructure in a short time window. Both required complex installations that would significantly interrupt the agency's daily business operations, and likely take at least a week to fully deploy.

iPolicy's integrated network security products quickly moved to the head of the line. It was clear the entire iPolicy solution could be deployed in under four hours, and just as important, the product's security and reporting features more than met the UDABC's other requirements. For example, the iPolicy Intrusion Prevention Firewall blocks network exploits, thus "shielding" the network until patches are tested and rolled out. As an additional security measure, protection is also provided for all 104 computer cash registers at the UDABC's 37 retail stores, as iPolicy's application-aware deep packet inspection firewall prevents attacks that can take over individual PCs and steal credit card data. The integrated URL and content filtering block access to "rogue" sites that install viruses, or drive-by download sites that chauffeur spyware into networks to steal customer information

Reporting tools provide an aggregate security view of the complete network and show real-time traffic and hacking attempts as they occur. Kevin Perry's team no longer has to leaf through huge log files to do forensic analysis of the attacks on their network – iPolicy's reporting capabilities list them side-by-side along with other network usage information.

### Results

Kevin Perry finally has peace of mind. He's confident that customer data is protected from hackers and viruses, and that his network is safe from attacks as he progresses through the CISP/PCI compliancy process. Numerous hours a week that were previously devoted to scrutinizing complicated security log files have effectively been eliminated and replaced with intuitive, graphical reports that let UDABC's IT staff identify network attack attempts within minutes.

After a year of solid performance, the UDABC strongly believes iPolicy security products are a smart defense against would be data thieves and network attacks.

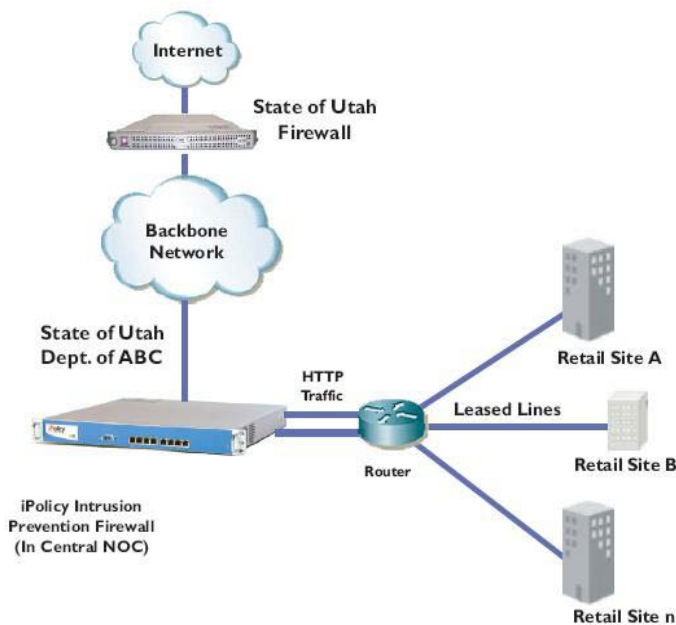


Figure 1 - Network diagram showing deployment of iPolicy's Intrusion Prevention Firewall 3300