CIPHEROPTICS
Network security made simple

SOLUTION NOTE

Data replication over IP

Moving to IP

As organizations look for simple, affordable and effective technologies to ensure that they can replicate and back up their data, more and more are turning to IP-based storage networking. Many have found that they can restore their application processes and resume their normal business practices as quickly as possible— even in the face of a major catastrophe— at a much lower cost when using IP-based storage networking.

Fibre Channel systems have long been the standard for storage networking. There were many features that made Fibre Channel ideal for storage application requirements, including exact timing, support for jumbo packet size and reliability. The advent of Gigabit and 10-Gigabit Ethernet connections is leading the change to IP.

The move to high-speed Ethernet and IP, is appealing because of lower cost, higher bandwidth and the ability to house data centers and storage servers many miles away. In addition, governmental requirements such as SEC 34-47638 (which requires financial organizations to have their backup data center on a different electrical grid), are accelerating the move to IP-based storage networking.

Securing storage data in transit

The move to IP changes many aspects of your networking infrastructure, including data security. When data is at rest, there are myriad ways to protect it from intrusion, tampering or theft. However, in the IP-based reality of many storage networking systems, the vulnerability of data in transit must now be addressed. Once your data leaves the protected environs of the storage area network there are many hazards it can encounter as it makes its way to your backup location. To effectively implement a secure, compliant and cost-effective storage networking solution, you must first understand where your vulnerabilities lie.

CipherOptics IPSec appliances

- Protect data in transit over untrusted IP networks
- Provide full-duplex, wire-speed AES or 3DES IPSec encryption (100 Mbps and Gigabit)
- Introduce virtually no latency
- Integrate transparently into existing IP networks
- Have received FIPS 140-2 Level 2 validation

How are you vulnerable?

Copper and fiber optic cables are vulnerable to attack. While many carriers offer “private” networks, in reality, there are very few instances where an organization owns dedicated fiber, with no repeaters or other equipment connecting its remote data centers. Even dedicated fiber is not impervious to eavesdropping or other attack. Considering that your organization’s most important information assets are carried over a wide area network it makes sense to protect the data in transit.

Some specific threats include:

- Sniffing -- someone with inexpensive “sniffer” technology and the motivation to access your proprietary data can easily tap into your network lines, undetected, and siphon off anything traveling over the line.
- Insider access – an employee, contractor or vendor with access to the network can circumvent perimeter security to access your data. **It happens more than you might think – more than half of security breaches are committed by insiders.**

> “Storage security has been sorely overlooked. With the rapid release of new software and hardware and the progression of technology and processing power, the threat of further loss is imminent. We simply must equally integrate security throughout the infrastructure and should not depend so much on robust perimeter security, such as firewalls."
>
> John Cirillo, author of
> *Storage Security: Protecting, SANs, NAS and DAS*

Secure storage issues

In implementing a solution that secures your storage data while it's in transit between sites, there are several issues you need to consider.

IPSec: authentication, confidentiality and integrity

IP Security (IPSec) is a standard that protects data in transit over an untrusted network and provides three levels of security: confidentiality, authentication and integrity.

- **Confidentiality – Keep your data private**
  IPSec uses industry standard encryption algorithms (AES and 3DES) to keep data secret
- **Authentication – Trust your sources**
  Verify the identity of the peer IP gateway to verify the source of the data
- **Integrity—Trust your data**
  Once communication with a trusted source is established, IPSec prevents that data from being altered as it traverses the network.

To protect the data on your IP storage network, any solution must use IPSec to provide the highest level of security.

Latency

Data replication (especially via synchronous and semi-synchronous modes) requires minimal network latency and high bandwidth. With these sensitivities in mind, storage networking security solutions must not impact performance. If a data replication application is slowed or interrupted, it can result in lost packets or incomplete transfer. With high-speed (100/1000base T) networks, encrypting data in transit requires highly efficient encryption/decryption cycles to provide security without adding latency.

Jumbo frame support

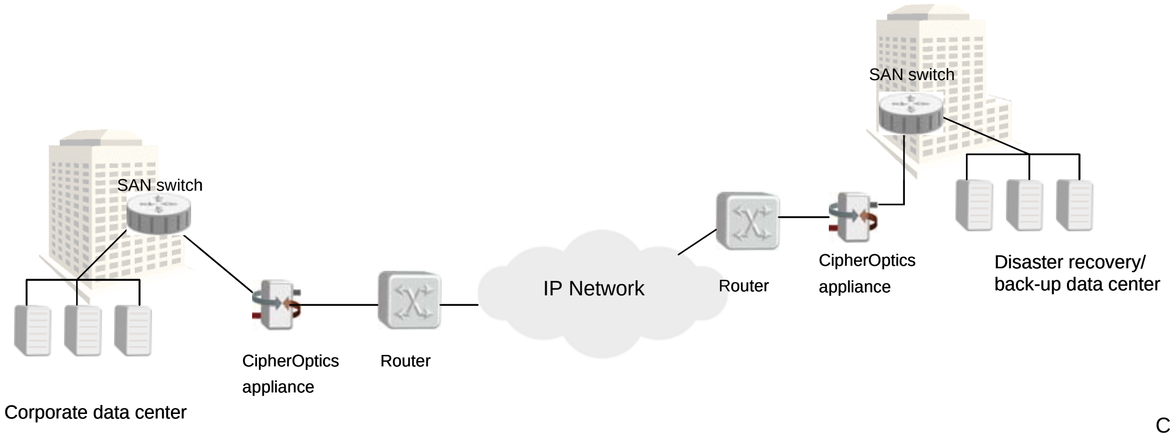
Jumbo frames are common in storage environments since most storage protocols utilize packet sizes greater than 1518 bytes. Any solution securing data in transit therefore must be able to accommodate these larger packet sizes.

The CipherOptics solution

CipherOptics network encryption appliances are uniquely suited to the demands of secure, IP-based storage networking. By having the lowest latency of any encryption solution, and providing IPSec-based data security, CipherOptics is leading the way for simple, yet robust, storage networking security.

CipherOptics network security appliances fit easily into existing IP storage networks, and can support FCIP and iSCSI. Their "bump-in-the-wire" implementation allows them to be added to the network just before the critical storage data leaves the data center. The CipherOptics encryption appliance is installed between the internal network and the WAN connection. One port is connected to the secure data center equipment, while the other port is connected to a wide area router or other devices in a non-secure network.

There are several solutions that provide encryption of data in transit, including multi-purpose devices (primarily a firewall or router with other functions) and VPN blades in multi-purpose chassis. While these provide encryption capabilities they have detrimental side-effects, most notably adding latency to applications and complexity to the network, and reducing network performance. A purpose-built appliance, like those from CipherOptics, however, takes a different approach and can perform these functions without adding complexity to the network or latency to the applications.



Secure IP storage networking

CipherOptics Inc.
701 Corporate Center Drive
Raleigh, NC 27607
T (919) 865-7330
F (919) 233-9751
www.cipheroptics.com