White Paper

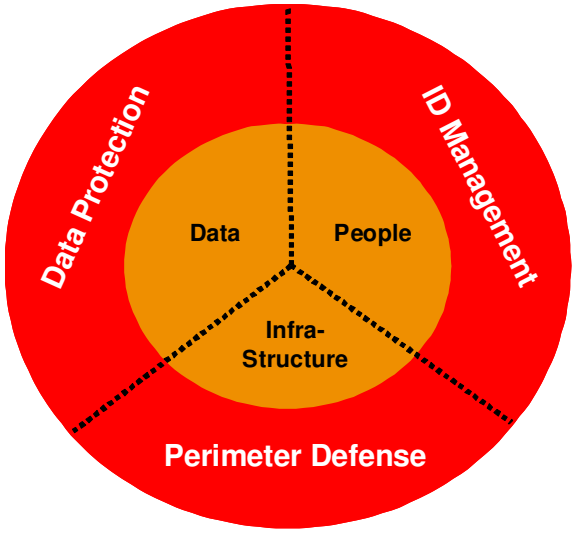
CIPHEROPTICS
Network security made simple

Best practices for protecting network data

Presented by CipherOptics Inc.
April 4, 2005

A company's value at risk

The biggest risk to network security is underestimating the threat to network security. Recent security breaches have proven that much of today's electronic data is not secure. Furthermore, as enterprises move to IP networks they are adding additional risk. The businesses that experienced these security breaches are not alone in their lack of a comprehensive security policy. Most organizations have implemented a porous security system that gives the illusion of security but does little to protect informational assets and intellectual property. There are three pillars that form the foundation for securing your most valuable company asset, data. Data protection, along with ID management and perimeter technologies, provide the three anchors that protect all aspects of the network: data and intellectual property, networking infrastructure and people. This paper will focus on data protection as a critical element of network security best practices.



Assessing risk

Assessing the risk comes down to some simple arithmetic: what is your data worth, and what would be the damage if it were compromised? After all, you have to know what data you have, know where it is, and assess the risks to it to be able to effectively protect it. It makes sense that organizations that deal with highly sensitive data and proprietary intellectual property – customer financial information, national security information, highly competitive product development information, patient medical records– should take a closer look at the areas of vulnerability on their network. A single breach on these networks can wreak havoc with long-term effects. Lawsuits from customers, fines for non-compliance to government regulations, degradation of an established brand—these consequences are very real, and often very difficult to overcome.

The truth of the matter is that current security technologies pose an unacceptable risk in protecting an organization's data and intellectual property. Today's firewall-based security technologies do not fully protect data resources. Only data protection throughout the network can safeguard critical and confidential data, regardless of the success or failure of other security technologies and policies. Therefore, data protection must be the primary layer of defense.

Data in motion: what's the worst that could happen?

Networks today are not the isolated, self-contained islands they once were. With Internet gateways giving network access to remote employees, customers, contractors and partners, the network has opened up, increasing productivity *and* security risks.

Network security has relied primarily on keeping the bad guys out. Hackers, thieves and other ne'er-do-wells seeking to do harm are prevented from getting in. Most of the time. However, the nature of networks today is dynamic. While data may spend some time on any number of devices – servers, desktops, disk arrays – some of it is in motion, traveling across the network, all the time. That data zipping around the network is the same data that is thoroughly protected while static. And it is more often than not completely unprotected while in motion.

Data residing on desktops, laptops and servers is usually protected with at least a password, if not more complex security. While always a good idea, it should not be enough to ensure a good night's sleep for IT security. After all, if data on the servers is important enough to be protected, what about when it travels the network? What happens if all else fails and the bad guys get in? Or, even more probable, what happens when the bad guy is *already in*? According to the *FBI 2004 Computer Crime and Security Survey*, more than 60% of security breaches are by insiders. So much for perimeter defense and ID management as a comprehensive network security strategy.

In the old days prior to all data being digital, the easiest way for someone to gather proprietary information was to insinuate himself into an organization and hang around the water cooler to catch up on what was going on, or to hang around the printer or fax, looking at documents (data) that may be proprietary, confidential or valuable. Nowadays, hanging on the network is the equivalent of hanging around the water cooler, only much more efficient. There are any number of tools available in the public domain that make it easy to pull data in transit off the network with no one ever knowing. And if you don't think you have anything valuable enough for someone to want, you may want to think again. There are any number of reasons your information may be an attractive target:

- Intellectual property – your organization's "special sauce" that gives you critical market differentiation and a leg up on the competition.
- Customer information – personal, financial and/or health information can be very valuable. In fact, protecting that information has spawned a growing number of federal and state regulations, including Gramm-Leach-Bliley, Sarbanes-Oxley and California Senate Bill 1386
- Employee information – personal information such as Social Security numbers, bank account numbers and health information
- Other secret information – including governmental information regarding homeland or national security, Department of Defense activities or communications, and personal, private data used by any number of agencies
- Business-enabling information – customer and prospect opportunities, plans and interactions

All networks are untrusted

Most enterprises and organizations with far-flung offices, remote back-up data centers and multiple buildings in a campus setting have a complex network to meet all of their communication and business needs. In fact, more than a single network, it is usually a network of networks that must communicate and share data with one another. This creates a situation where data is physically leaving a protected facility and moving to another. Whether it's going over the Internet, a service provider backbone or a wireless link between buildings, that data, which has been protected while at rest on servers, has moved out to where it is available to anyone with the motivation and means to get it.

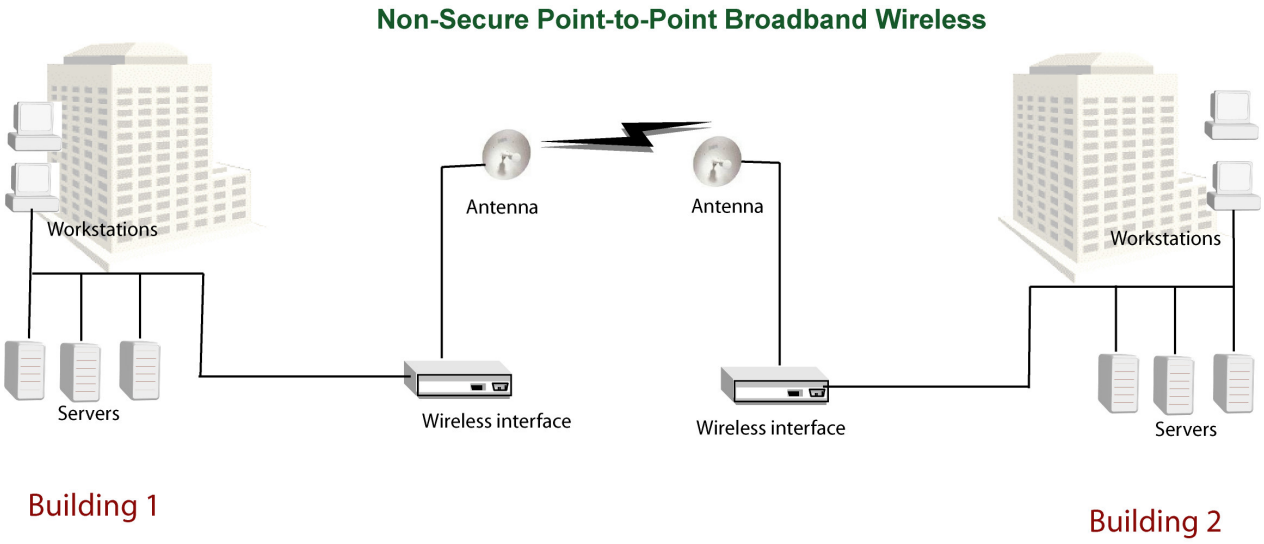
The Internet is understood to be untrusted. Special precautions are taken when opening up a gateway to the Internet, including firewalls, intrusion detection and virus protection. However, a wide range of networks – in fact all networks – should be untrusted, and treated as such. Go back to the fundamentals of risk assessment and you'll see that the more sensitive the data, the more untrusted the network – any network.

All networks have vulnerabilities that can put data at risk. Wireless, MPLS, and storage IP networking are just a few examples of common networks where data in transit is susceptible to unauthorized access.

Example 1

Broadband wireless link between buildings

Many organizations have multiple networks in different facilities that must exchange information. When fiber is impossible or too cost-prohibitive, high-speed wireless provides an inexpensive and easy solution. However, all data transmitted over the air through the wireless links is at risk to anyone wanting to access it.

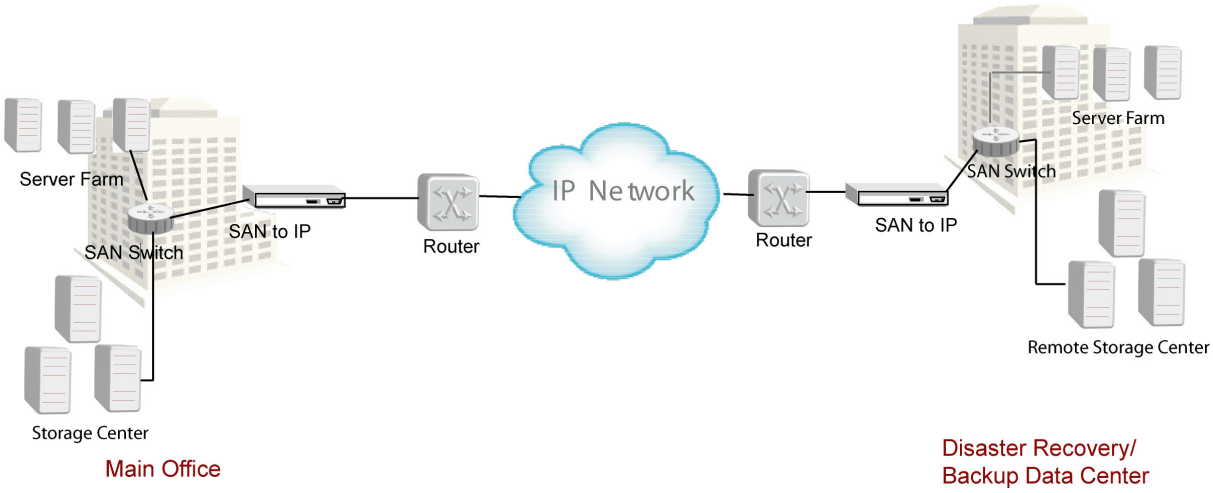


Example 2

Storage IP Networking

It is becoming increasingly common for organizations to store and archive their data in a remote facility. Once again, however, this data must travel over untrusted networks to reach its destination, meaning it could be accessed without anyone knowing it.

Non-Secure Data Replication over IP

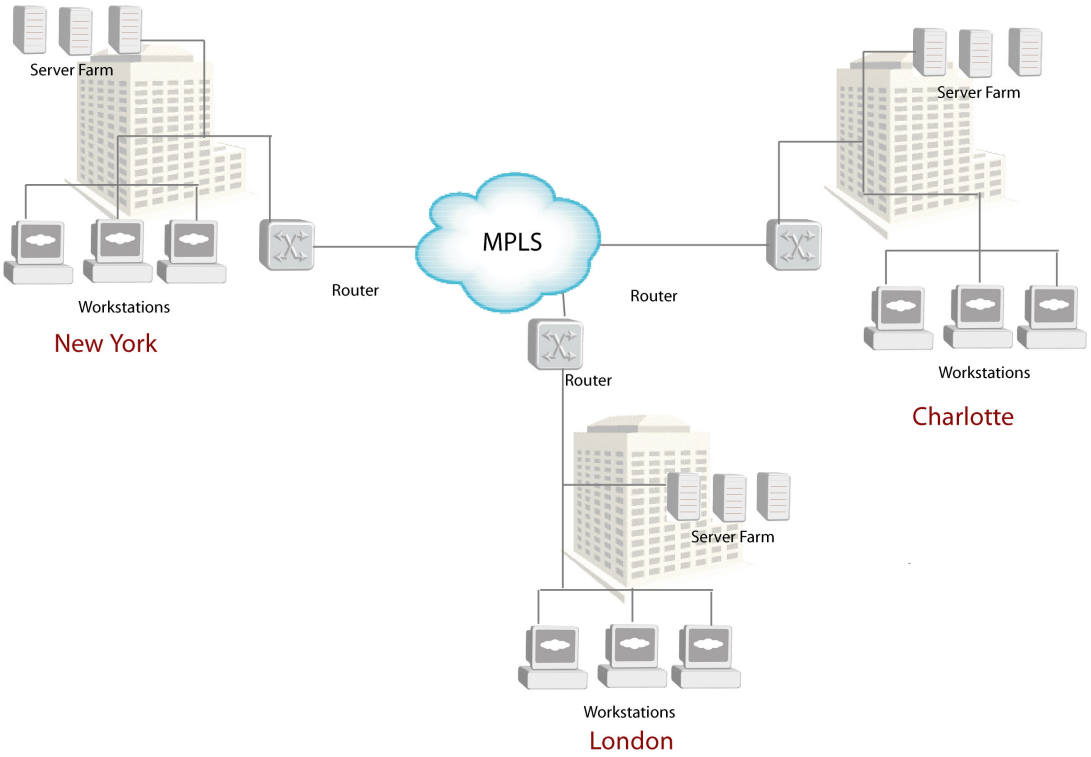


Example 3

MPLS

MPLS (multi-protocol label switching) networks are becoming more and more popular as service providers look for ways to enable multiple customers to have VPNs on the same network. However, the VPNs on the MPLS network simply separate user groups, they don't protect the data

Non-Secure MPLS Network



Data protection – best practice for network security

Understanding that data in transit is vulnerable both on and off the network begs the question of how to protect it. Your data is running around the network in packets that contain addresses, protocol ids, and the actual data. If you protect the packet from its source to its destination you have created an excellent foundation for a secure network.

There are three main aspects of data protection on the network:

- Confidentiality – Keep your data private
- Authentication – Trust your sources
- Integrity—Trust your data

IP Security (IPSec), defined by the Internet Engineering Task Force (IETF), is the accepted standard for protecting data in transit over an untrusted network and provides the three levels of security. IPSec is a suite of security protocols that protects IP packets. IPSec is implemented by defining security policies that answer these questions:

- What traffic do you want to protect?
- How do you want to protect it?
- What are the endpoints?

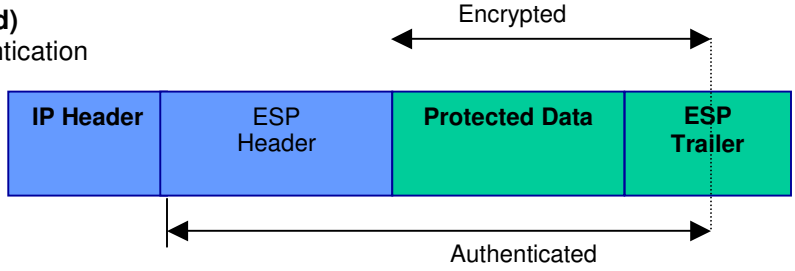
IPSec works on Layer 3, the network layer of the Open Systems Interconnection 7-layer networking model. By running on Layer 3, IPSec is able to function transparently to higher layer applications; the applications do not require any knowledge of IPSec in order to use it. Combined with Internet Key Exchange (IKE), IPSec users can exchange keys, authenticate one another, and securely tunnel encrypted data between peers. By enabling IPSec everywhere on the network that sensitive data travels, the vulnerability of data traveling in the clear is eliminated.

IPSec modes of protection
IPSec protects IP packets by defining which traffic is to be protected, what protection the traffic will use and which network host or gateway will receive the traffic. IPSec uses a protocol called Encapsulating Security Payload (ESP) that provides proof of data integrity, data source authentication and anti-replay by inserting a new IP address and ESP header in front of the packet to be protected. This protects the entire IP packet including the originating IP address. Using ESP controls both the encryption and authentication used to protect the IP payload.

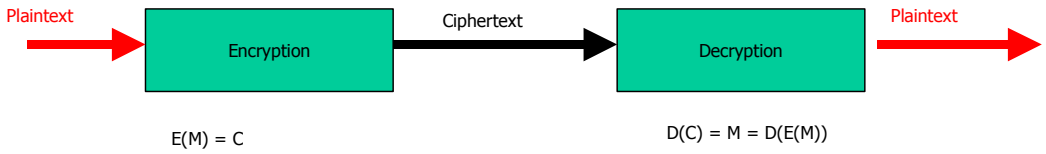
Tunnel mode

ESP (encapsulating security payload)

- Data integrity + authentication
- Anti-replay service
- Confidentiality



IPSec encryption
IPSec encryption enables confidentiality of data as it travels on the network.



- Uses symmetric keys (same keys are used for encryption and decryption)
- Uses Diffie-Hellman algorithms and IKE/ISAKMP protocols to derive keys
- Encryption algorithms such as AES

AES (Advanced Encryption Standard) was issued as FIPS Publication 197 by NIST (National Institute of Standards and Technology). AES supports key sizes up to 256 bits, in contrast to 56-bit keys offered by earlier algorithms. The higher the number of bits, the more complex the key, and the more secure the data.

IPSec packet authentication and integrity
Packet authentication is a critical part of data protection. With IPSec, packet authentication provides proof of identity – who's on the other end of a channel. It also ensures message integrity by providing the source of the message and proving the message has not been altered though a digital signature, or message authentication code (MAC). Authentication is applied to all bytes in the header and payload, and the algorithm specifies the length of the authentication data. The process is: encrypt first, then authenticate.

Internet Key Exchange (IKE)
IKE is used to ensure security for virtual private network negotiation and remote host or network access. IKE defines an automatic means of negotiation and authentication for IPSec security associations (SA). Security associations are security policies defined for communication between two or more entities—the relationship between the entities is represented by a key. The IKE protocol ensures security for SA communication without the pre-configuration that would otherwise be required.

CipherOptics enables IPSec everywhere

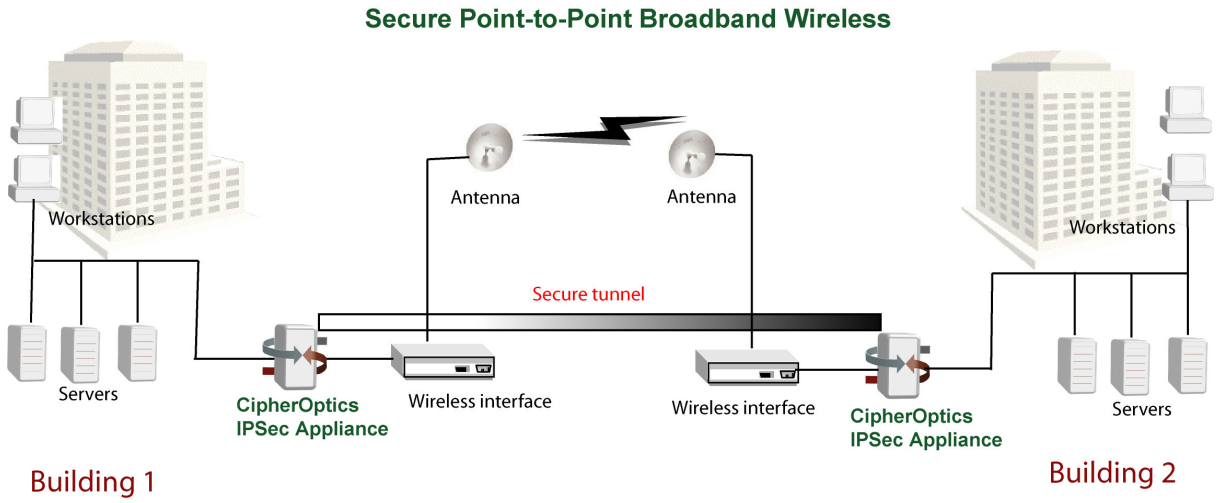
There are several ways to enable IPSec on the network. The CipherOptics approach is to use purpose-built appliances designed for Fast Ethernet and Gigabit Ethernet IP networks. With its proprietary TILEA™ architecture, CipherOptics appliances are paving the way for IPSec everywhere.

TILEA encryption architecture

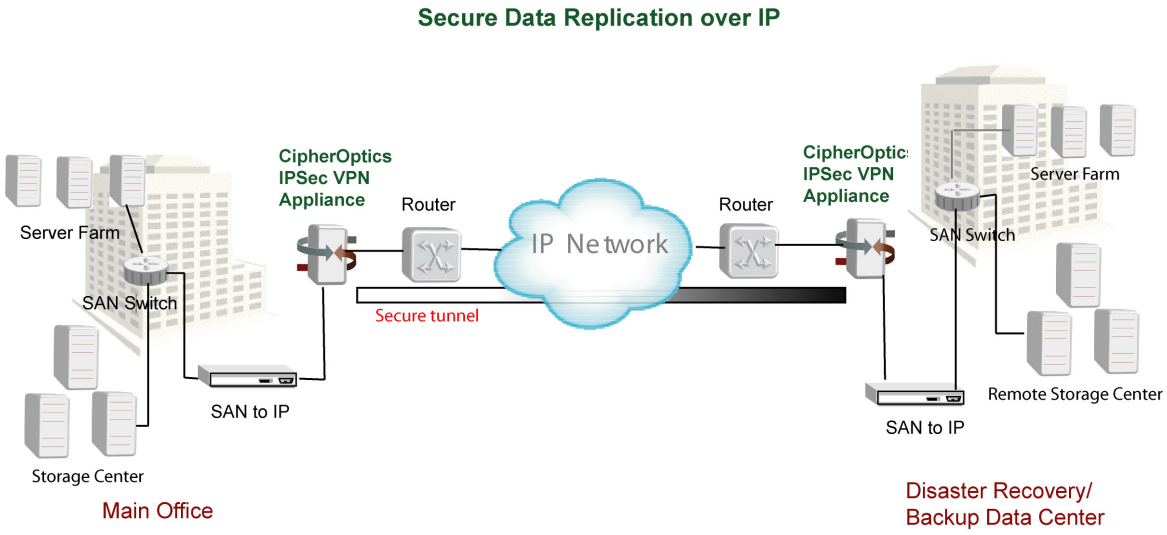
TILEA (Transparent In-Line Encryption Architecture) uniquely solves the problems of latency and throughput that hamper other IPSec solutions, including VPN blades and firewall extensions. TILEA follows the IPSec standard, is FIPS 140-2 Level 2 validated and is interoperable with other IPSec solutions. Its performance is based on its unique, fast policy-look-up-engine, which makes its encryption and decryption cycles in the micro-second range, exponentially faster than any other IPSec solution at 100 Mbps and above. This means that there is no effect on network performance with 1.9 Gbps full-duplex throughput and virtually no latency on the applications. TILEA also enables CipherOptics' IPSec appliances to have "bump-in-the-wire" implementation; it quickly and easily integrates into existing IP networks without adding any complexity.

To show how CipherOptics IPSec appliances provide data protection, let's re-visit the vulnerable networks previously.

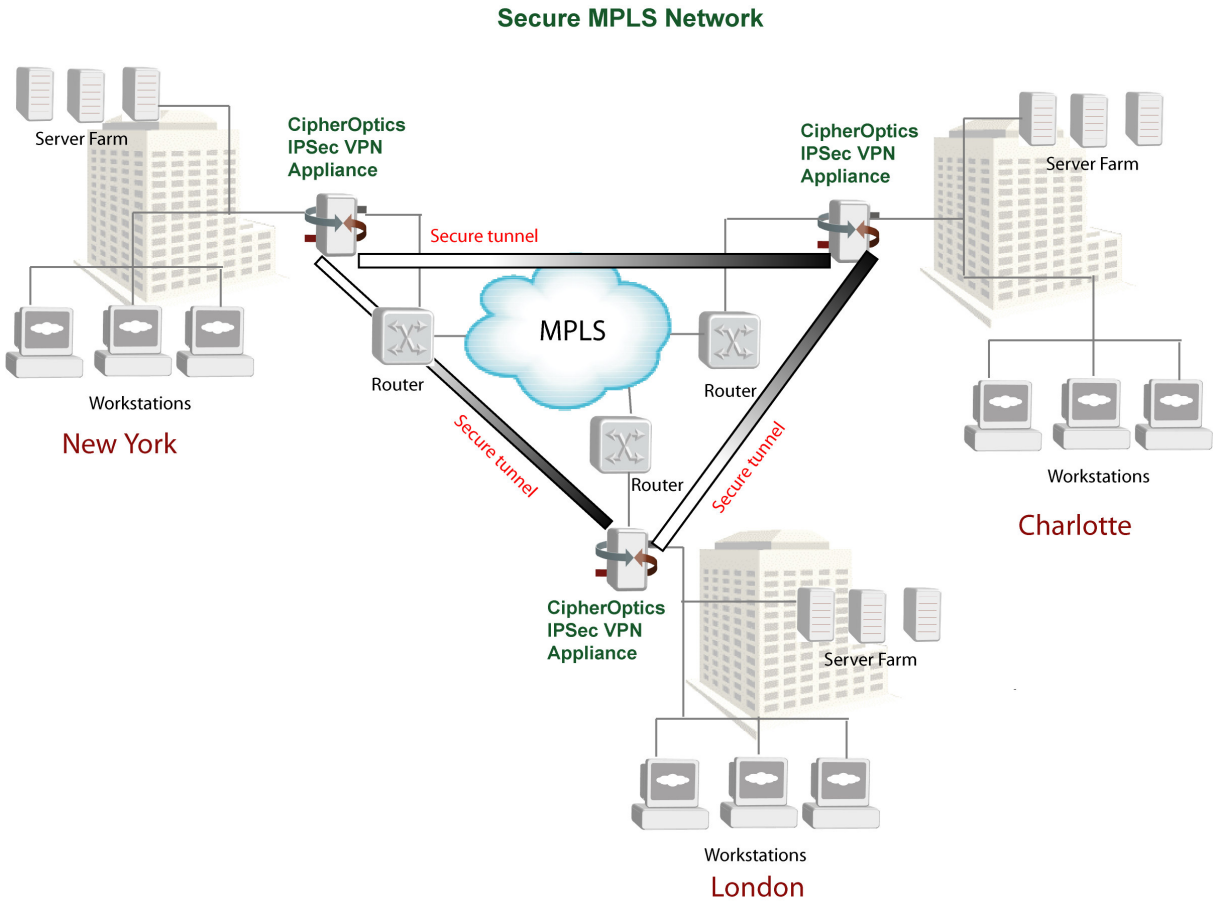
High-speed broadband wireless network



Storage IP Networking



MPLS



About CipherOptics

CipherOptics, the leading innovator of gigabit-speed IPSec appliances, protects data in transit as it travels over IP networks. With easy installation, virtually no latency and robust AES encryption capabilities, CipherOptics appliances outperform router and firewall add-on solutions in price, performance and network transparency.

The CipherOptics family of IPSec appliances is field-proven in some of the most security sensitive networks in the world, and has received FIPS-140-2 Level 2 validation. We enable government agencies, financial institutions and global enterprises to secure all data communications while maximizing broadband network capacities at a very affordable cost.

CipherOptics
Corporate Headquarters
701 Corporate Center Drive
Raleigh, NC 27607
(919) 865-3300 phone
(919) 865-9751 fax
www.cipheroptics.com