725 Software Security

Oral presentation

11.10.04

Christian H. Mosveen

Paper

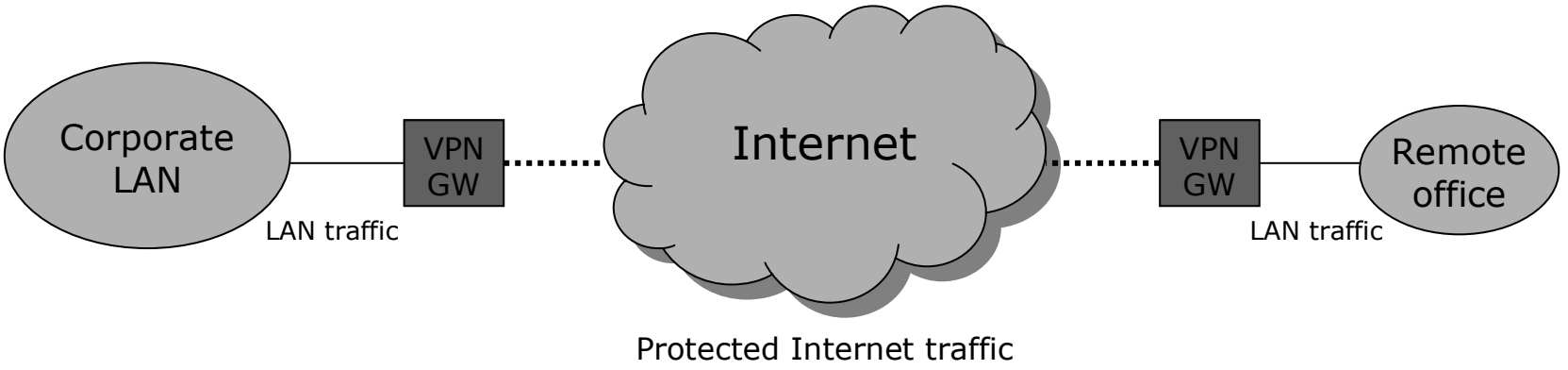
Making the Gigabit IPsec VPN Architecture Secure

Robert Friend

Computer 37:6, p. 54-60, IEEE
2004

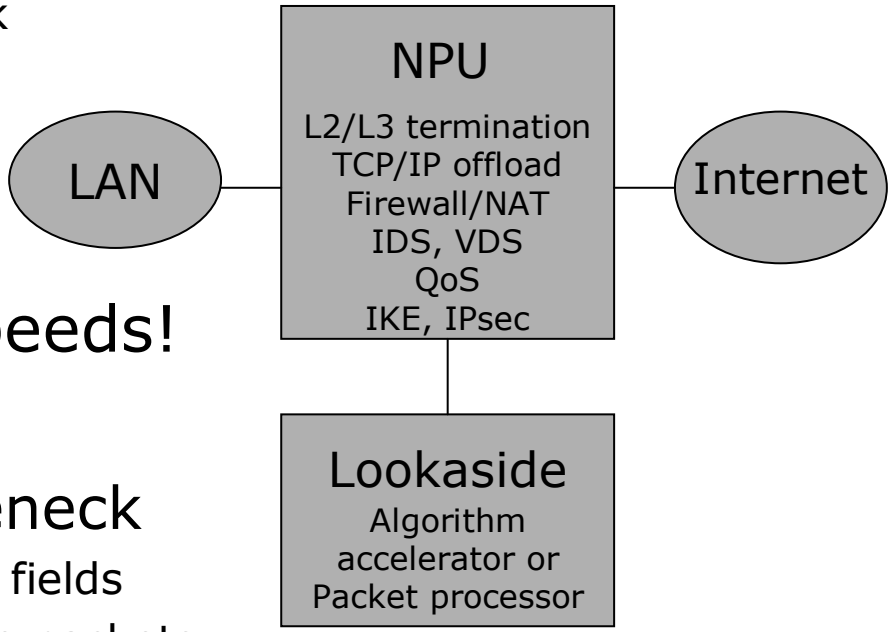
Appreciative point

- Virtual Private Networks, summed up
  - ”A traditional site-to-site VPN is a static connection that securely extends the corporate LAN across the untrusted Internet to the remote office, where both end points consist of corporate VPN gateways. The VPN gateways decapsulate protected Internet traffic and present it to the local network as LAN traffic. Thus, the remote office appears to be part of the corporate network.”



Present architecture

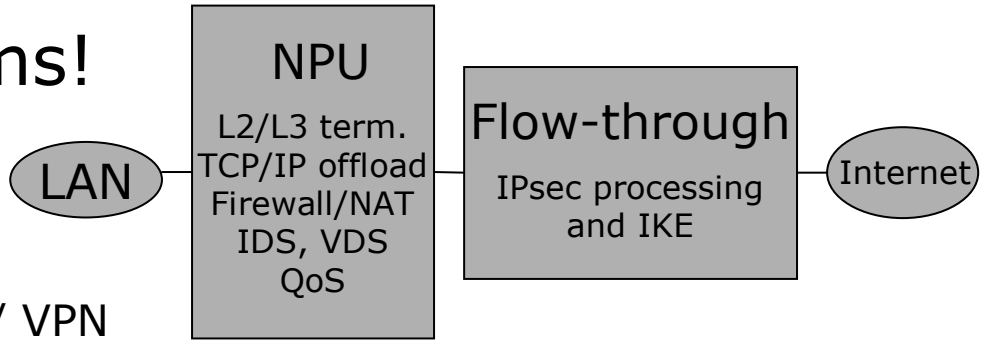
- Software
  - Software is slow -> Bottleneck
- Lookaside
- Will struggle at Gbit speeds!
- Because:
  - VPN becomes a bottleneck
    - General: NPU reads a few fields
    - VPN: NPU processes entire packets
  - NPU has limited bandwidth
    - Traffic travels across its bus twice



Proposed architecture

- Flow-through

- Solves the problems!
- Because:
  - Separation
    - Specialized: General / VPN
  - Linear data path
    - Traffic travels at line speeds



Cost comparison

Table 1. Processing costs of adding IP security measures.

Processor	Cryptography (AES/SHA-1)	IPsec protocol and packet processing	IKE protocol and public-key processing	Total Pentium bandwidth	Pentium cost*	Multigigabit security processor cost	Total VPN cost
Software only	7.6 GHz	1 GHz	2.5 GHz	11.1 GHz	$851	$0	$851
Lookaside	0.0 GHz	1 GHz	0.1 GHz	1.1 GHz	$84	$150	$234
Flow-through	0.0 GHz	0 GHz	0.0 GHz	0.0 GHz	$0	$100	$100

- Appreciative point
  - Table provides conclusive argument
- Critical point
  - The numbers are not well explained

Question

- Can you think of any disadvantages with the flow-through approach, or any alternatives in which the lookaside approach would be better suited?