CICM in a HA High Performance Security Gateway

IETF81, Québec City

V. Roca, F. Schuler, L. Jacquin
HA, High Performance IPsec gateway

- idea: physical separation between the trusted and untrusted domains

- “red domain” (considered secure) plaintext
- “black domain” (considered unsecured) ciphertext

- secure network
- remote gateway
CICM usage

 IKE
  - runs in the red PC
  - IKE/IPsec session keys are pushed in the crypto module

 IP/IPsec processing on each domain

“red domain”
data traffic
IKE

secure network

CICM::KeyProtocolSender
part of the API

unsecured network
remote gateway

“black domain”
With a clear API, alternatives are “easy”

- different layout (or “cheap version”)
  - single PC + external crypto module
  - no physical separation anymore
  - full software solution

![Diagram showing red and black domains with CICM and secure/unsecured networks]