Making the Gigabit IPsec VPN Architecture Secure

Robert Friend

Computer 37:6, pp 54-60, IEEE 2004

Presented By
Mike Cochrane

Definitions

- Virtual Private Network (VPN)

  “Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.”

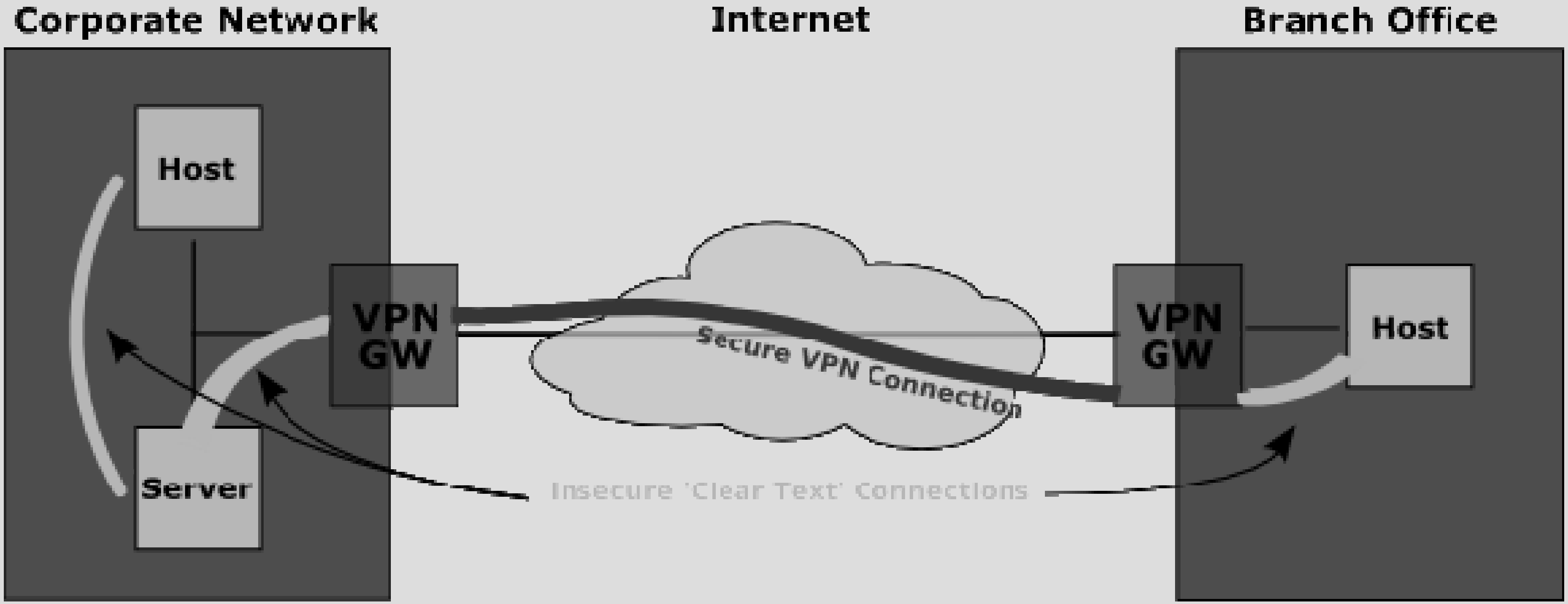
- IP Security (IPSec)

  “... A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer...”

Source: Cisco Internetworking Terms and Acronyms http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

VPN Usage

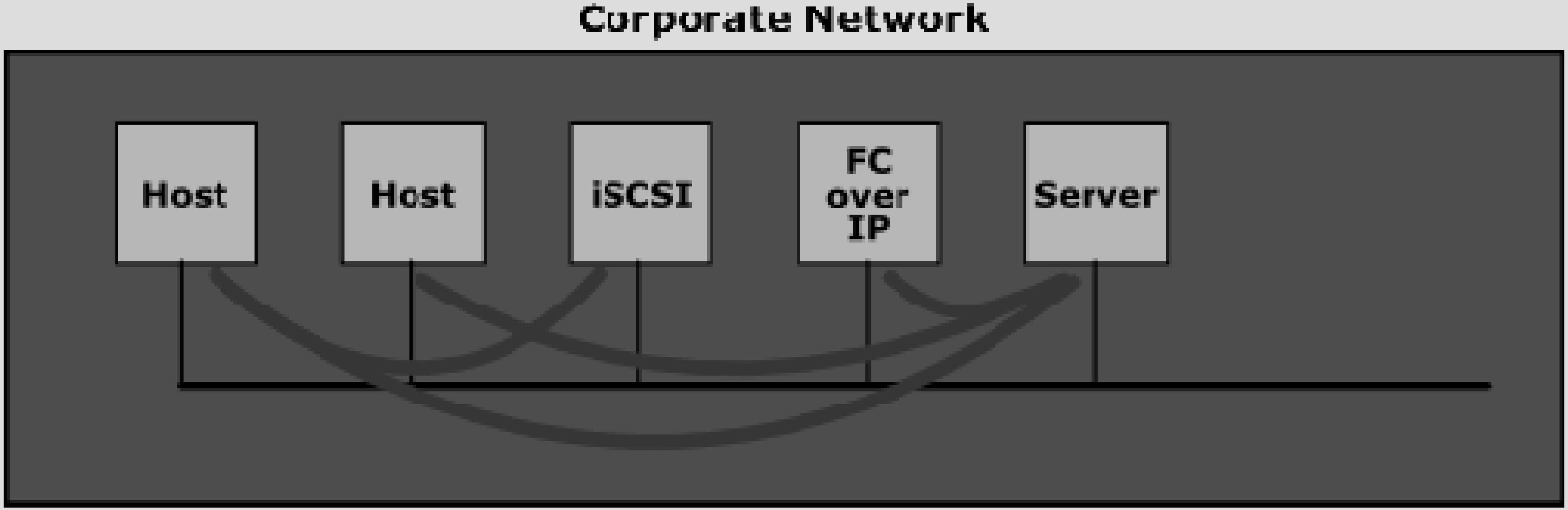
Extranet VPN



- **VPN Gateways between sites**
- **Unencrypted Data on the local network**

VPN Usage

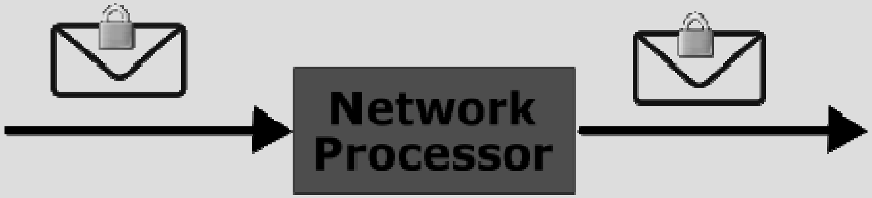
Intranet VPN



- VPN Connections between nodes
- All nodes have VPN capabilities
- All data is encrypted

VPN Implementation

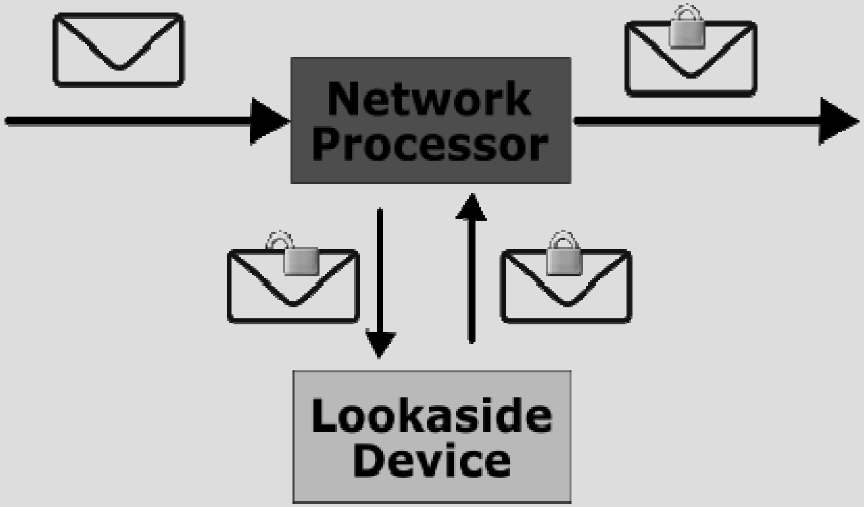
- Software



  - **VPN implemented in software on the host.**
  - **All IPSec and encryption functions performed before being sent to the network processor.**
  - **High processing load on host.**
  - **~11GHz Pentium CPU required for full-duplex Gigabit channel.**
  - **No special hardware required.**

VPN Implementation

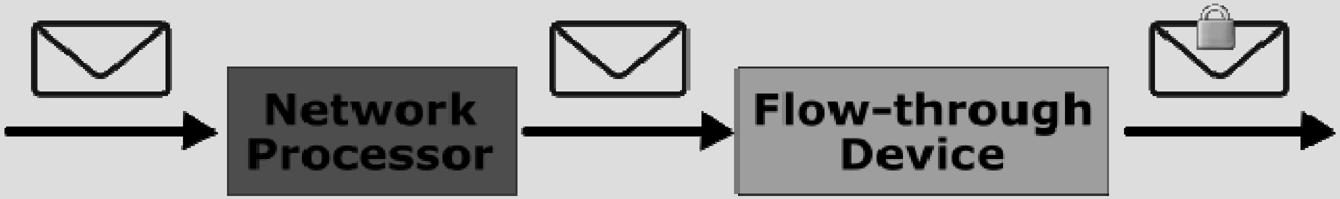
- Lookaside Architecture



  - Host sends 'clear text' packets to network processor.
  - Some IPSec functions performed by network processor.
  - Lookaside Device does compute-intensive processes.
  - Requires significant redesign of network processor to add lookaside communication bus.
  - Network Device manufacturer supports IPSec firmware.

VPN Implementation

- Flow-Through Architecture



  - Host sends 'clear text' packets to Network processor.
  - Network processor sends 'clear text' packets to flow-though device.
  - Flow-Through device does all IPSec VPN functions.
  - Requires minimal redesign of network processor to add VPN support.
  - Simply connects to output of Network processor before the packets leaves the system.
  - IPSec firmware maintained by Flow-through device manufacturer.

Critical Comment

- Performance Analysis
  - The author has had some assumptions in this section but has not clearly stated what they were.
    - What IPSec features were selected.
    - What protocols are being used to implement these features.
  - How the price for the Flow-Through implementation was arrived at. The author suggests that these are not currently available but gives a cost for their use.
  - The author lists three compute-intensive functions, Compress, Encrypt and Authenticate. The performance analysis neglects the compress function.

Discussion Question

- Is IPSec the most appropriate protocol for Intranet secure communications?