IPSec
Hardware Resource Requirements Evaluation

.

Alberto Ferrante and Vincenzo Piuri

DTI, University of Milan

{ferrante, piuri}@dti.unimi.it

Jeff Owen

AST, ST Microelectronics

jefferson.owen@st.com

Presentation Outline

1. IPSec;
2. Testbed Network
   and Description of Tests;
3. Performance Results;
4. Considerations on Performance;
5. Conclusions and Future Work.

IPSec

- Is a suite of protocols
  - adding security at IP (network) level;
- makes extensive use of cryptographic functions;
- it is included as security mechanism in IPv6.

AH, ESP

- Is mainly composed of two protocols:
  - Authentication Header (AH);
  - Encapsulating Security Payload (ESP);
- both protocols can be used in:
  - transport mode;
  - tunnel mode;
- Addictional protocol:
  - IP Compression (IPComp).

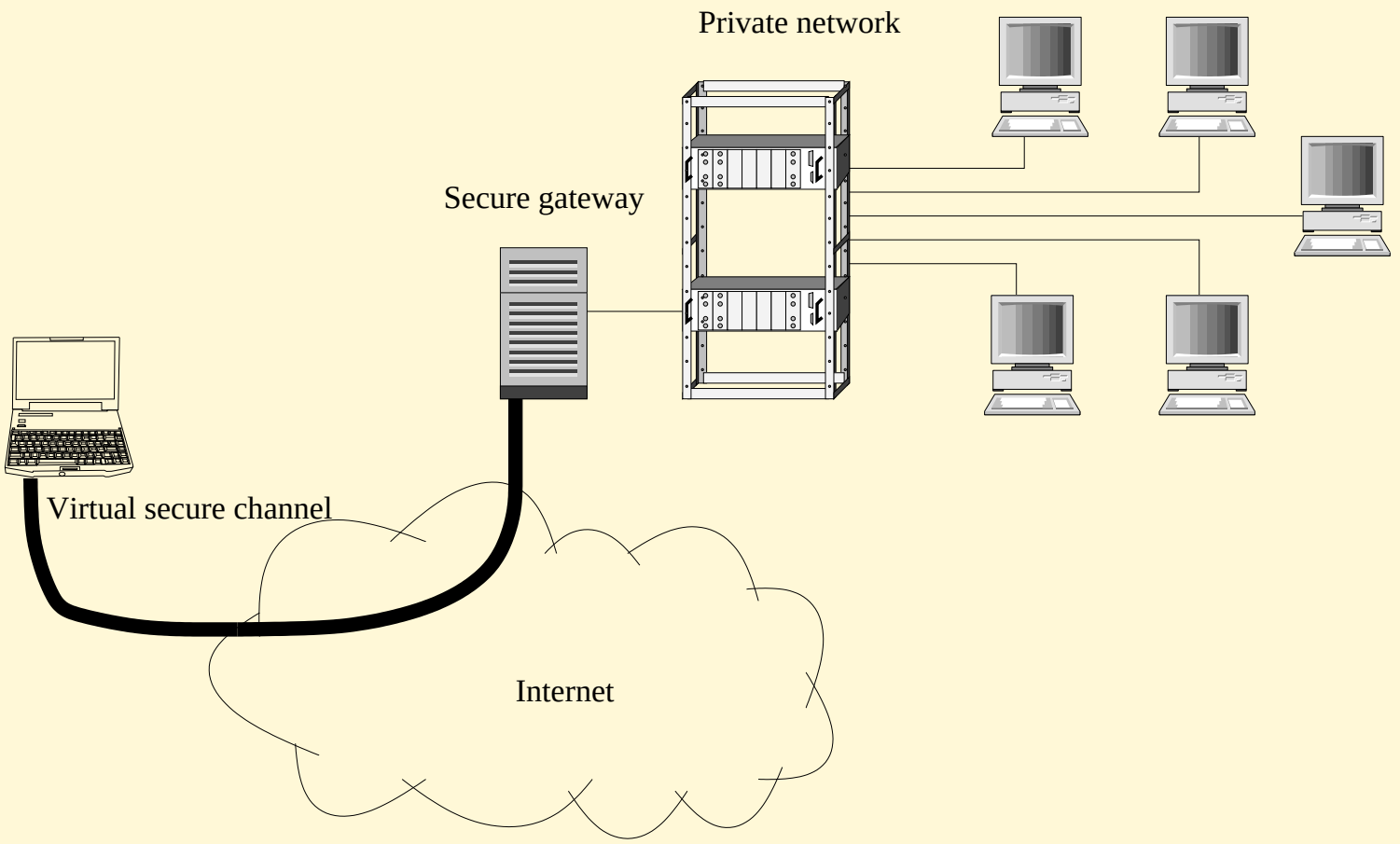
Databases

- IPSec uses two databases:
  - the Security Policy Database (SPD);
  - the Security Association Database (SAD):
    - the records are the Security Associations (SAs).

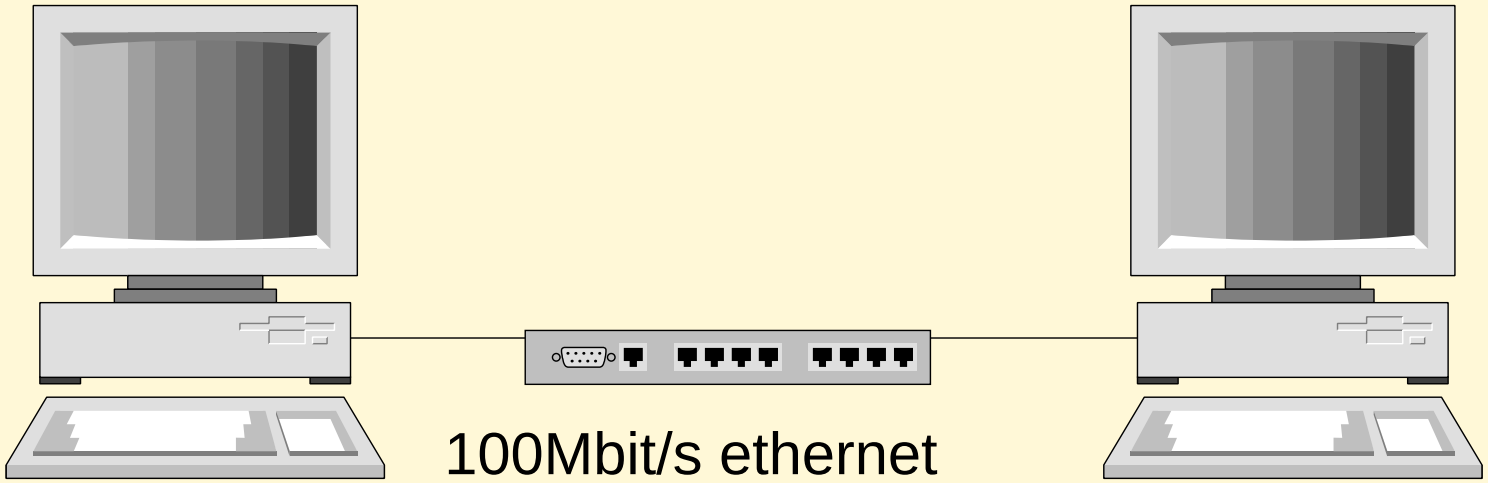
Security Associations

- Each SA contains:
  - protocol/algorithms settings;
  - keys for cryptographic algorithms;
- SAs are mono-directional:
  - two SAs need to be created for normal bidirectional communications.

IPSec - Scenario



Testbed Network (1)



Testbed Network (2)

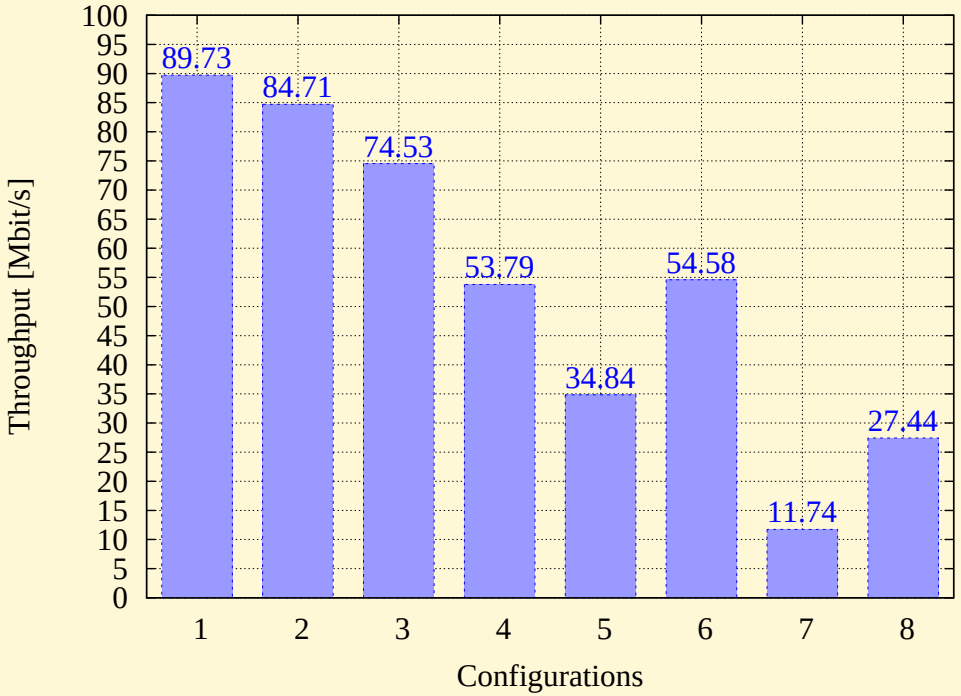
- *Netperf* tool was used for the tests and to measure:
  - average network throughput;
  - average CPU effort;
- a set of *Bash* scripts were used to measure:
  - instantaneous CPU load;
  - instantaneous network traffic.

Tests

- No IPSec;
- ESP in tunnel mode:
  - NULL + HMAC-SHA-1;
  - AES 128;
  - AES 128 + HMAC-SHA-1;
    - no IPComp;
    - IPComp;
  - AES 128 + HMAC-SHA-2 256;
- ESP in tunnel mode + AH tunnel mode:
  - ESP: AES 128; AH: HMAC-SHA-1.

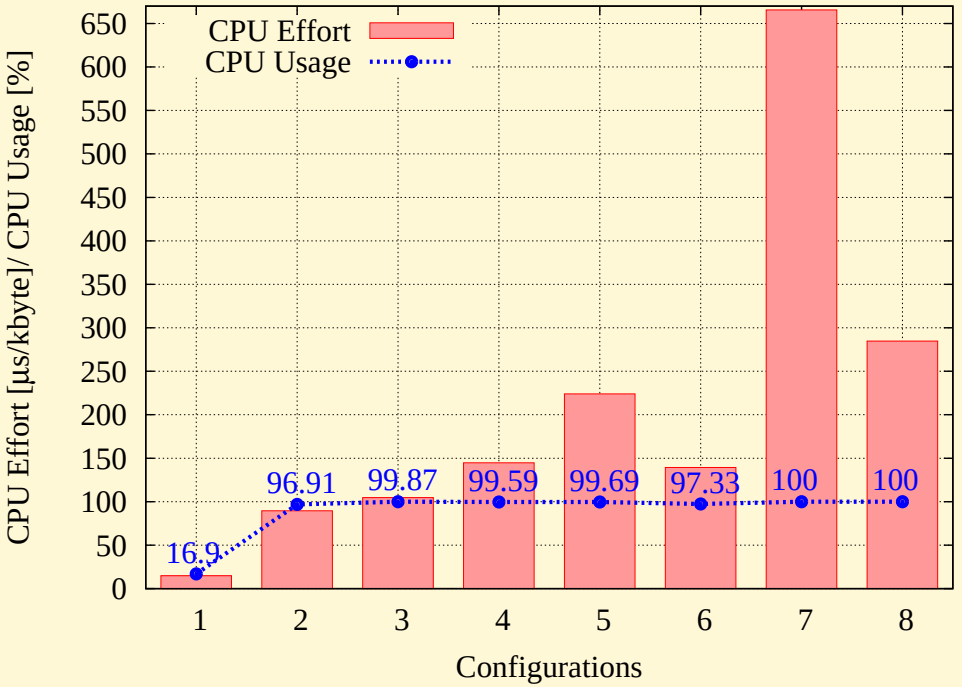
Performance: 100Mbit/s net.

Throughput



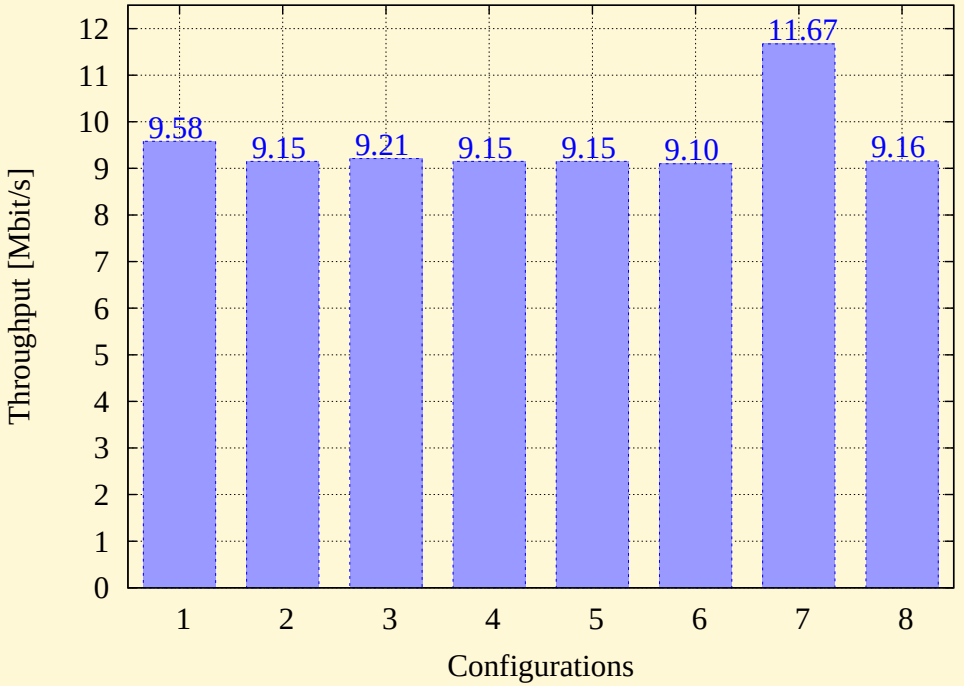
1. No IPSec
2. ESP (NULL, HMAC-SHA-1)
3. ESP (AES 128)
4. ESP (AES 128, HMAC-SHA-1)
5. ESP (AES 128, HMAC-SHA-2 256)
6. ESP (AES 128), AH (HMAC-SHA-1)
7. ESP + IPComp useful
8. ESP + IPComp not useful

CPU Effort and Usage



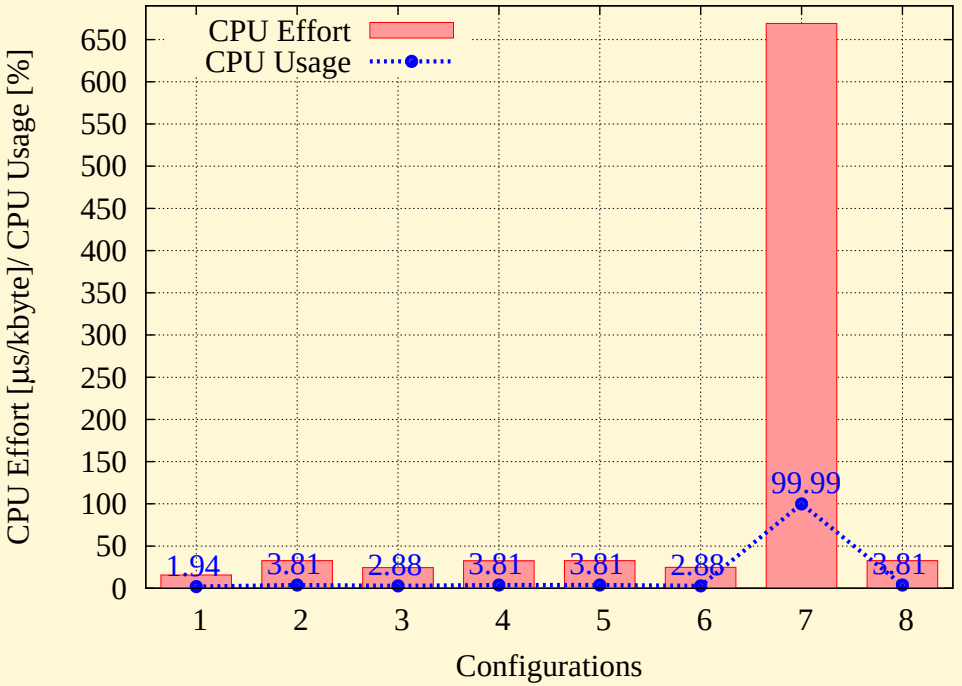
Performance: 10Mbit/s net.

Throughput



1. No IPSec
2. ESP (NULL, HMAC-SHA-1)
3. ESP (AES 128)
4. ESP (AES 128, HMAC-SHA-1)
5. ESP (AES 128, HMAC-SHA-2 256)
6. ESP (AES 128), AH (HMAC-SHA-1)
7. ESP + IPComp useful
8. ESP + IPComp not useful

CPU Effort and Usage



Performance Considerations (1)

- For secure gateways
  there would also be
  the computational load for:
  - management of databases;
  - VPN server;
  - routing, firewalling, . . . ;

Performance Considerations (2)

- hardware acceleration for IPSec is desirable:
  - in high speed networks:
    - it is the only way to obtain desired performance;
  - in low speed networks:
    - it helps optimizing overall system effi ciency.

Performance Considerations (3)

- IPComp helps
  improving network performance
  in low bandwidth environments, but:
  - it is very resource consuming;
  - an accelerator is needed for devices
    with limited computational capabilities.

IPSec Settings (1)

- Encryption should be used only when it is really necessary;
- suitable algorithms (and settings) need to be selected:
  - 3-DES is obsolete and slow in software!
  - 128-bit keys for AES are enough to protect most of the information.

IPSec settings (2)

IPComp:

- is very useful in some cases;
- is very performance killing in some others;
- its usefulness can be evaluated a priori.

Conclusions and Future Work

- These tests allowed us to understand:
  - IPSec requirements;
  - possible settings to be used;
- a performance study
  in an IPv6 environment
  and in embedded system environment
  is ongoing.