Securing Disaster Recovery Data in Transit

Business continuity requirements and regulatory mandates drive organizations to establish contingency plans for catastrophic events that put sensitive data and system availability at risk. These disaster recovery plans typically include the backup of massive amounts of data to storage area networks (SANs) or fully functional and redundant disaster recovery sites.

Today's remote sites usually store all of an organization's business critical information as well as sensitive information about employees and customers that are subject to government and industry regulation. Every disaster recovery and business continuity (DRBC) plan must therefore address the issue of protecting data streams over the network against interception or modification to ensure data integrity, privacy, and maintain compliance with regulatory mandates. Experts agree that encryption is the most robust method for protecting sensitive data in transit to disaster recovery sites.

Key Benefits

Protect sensitive data in transit

Ensure data integrity, privacy, and maintain compliance with regulatory mandates

Eliminate Cost & Complexity

Proven Compliance through Layer 2 Encryption

Data Explosion Drives Need for WAN Encryption

Financial institutions, government agencies, and telecommunications companies transmit large volumes of sensitive data over high-speed Ethernet WANs that connect offices and data centers with disaster recovery sites. The consolidation of datacenters and rise of bandwidth intensive applications such as voice, video, virtualization, and cloud computing, and the consolidation of datacenters are causing exploding data volumes transmitted over ultra high-speed wide area networks. Because of its high overhead and other technical limitations, traditional router-based encryption often does not scale cost-efficiently to the levels of throughput required to protect data sent over such high-bandwidth networks.

Eliminate Cost & Complexity

SafeNet network encryption solutions provide easy to deploy protection for data transmitted to disaster recovery sites and offsite data storage facilities while preserving full network performance, RPO/RTO (recovery point objective/recovery time objective) objectives and service level agreements.
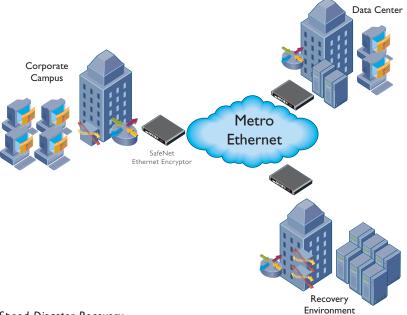
In the current economic environment, companies are looking to cut cost and complexity of compliance. Instead of purchasing costly bandwidth upgrades with high monthly recurring charges, companies deploy the Gigabit Ethernet encryptor in place of their legacy IPSec encryption and effectively double their available bandwidth in addition to the 10 fold latency improvement.

Through central policy management, SafeNet further eliminates cost. SafeNet's Network Security Management Center allows network administrators to centrally configure, monitor and manage network encryption policy from a single web-based console. It helps companies define granular security policies that can be distributed across multiple devices, thereby not only lowering policy management cost but also easily generating data security audit trails to meet compliance auditing requirements. SafeNet's purpose-built appliances easily integrate into existing networks in a matter of minutes. In contrast to traditional IPsec routers, there are no error-prone, complex routing tables to configure and maintain, thereby reducing maintenance cost and opportunities for misconfiguration. Once installed, SafeNet WAN encryptors require virtually no ongoing configuration and maintenance.

Proven Compliance through Layer 2 Encryption

An increasing number of legislative and industry mandates such as Sarbanes Oxley, PCI-DSS, State Privacy Laws and HIPAA require the protection of sensitive data in transit. By encrypting sensitive data at the network link layer (layer 2), companies ensure robust compliance with mandates because all data traversing the network is encrypted without exception, thereby dramatically reducing proof requirements and cost of compliance efforts.

Corporate Campus

Data Center

SafeNet Ethernet Encryptor

Metro Ethernet

Recovery Environment

High-Speed Disaster Recovery

Most Secure Layer 2 Encryption Solution

The SafeNet Ethernet Encryptor 10G provides a FIPS 140-2 Level 3 and Common Criteria EAL-4 certified network security solution that enables companies to utilize all available network bandwidth and eliminate complex administration. Designed to overcome the technological limitations of IPsec, the SafeNet Ethernet Encryptor moves sensitive data faster and more efficiently at network layer 2, thereby lowering the cost of network security and compliance.

Layer 2 network encryption is the superior, low latency solution to protecting data in transit over the WAN. Instead of costly bandwidth upgrades with high monthly recurring costs, companies deploy high-speed Ethernet Encryptors to immediately double encrypted bandwidth over IPsec.

Complete Portfolio of Encryptors

SafeNet's complete family of high-speed network encryptors for all network protocols provide the fastest and easiest way to integrate robust network security to protect mission-critical data for Enterprise and Government organizations. Multi-Gigabit throughput and lowest latency make SafeNet's encryptors the ideal solution for protecting massive amounts of data in motion, including time-sensitive voice and video streams. With solutions for ETHERNET, SONET, LINK, ATM, FRAME and IPsec encryption, SafeNet offers the world's only complete suite of high-speed WAN encryption for every topology, performance range and network design requirement.

Enterprise Data Protection

SafeNet Network Encryptors are a key component of SafeNet's comprehensive enterprise data protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet Enterprise Data Protection (EDP) is the only complete solution that secures data across the connected enterprise, from core to edge, with 360-degree protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/EDP

SafeNet
The Foundation of Information Security

www.safenet-inc.com