The Check Point VPN-1/FireWall-1 NGX Medium Robustness Evaluation

Malcolm Levy - Check Point, Certification Manager
Nir Naaman - Metatron, V.P., Security Services

20 September 2006

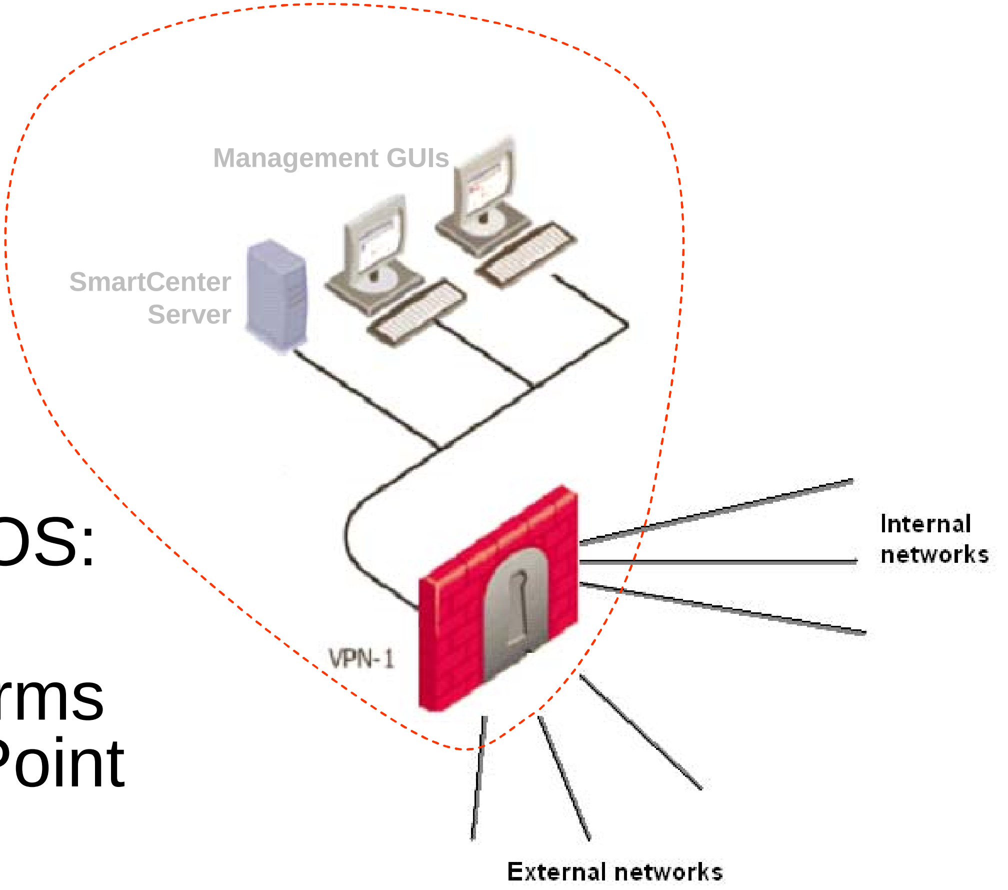
7th International Common Criteria Conference

Contents

- Introduction
- Evaluation goals
- Challenges
- Solutions
  - Project coordination
  - Evaluation of IKE/IPSec Functionality
  - Partner evaluations
- Conclusions

Introduction

- VPN-1 NGX is:
  - A Firewall
  - A VPN gateway
  - An IDS/IPS
  - A remote access gateway
  - ...
- Includes proprietary OS: SecurePlatform
- TOE hardware platforms produced by Check Point hardware partners



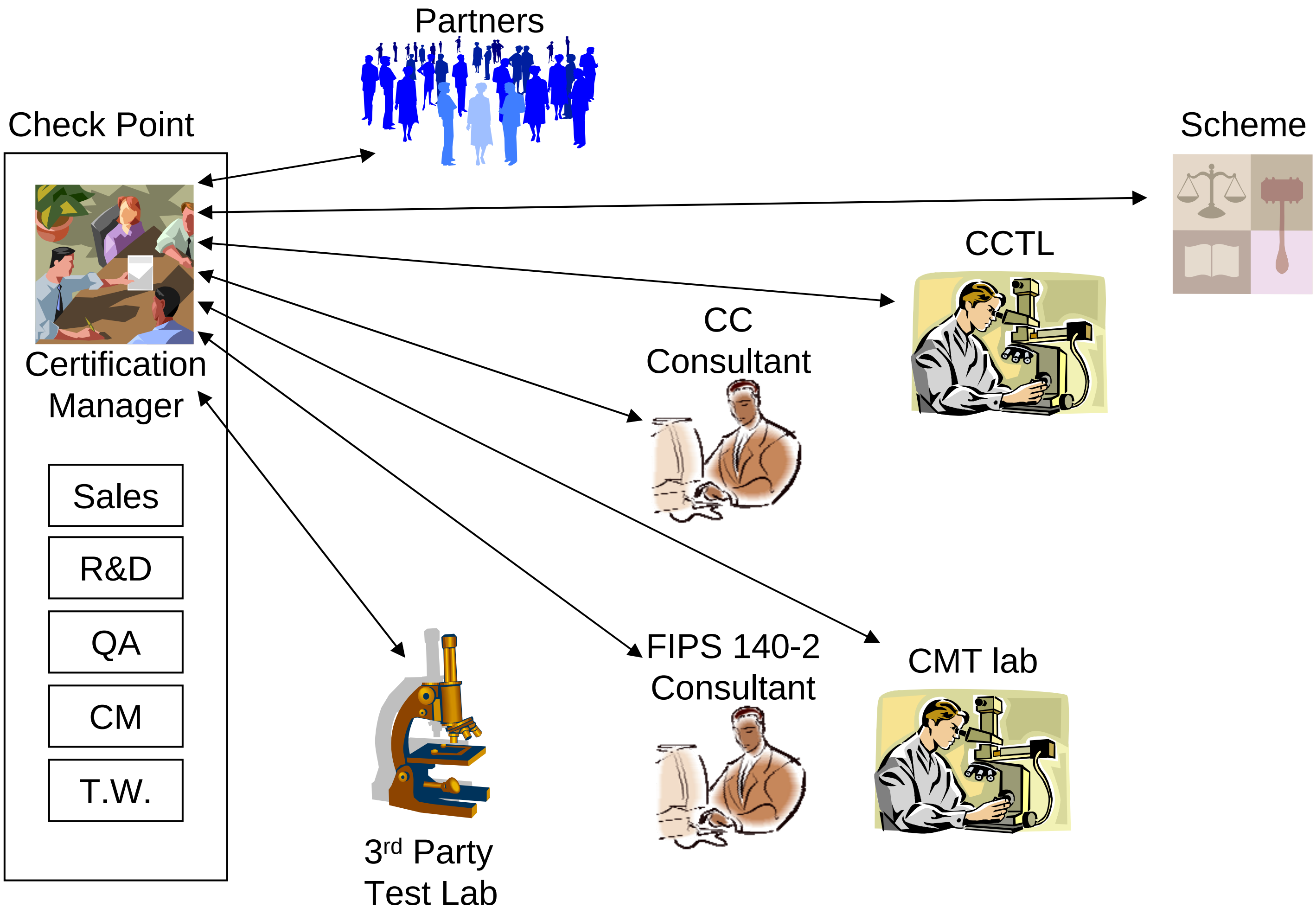
Evaluation Goals

- Customer-identified goals:
  - Medium robustness firewall PPs (proxy/traffic filter)
  - Fully evaluated IKE/IPSec functionality
  - IDS/IPS functionality
  - Hardware in TOE
  - Management server and GUIs in TOE
- Customers demanded **usable** and **secure** TOE:
  - Distributed
  - Remote management
  - IDS/IPS updates
  - Support for NTP, RADIUS, SecurID, LDAP, VLANs, …
  - Support for Diffie Hellman groups 14 to 18, RSA 4096, …
  - Certificate-based authentication for both end-users and administrators

Challenges

- Multiple (sometimes contradicting) PPs
- Complex, fully-functional product
- IKE/IPSec as claimed security functionality
- Hardware developed by Check Point partners

Project Coordination



Partners

Check Point

Certification Manager

Sales

R&D

QA

CM

T.W.

Scheme

CCTL

CC Consultant

FIPS 140-2 Consultant

CMT lab

3rd Party Test Lab

IKE/IPSec Evaluation

- VPN SFRs (claimed and evaluated security functionality)
  - Cryptographic Algorithms (FCS_COP.1)
    - Confidentiality (3DES, AES)
    - Integrity (SHA-1)
    - Authentication (RSA)
    - Key exchange (Diffie Hellman)
  - VPN functionality
    - Confidentiality Protection (FDP_UCT.1)
    - Integrity Protection (FDP_UIT.1)
    - Trusted Channel (FTP_ITC.1)
  - VPN Protocols
    - IKE (FCS_CKM.1)
    - IPSec (FCS_COP.1)
  - In addition:
    - Random number generation
    - Certificate validation

IKE/IPSec Evaluation

- Scheme required claimed cryptographic protocols (IKE, IPSec, TLS) to be evaluated via analysis and testing
- Analysis (ADV class)
  - ADV_FSP.2 requires **complete** details
  - Referencing RFC is insufficient (e.g. “SHOULD”)
  - Check Point provided complete description of TOE behavior for all IKE/ESP packet/payload types.
- Testing (ATE class)
  - Testing of protocol compliance
  - PD 0105 gives example of expectations for testing: behavior when receiving incorrect hash from peer
  - Check Point outsourced a large part of the IKE/IPSec protocol testing work to ICSA Labs

Partner Evaluations

- Made extensive effort to assure that hardware partners could certify too – in the context of evidence development and testing:
  - Nokia and Resilience appliances will have their own certification
  - Included “commodity” H/W: IBM, Sun, HP, Crossbeam, Dell, Patriot, Siemens, SuperMicro, Toshiba

Conclusions

- Customers are becoming CC-aware
  - Demanding higher assurance evaluations
  - Requiring useful boundaries of the TOE
  - Distinguishing between **claimed** and **included** functionality
- Schemes are becoming serious about providing value to the customer
- Vendors must adapt to this changing landscape in order to meet customers’ needs

Benefits of CC Evaluation

- PPs are a mechanism for customers to establish their generic security requirements
- Check Point customers receive value:
  - Third-party assurances for security functionality
  - Functionality added to meet new requirements
  - CC analysis helps vendor identify missing or desirable functionality
  - Improved delivery procedures
  - CC evaluated configuration guidance
- Evaluation results highlight Check Point product differentiators in relation to its competitors

Questions?

- Malcolm Levy

  Certification Manager

  Check Point Software Technologies Ltd.

  malcolm@checkpoint.com

- Nir Naaman, CISSP

  V.P., Security Services

  Metatron, Ltd.

  nir.naaman@metasec.com