CIPHEROPTICS
Network security made simple

SOLUTION NOTE

Securing Broadband Wireless

Moving to broadband wireless

Many organizations that rely on high-speed IP/Ethernet data communications have adopted broadband wireless as a solution to their increasing need for bandwidth capacity and reduced networking costs. The need for high-speed networking has been driven by the growth in high-bandwidth applications, such as voice-over-IP, IP storage networking and video conferencing. It has been relatively easy for organizations to send data over high-speed fiber optics networks, but more difficult to maintain that speed from the network hub to the user. By effectively addressing the “last mile” problem, high-capacity broadband wireless enables buildings and campuses to be connected at high speed without the high cost of installing/leasing and maintaining optical fiber for each location.

Securing wireless data in transit

The move to wireless changes many aspects of your networking infrastructure, including data security. Point-to-point wireless can be implemented using licensed or unlicensed frequency bands or line-of-sight optical technology. However, the “air” that wireless network data travels through is not secure. The insecure airspace expands geometrically beyond the wireless radio dishes to anywhere the wireless signal can be intercepted. This extra space for unauthorized interception leads to a significant additional risk placed upon network and security managers managing wireless wide-area networks. To effectively implement a secure and cost-effective broadband wireless solution, you must first understand where your vulnerabilities lie.

How are you vulnerable?

In wireless transmissions, there is no sophisticated standard to enforce the overall protection of the headers and payload while the data is in transit. Additionally, the architecture of wireless networks influences the probability of theft. Since the size of the spectrum varies dependent on distance and location, transmission paths are vulnerable to unauthorized individuals with sensitive monitoring equipment designed to intercept the data.

CipherOptics IPSec Appliances

- Protect data in transit
- Provide full-duplex, wire-speed AES or 3DES IPSec encryption (100 Mbps and Gigabit)
- Introduce virtually no latency
- Simple, transparent implementation
- Provide data confidentiality, integrity & authentication
- FIPS 140-2 Level 2 validated

In point-to-point wireless data transmissions, this virtual communication link is inherently un-secure unless that data stream is encrypted. 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.**

Department of Defense Directive 8100.2

Released in April of 2004, DoD 8100.2 establishes the policy under which commercial wireless devices can be used on the department’s networks. Many of the requirements outlined in 8100.2 relate directly to the security of wireless networks.

Authentication
Section 4.1.1 requires identification and authentication be provided at both the device and network level

Encryption
Section 4.1.2 states that encryption is required when data is transmitted over the wireless network. Section 4.1.2.2 specifies that a FIPS-validated encryption module must be used.

CipherOptics’ IPSec appliances are FIPS validated and provide the authentication and encryption as specified in DoD 8100.2

Secure broadband wireless issues

In implementing a solution that secures your broadband wireless links, 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 government 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 broadband wireless network, any solution must use IPSec to provide the highest level of security.

Latency

Many applications, including voice-over-IP, data replication over IP and video conferencing require minimal network latency and high bandwidth, and are often running over broadband wireless networks. With these sensitivities in mind, security solutions must not impact performance. If a data replication application is slowed or interrupted, it can result in lost packets, incomplete transfer or garbled video or voice. With high-speed (100/1000 base T) wireless networks, encrypting data in transit requires highly efficient encryption/decryption cycles to provide security without adding latency.

Wire-speed throughput – maximizing bandwidth

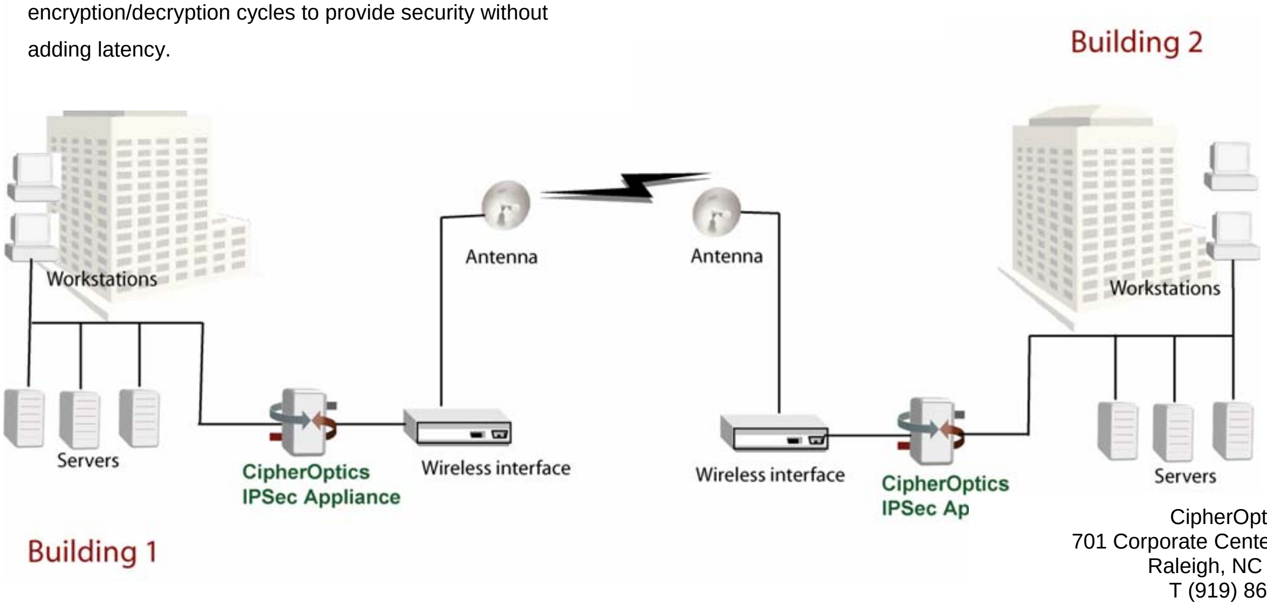
Because so many of the applications running on wireless networks are bandwidth-intensive, any solution used to secure the network must not cause processing bottlenecks, slowing down the network. CipherOptics' TILEA™ architecture features the fastest encryption/decryption cycle available, enabling full-duplex gigabit wire-speed encryption.

The CipherOptics solution

CipherOptics IPSec appliances are uniquely suited to the demands of secure, broadband wireless 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, wireless security.

CipherOptics IPSec appliances fit easily into existing networks, supporting any IP-based protocol. Their "bump-in-the-wire" implementation allows them to be added to the network just before the data leaves to be transmitted over frequency bands. The CipherOptics IPSec appliance is installed between the internal network and the wireless interface connection. .

There are several solutions that provide encryption of data in transit, including multi-purpose devices (primarily a firewall with other functions) and VPN blades as add-ons to routers. While these provide encryption capabilities they have detrimental side-effects, most notably adding latency to applications 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.



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