

Integrated site-to-site encryption over the HN network

The optional Hughes IPSec Encryption (HN IPSec) feature is the perfect solution for customers looking for true site-to-site encryption. HN IPSec is integrated with Hughes' TCP acceleration technology to overcome the inherent performance penalty that IPSec VPNs typically cause standard satellite solutions. HN IPSec uses a 128-bit AES encryption to offer true bidirectional site-to-site encryption over the HN network.

HN IPSec incorporates the following features:

- True site-to-site encryption—from customer data center to remote site
- 128-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

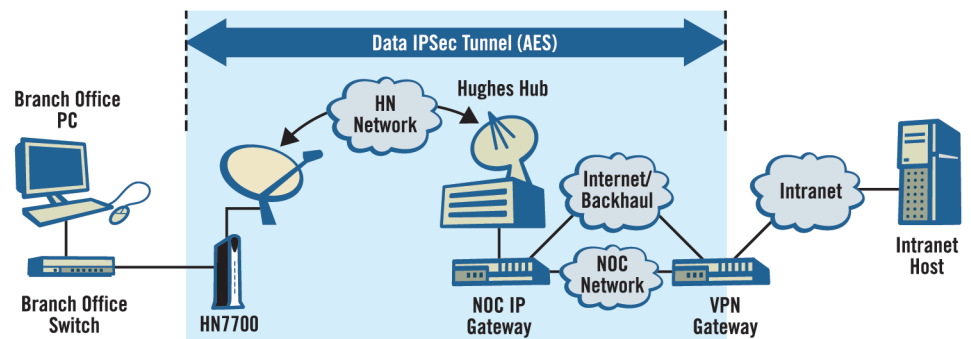
ensures that the data is encrypted end-to-end between the customer's remote site and the data center.

The HN 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 a HN system. HN IPSec's strong software integration within the HN system minimizes the throughput degradation associated with the IPSec implementation.

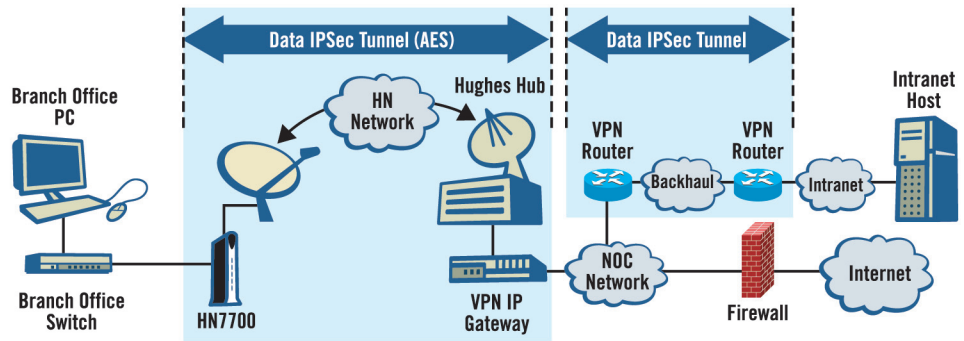
The following diagram shows a HN network with HN IPSec enabled.

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 NOC (Network Operations Center) IP gateway performs the routing and prioritization of the IPSec packets.

The HN IPSec feature provides a standards-based IPSec/IKE implementation for encrypting user data traffic and managing encryption keys in a HN network. IKE (Internet Key Exchange) protocol is used to automatically generate and maintain 128-bit session keys and to set up an IPSec tunnel between the HN remote terminal and the VPN IP gateway in the customer's data center. This



HN 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 NOC 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 NOC and the data center.

Implementation of the HN IPSec solution in an existing HN network is very simple and involves installation of the VPN IP gateways and upgrading the software versions of some of the HN system components. The HN IPSec

solution is supported only on the HN7000 series of remote terminals. The HN IPSec module provides detailed statistics for monitoring and troubleshooting IPSec tunnels.

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

Key Benefits of HN IPSec

- True site-to-site encryption from customer data center to remote location
- TCP acceleration on encrypted traffic
- Secure 128-bit AES encryption
- Redundant implementation
- Data center diversity support

For additional information, please contact us at globalsales@hns.com