

## Integrated site-to-site AES 256 encryption over HN/HX networks

The optional Hughes IPsec Encryption (Hughes IPsec) feature is the perfect solution for customers looking for true site-to-site encryption. Hughes IPsec is integrated with Hughes' TCP acceleration technology to overcome the inherent performance penalty that IPsec VPNs typically cause standard satellite solutions. Hughes IPsec uses a 256-bit AES encryption to offer true bidirectional site-to-site encryption over HN/HX Systems.

### Hughes IPsec incorporates the following features:

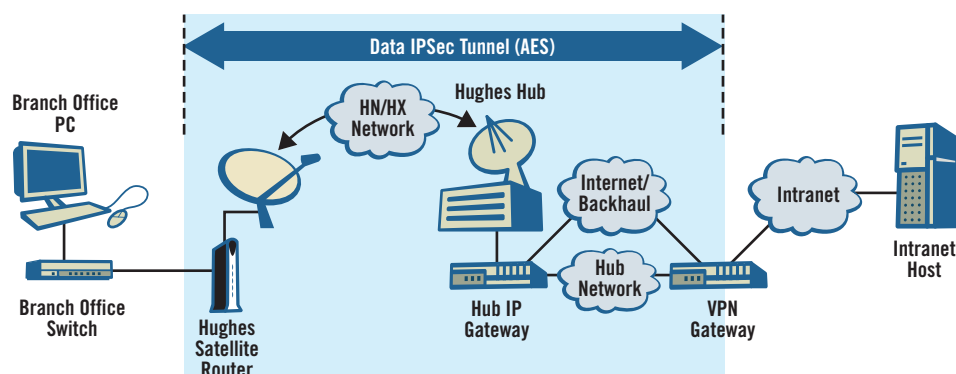
- True site-to-site encryption—from customer data center to remote site
- 256-bit bidirectional AES encryption
- Hughes' industry-leading acceleration technology, advanced routing, and prioritization features on the encrypted traffic
- Server redundancy
- Split-tunnel mode
- Data center diversity

The Hughes IPsec feature provides a standards-based IPsec/IKE implementation for encrypting user data traffic and managing encryption keys in HN/HX networks. IKE (Internet Key Exchange)

protocol is used to automatically generate and maintain session keys and to set up an IPsec tunnel between the HN/HX remote terminal and the VPN IP gateway in the customer's data center. This ensures that the data is encrypted end-to-end between the customer's remote site and the data center.

The Hughes IPsec provides true site-to-site encryption with no unencrypted portions en route, while still being able to use Hughes' patented Performance Enhancing Proxy (PEP) for TCP acceleration, as well as all other routing, prioritization, and access control functions provided within HN/HX Systems. Hughes IPsec's strong software integration within the HN/HX Systems minimizes the throughput degradation associated with the IPsec implementation. The following diagram shows a typical HN/HX network with Hughes IPsec enabled. The Hughes IPsec implementation requires the installation of a redundant pair of VPN IP gateways at the customer's data center. The VPN IP gateway implements the IPsec tunnels and also performs the TCP acceleration functions while the Hughes hub IP gateway performs the routing and prioritization of the IPsec packets.

The HN IPsec implementation requires the installation of a redundant pair of VPN IP gateways at the customer's data center. The VPN IP gateway implements the IPsec tunnels and also performs the TCP acceleration functions while the Hughes hub IP gateway performs the routing and prioritization of the IPsec packets.



Hughes Network Systems, LLC (Hughes) is the world's leading provider of satellite broadband for home and office, delivering innovative network technologies, managed services, and solutions for enterprises and governments globally. HughesNet® is the #1 high-speed satellite Internet service in the marketplace, with offerings to suit every budget. To date, Hughes has shipped more than 2.5 million systems to customers in over 100 countries, representing over 50 percent market share. Its products employ global standards approved by the TIA, ETSI, and ITU organizations, including IPoS/DVB-S2, RSM-A, and GMR-1. Headquartered outside Washington, D.C., in Germantown, Maryland, USA, Hughes operates sales and support offices worldwide, and is a wholly owned subsidiary of EchoStar Corporation (NASDAQ: SATS), a premier global provider of satellite operations and digital TV solutions. For additional information about Hughes, please visit [www.hughes.com](http://www.hughes.com).

Hughes IPsec additionally supports data center diversity where a second pair of VPN IP gateways may be placed in an “alternate” physically diverse data center. Two VPN routers (not shown in the previous diagram) provide a management IPsec tunnel over the backhaul over which the VPN IP gateway’s management traffic is carried.

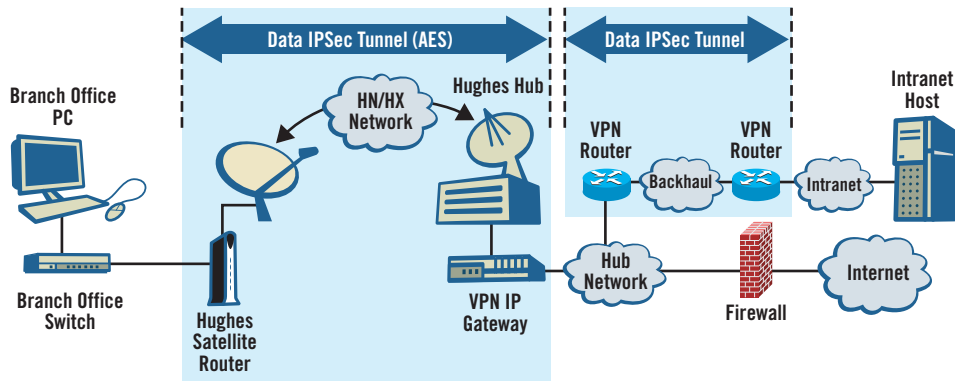
HN IPsec can also be implemented in a split-tunnel mode where the hub IP gateway performs the function of the VPN IP gateway as well. This configuration, as shown, may be useful to customers who need to selectively route their traffic to either the Internet or their own data center. Traffic destined for the data center is sent over a second IPsec tunnel between the Hughes hub and the data center.

Implementation of the Hughes IPsec solution in an existing HN or HX network is very simple and involves installation of the VPN IP gateways and upgrading the software versions of some of the HN/HX System components. The Hughes IPsec solution is supported on the HN7000S series/HN9200/HN9400 and HX series of remote satellite routers. The Hughes IPsec module provides detailed statistics for monitoring and troubleshooting IPsec tunnels.

Every HN/HX System comes standard with DES encryption on the outroute carrier. However, the optional Hughes IPsec feature is an elegant solution for customers looking to implement standards-based, site-to-site encryption over their HN/HX network without losing the advanced TCP acceleration features.

## Key Benefits of Hughes IPsec

- True site-to-site encryption from customer data center to remote location
- TCP acceleration on encrypted traffic
- Secure 256-bit AES encryption
- Redundant implementation
- Data center diversity support



For additional information, please contact Hughes at [globalsales@hughes.com](mailto:globalsales@hughes.com) or visit [www.hughes.com](http://www.hughes.com).