ciena
Experience. Outcomes.

TRUSTED ASSURED NETWORKING RELIABLE & SECURE

APPLICATION NOTE

Protecting In-Flight Data: Network Encryption for State and Local Government

Modern government depends increasingly on the secure collection and distribution of information among agencies and citizens. This information needs to be networked and shared among geographically dispersed data centers, government offices, and other remote locations. Security and privacy are essential to establishing and holding the public's trust in government. This trust extends to information technology systems that contain taxpayer information, public safety records, healthcare records, educational records, and other personal and often sensitive information.

At the same time, government must adopt networking systems that offer high performance and the ability to economically scale. If implemented properly, IT systems can reduce the burden on government while improving citizen service and lowering operational cost. For example, consolidating data centers and adopting cloud applications through a modern network allows state or regional governments to assure ready availability and security of citizen information such as tax records, while reducing cost from redundant networks and outmoded manual systems.

In some cases, such as handling of health care records or certain law enforcement information, regulatory compliance must be maintained. Encryption is an essential piece of a modernized IT network implementation.

The Ideal Network Encryption Solution

Whether network encryption is part of a private optical network or provided by a service provider as part of a managed service, key points to consider include:

Regulatory compliance – State and local government entities must be cognizant of regulations that may apply to the applications carried by their networks. For example, state-level Medicaid provider networks carrying patient health records must ensure HIPPA compliance. Regional and local governments sharing taxpayer or judicial information must make reasonable efforts to assure citizen confidentiality. It's essential the chosen solution meets compliance requirements.

Benefits

- Protects network workflows of all types, including imaging, data files and video
- Assures public confidence in government IT systems that contain personal information
- Protects citizens from identity theft
- Prevents theft of government operational information
- Protects against malicious interruption of critical public safety operations
- Reduces financial risks from stolen information
- Protects commercial interests, including patents, competitive information, etc.

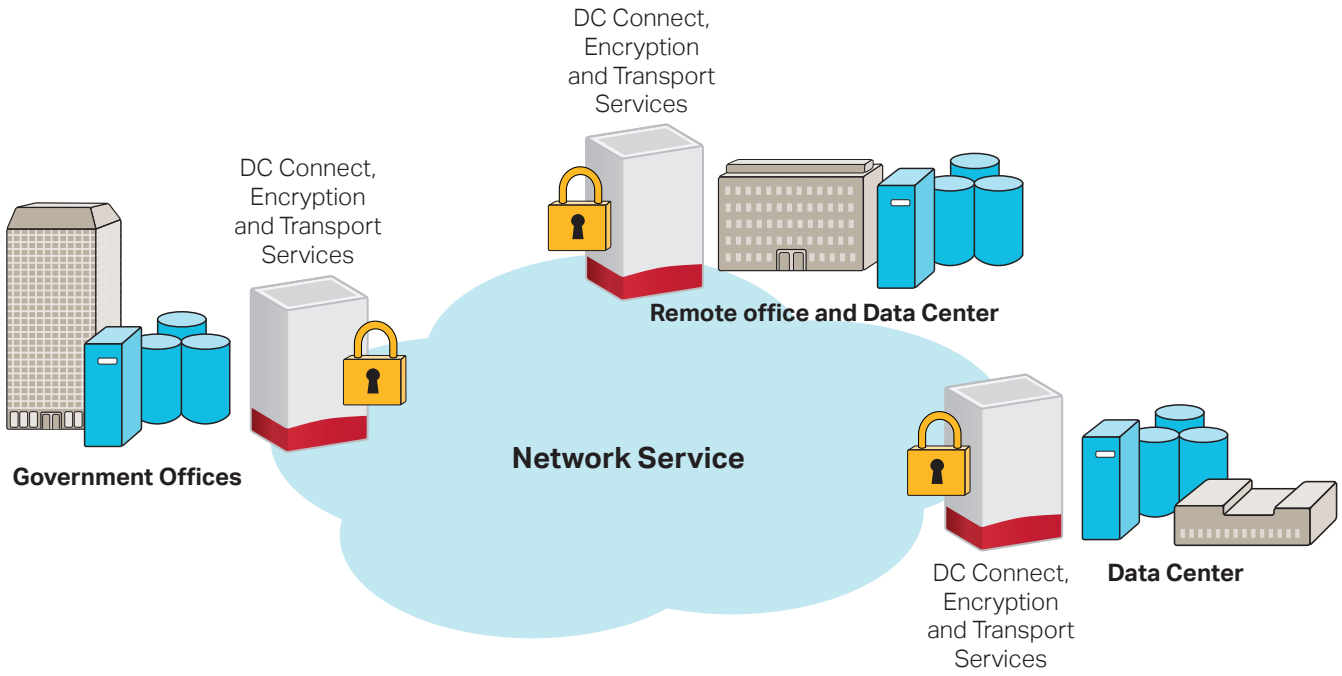

Figure 1. Encryption in a government network

Latency – For latency-sensitive protocols and applications, delay parameters offered by the encryption solution can be impactful. State-of-the-art encryption solutions offer hardware-related latency parameters in the region of several microseconds.

Transparency and scalability – Networks are constantly evolving. Services that run over networks today will likely be different from those that will require support in the future. It's important the chosen solution supports protocol-agnostic encryption that offers the flexibility to support a variety of client and transport interfaces. Network bandwidth itself will probably change too, so scalability is crucial.

Management – Whether encrypted links are managed by government or a service provider, the "owner" of the data—the end-user—should maintain control of the encryption keys, issue new keys as needed, and have visibility to security alarms and logs. This is accomplished by separating the network management from the encryption key management. If the encrypted service is purchased from a service provider, the provider will manage the links, their provisioning, administration, and performance monitoring, but will not have control of key distribution or maintenance. Depending on the organization's security policies, key distribution can be performed manually or automatically over secure, encrypted tunnels.

A comprehensive security approach must encompass not just "data at rest," including data residing in databases, file, and storage systems, but also in-flight encryption to ensure data is protected from unauthorized discovery as it traverses the network. Today's in-flight encryption techniques can camouflage traffic so it cannot be read or manipulated, and even disguise the fact that there is traffic flowing at all.

Connect with Ciena now