

Network Security for Financial Companies and Banks

The financial industry is faced with increasing pressure to secure financial data both at rest and in motion while at the same time looking to take advantage of advanced business applications and virtualized infrastructures that require fast and reliable connectivity. These two opposing forces often put network and security administrators at odds as they attempt to make tradeoffs between performance and security. This solution note highlights how Certes Networks TrustNet Manager solution can eliminate these tradeoffs by protecting all forms of sensitive information including data in motion, voice and video without impacting the performance or reliability of the networks they traverse.



Why You Should Encrypt Data in Motion

1. Data Security is more than PCI.

In addition to PCI nearly every US State and Most European and Asian Governments have their own data protection requirements, which all have their own audit and fine structures.

For financial companies this means that in addition to what is likely to be a massive post breach customer exodus, companies that fail to protect their customer's data will find a long line of auditors, regulators and bureaucrats on their doorstep waiting to levy fines.

The take away is that customers and regulators are no longer willing to give financial companies a pass if unprotected data is breached. In fact, even in the absence of a breach, companies that fail to take steps to secure data are viewed as less desirable to do business with.

2. SSL/Tokenization are not enough.

Many believe that technologies such as SSL or Tokenization can cover their security needs, but the truth is they only solve a small part of the problem.

SSL was designed and is best suited to protect web-based applications. Tokenization is limited to making point-of-sale transactions more secure. While these are both useful, each provides only transactional security for front-end processes.

Companies also need to protect their back-end processes (network traffic between sites and data centers for example) which carry bulk information and are therefore much more lucrative (and damaging) from a cyber crime perspective. Front-end security protects your customers – Back end security protects the company.

3. PCI Auditors are looking for it.

If your business falls under the umbrella of "Finance" or "Banking" a looming PCI audit is a matter of when, not if. Once only the concern of large companies, the reach of auditors is extending to smaller markets.

Companies that fail audits are subject to very expensive and far reaching follow audits and are forced to implement remediation plans that may not align with their business plans.

Even companies using so called "private" networks are learning the hard way that auditors are on the look out for open Internet gateways on these transport networks. More telling is the Ethernet and MPLS providers make no assurances regarding data security traveling over their backbones, where data is sent in the clear.

While many firms understand the need for, and comply with, secure storage and end point security, few understand that data sent over a service provider network (even when the network is marketed as private) must also be secured by being rendered unreadable, unusable, and undecipherable. Failure to protect data in this way leaves data in the clear, exposing it to theft, replication and unauthorized monitoring. Any questions about the security of these "private" networks are quickly answered by asking the provider for a guarantee of security and indemnified coverage in the case of a data breach over their backbone. If the provider is not able or willing to offer this level of protection than any claims of security should be called into question. Dont rely on your secure providers assurances if they refuse to back their claims.

A Much Needed Breakthrough in Network Security

The good news for financial companies is that a recent breakthrough in IPsec VPN technology has made it possible to encrypt any network topology (from simple point-to-point to full mesh and cloud) without using tunnels. This means you can now secure any network quickly and easily without impacting performance, visibility or reliability. With TrustNet Manager from Certes Networks it is now possible to quickly and easily comply with PCI and other data protection requirements for data in motion without adding complexity or downgrading network or application performance. Using TrustNet Manager financial companies can:

Improve Security

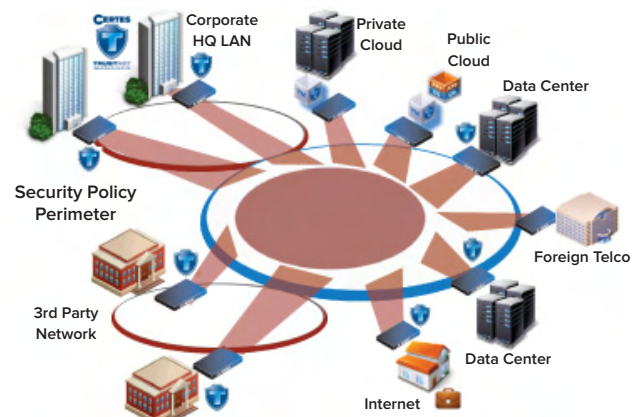
- Expand security without impacting availability or visibility
- Separate access and permissions for security and network team
- Enable automatic key rotations and Persistent Authentication
- Securely connect to public and private clouds

Save Time

- Takes only minutes to set up and manage
- Allows security "Green Zones" to help reduce the scope of compliance audits
- Allows network monitoring/troubleshooting without deactivating encryption

Reclaim Performance

- Replaces IPsec tunnels and runs at the full line rate
- Allows Secure Load Balancing, Disaster Recovery and High Availability
- Supports VoIP, Video QoS

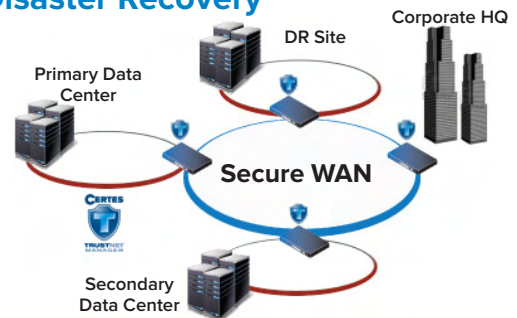


Compliant Network Security for Financial Companies

Certes Networks helps financial companies meet their security requirements with TrustNet Manager, an innovative data protection solution that provides high performance encryption over any network. The solution offers easy set-up, flexible deployment options, and global control of the generation of policies and dynamic distribution of keys. TrustNet enables organizations to encrypt data, voice and video over any type of network using standards based algorithms without compromising application or network performance. The scenarios outlined below describe three common use cases for TrustNet Manager within networks bound by PCI and other data privacy regulations.

Secure Data Center Networking and Disaster Recovery

Many financial companies maintain their own data centers and outsource back up and DR to third party providers or connect over provider networks. Best practices call for this data to be synchronously (or regularly) backed up to secondary data centers and disaster recovery sites with high throughputs.

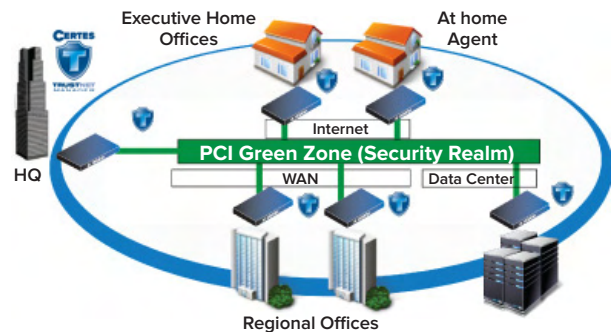


- If this data contains financial data, PCI and many other government based regulations require that this data be encrypted in motion.
- With TrustNet Manager data can be encrypted at wire rate from 3Mbps to 10Gbps and with Certes Networks' unique variable speed encryption option you only pay for the bandwidth you consume.

PCI Compliant Network Segmentation

When financial networks connect to regional offices, partners, third party agents or telecommuters, data security must be maintained. In some cases data flows must be cryptographically segmented from each other and from other parts of the business for SEC compliance.

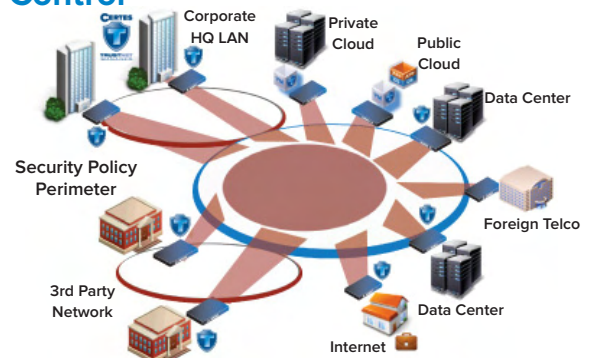
- TrustNet Manager makes it easy to cryptographically segment data within a common network. Policies can be managed from a single interface, even when connecting to third party networks.
- Certes Networks' unique ability to define and enforce security policies based on VLANs or applications (ports and/or protocols) gives you the flexibility to carve out secure communication zones without changing the network or disrupting operational performance.



Enterprise Wide Policy Control

When financial networks span multiple infrastructures and transport technologies security administrators have a difficult time defining network wide policies to ensure data security and compliance without third party involvement and/or network design changes.

- TrustNet Manager makes it easy to define and implement carrier independent data security policies on any network or group of networks without altering data flows, performance, availability or carrier SLAs.
- This technology is also extensible to the cloud allowing financial companies to take advantage of the cost and performance gains of virtualized infrastructures even for sensitive workloads.



About Certes Networks

Certes Networks is a leader in cloud security and multi-layer encryption solutions for high performance networks. The Company provides advanced network and cloud security solutions that make Wide Area Networks, Data Centers and both Private and Public Clouds safe for sensitive workloads. Certes Networks helps organizations improve security, decrease risk, and reduce the cost of compliance while enabling high performance and secure connectivity to critical infrastructures.