Ecole d'Ingénieurs du Canton de Vaud

VPN Solution

Christian Tettamanti

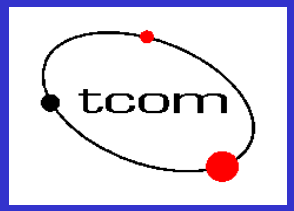
christian.tettamanti@eivd.ch

Stefano Ventura

stefano.ventura@eivd.ch

TCOM Institute

EIVD



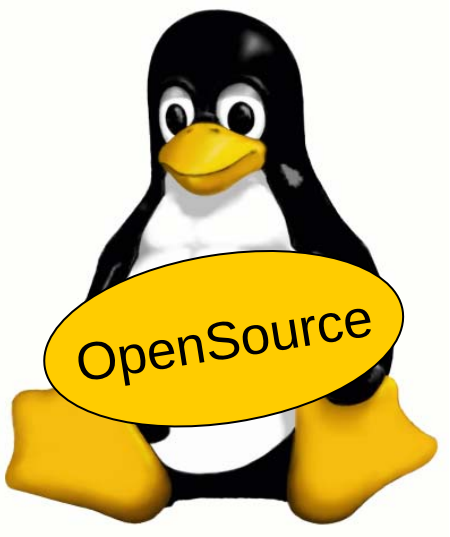
VPN - Virtual Private Network

Start date : 01.02.2002
Duration : 1+1 years

Stefano Ventura	prof. HES
Christian Tettamanti	ing. HES
Pascal Gachet	ing. HES

Gérald Litzistorf	prof. HES
Philippe Logean	ing. HES
Nicolas Sadeg	ing. HES

VPN - Goals Of The Project



VPN Project

Phase I
Protocols

Phase II
Authentication

Phase III
Deployment

Christian Tettamanti, ing. HES

VPN - Goals Of The Project

- Phase I
  - Research and study of remote access solutions
  - Secure access on internal private network
  - Interoperability tests
  - Study of VPN protocols (L2TP, PPTP, IPSec)
  - LAN-to-LAN and HOST-to-LAN scenarios

Christian Tettamanti, ing. HES

VPN - Goals Of The Project

- Phase I

  Protocols
  - PPTP point-to-point tunneling protocol
  - L2TP layer 2 tunneling protocol
  - IPSEC IP security protocols
    - IKE → authentication
    - AH → integrity
    - ESP → confidentiality, integrity

Christian Tettamanti, ing. HES

VPN - Goals Of The Project

Phase II
Authentication

- Phase II
  - Research and study of secure authentication mechanisms
  - Study of Public Key Infrastructure (PKI)
  - Interoperability tests

Christian Tettamanti, ing. HES

VPN - Goals Of The Project

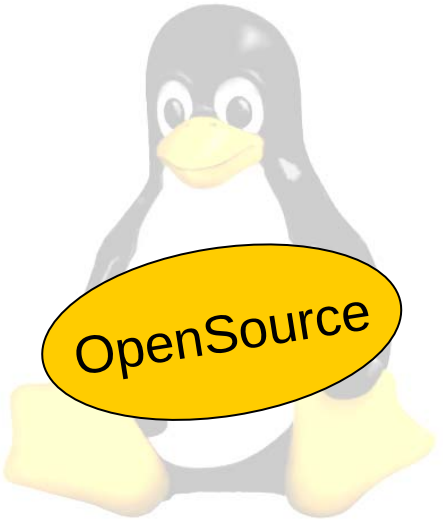
- Phase III
  - Deployment
    - LAN-to-LAN between EIG and TCOM
    - HOST-to-LAN at EIVD

Christian Tettamanti, ing. HES

VPN – Open Source Software

Different solutions based on Open Source

- Server OS: Slackware Linux
- Firewall: Netfilter/iptables
- Gateway VPN: OpenSwan
- PKI Authority: OpenCA
- VPN Clients: Win2K: SSH Sentinel*
  Linux: OpenSwan



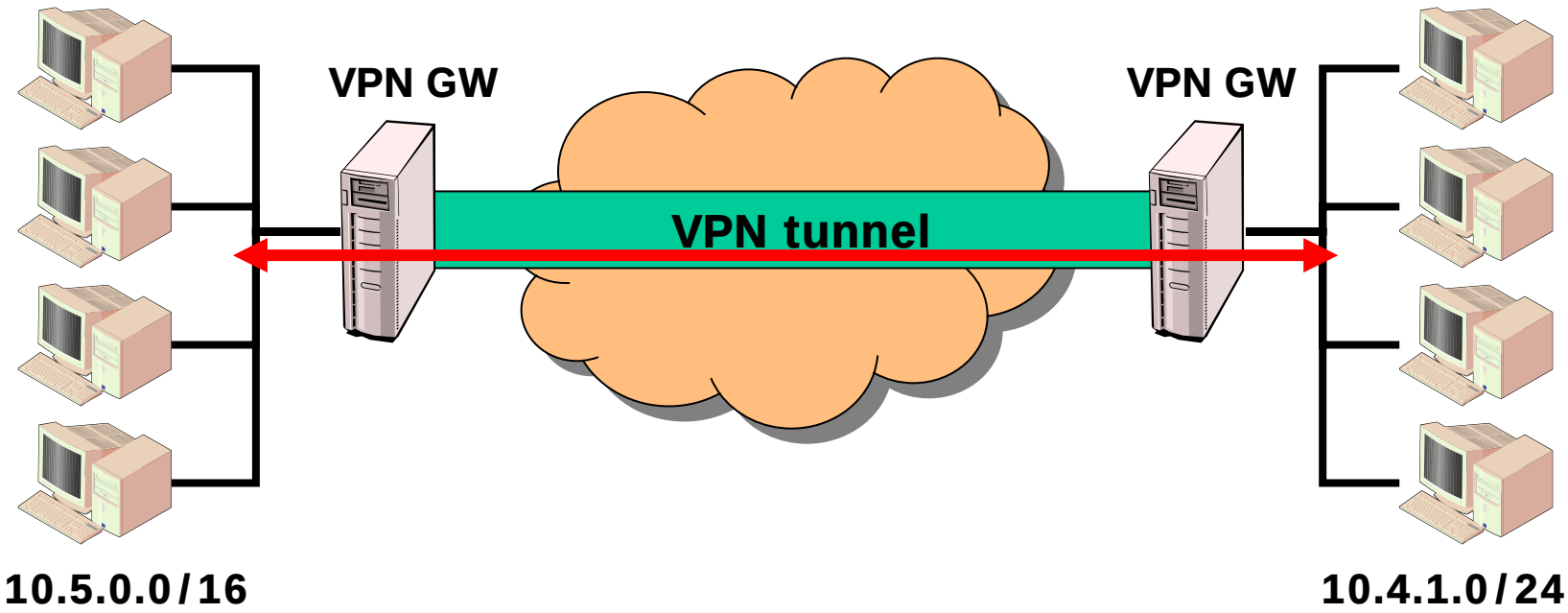
*Free License for universities

Christian Tettamanti, ing. HES

VPN – Scenario 1

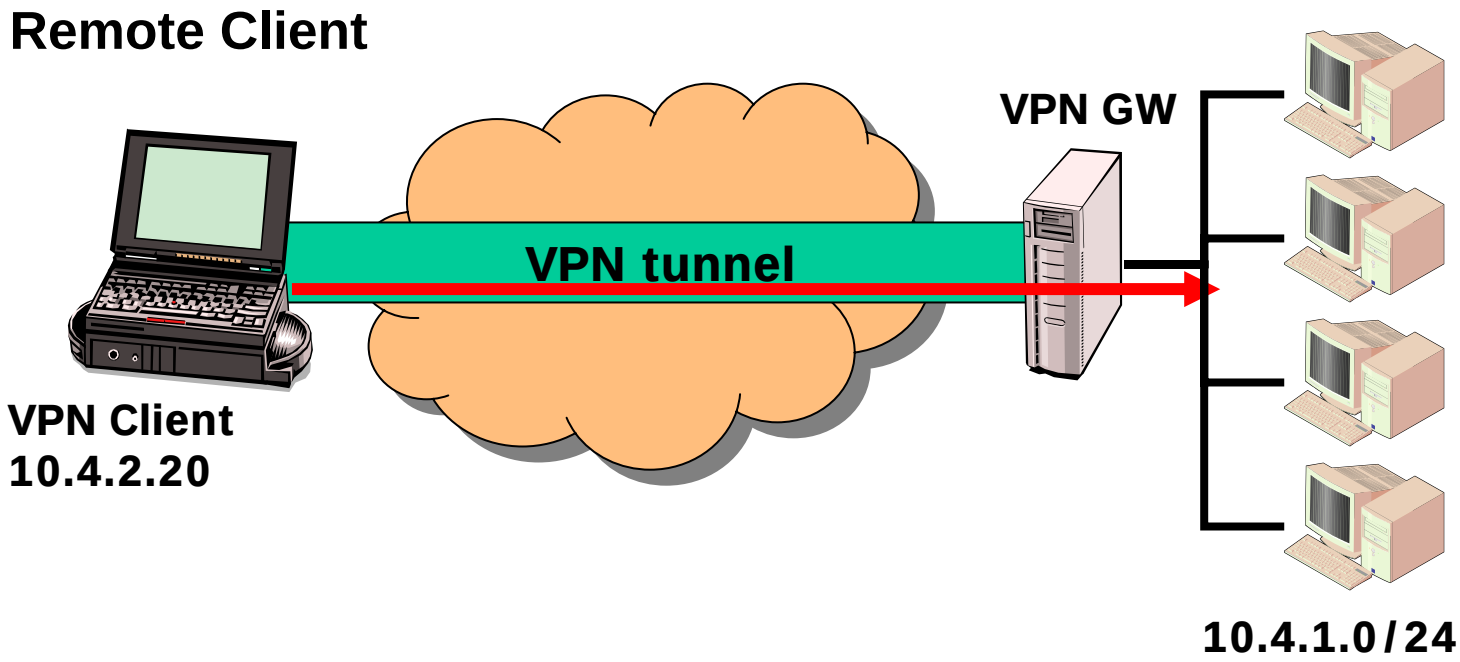
EIG – Proprietary Solutions

EIVD – Open Source Solutions



Christian Tettamanti, ing. HES

VPN – Scenario 2

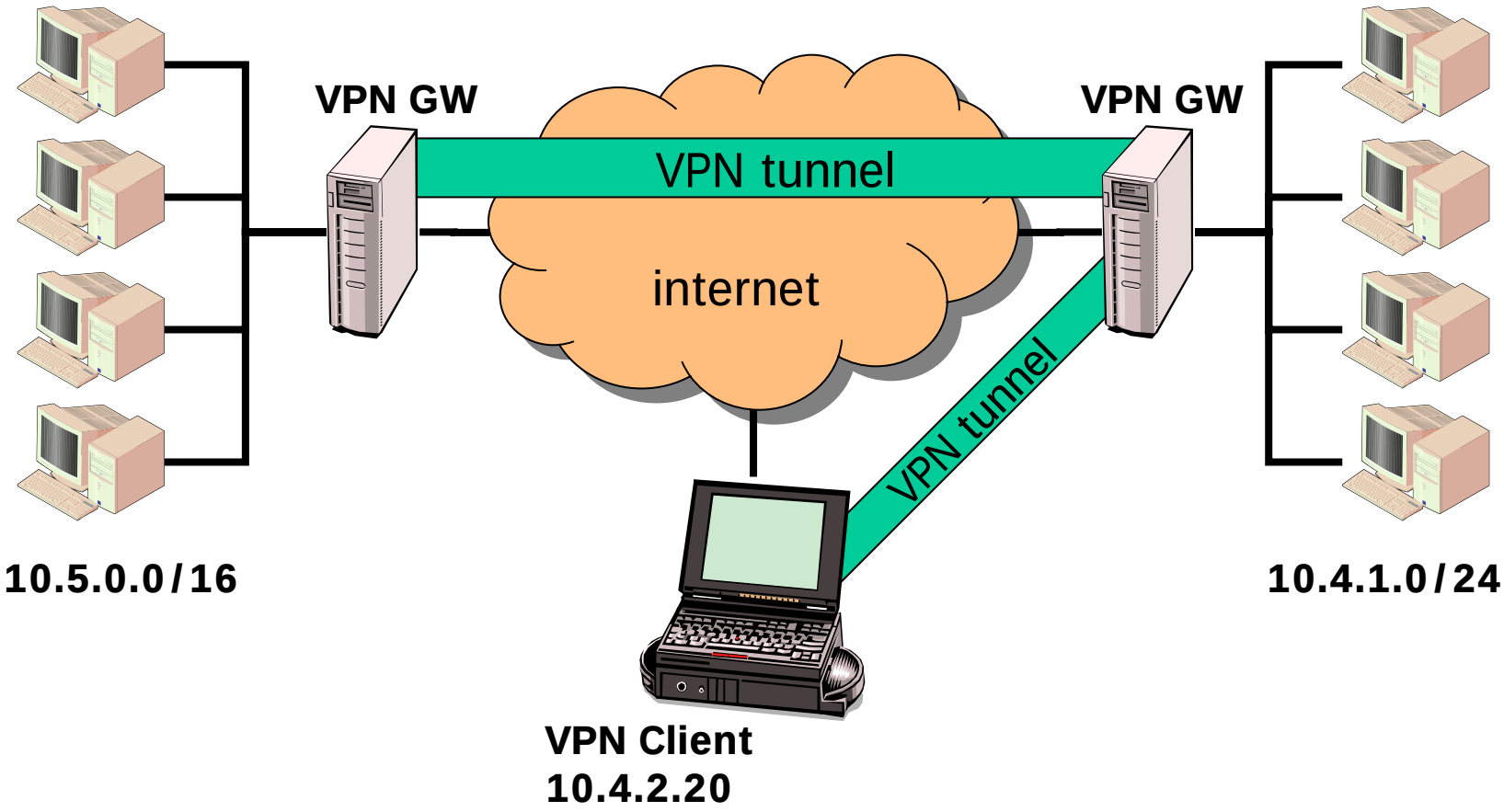


Christian Tettamanti, ing. HES

VPN – Scenario 3

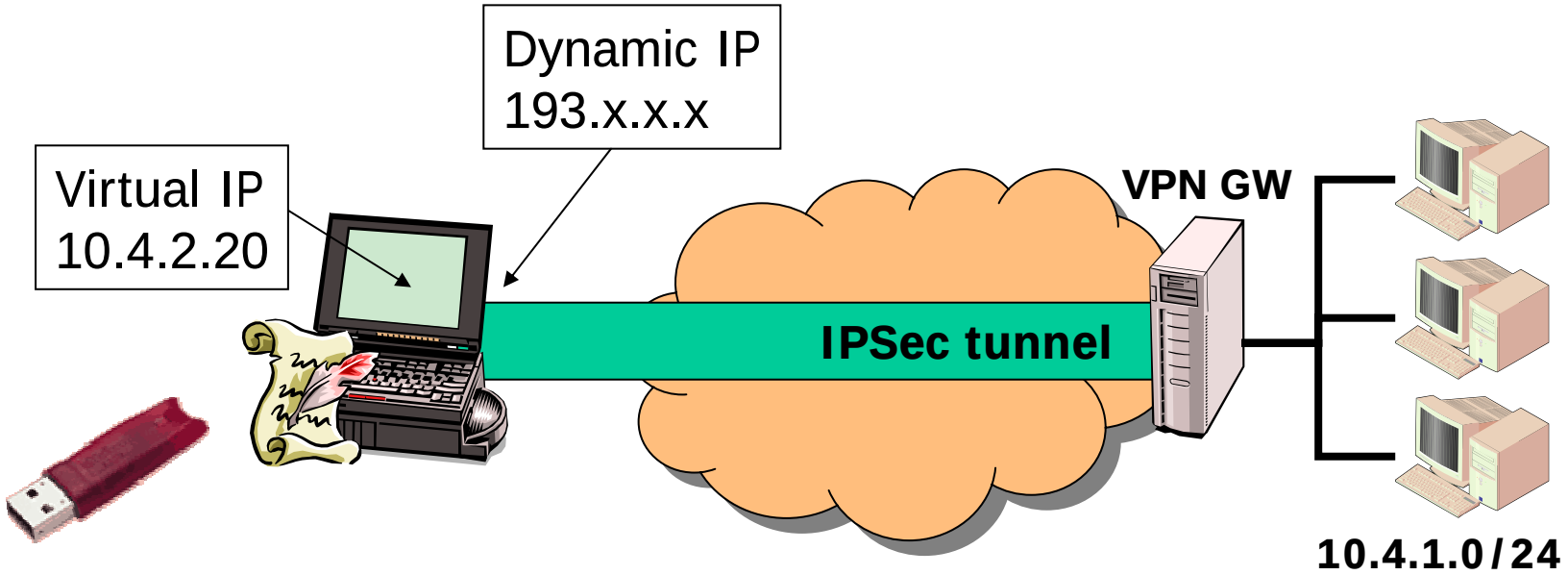
EIG – Proprietary Solutions

EIVD – Open Source Solutions



Christian Tettamanti, ing. HES

VPN – Remote Client Authentication

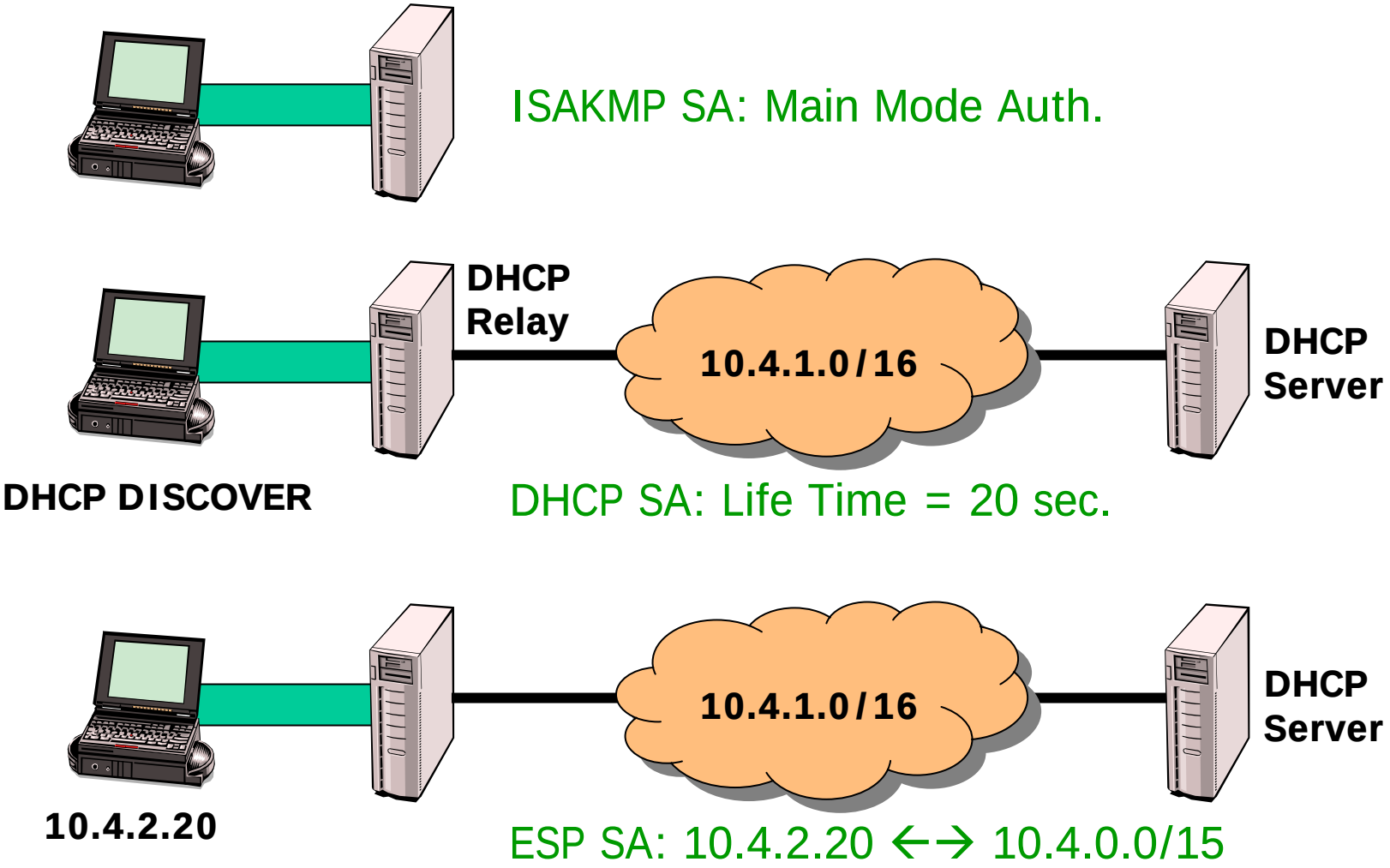


- The remote client authenticates himself on gw VPN
- The authentication is based on X.509 certificates
- The client acquire a private IP address with DCHP-over-IPSEC
- The remote client is part of the internal private network

Christian Tettamanti, ing. HES

VPN – DHCP-over-IPSec

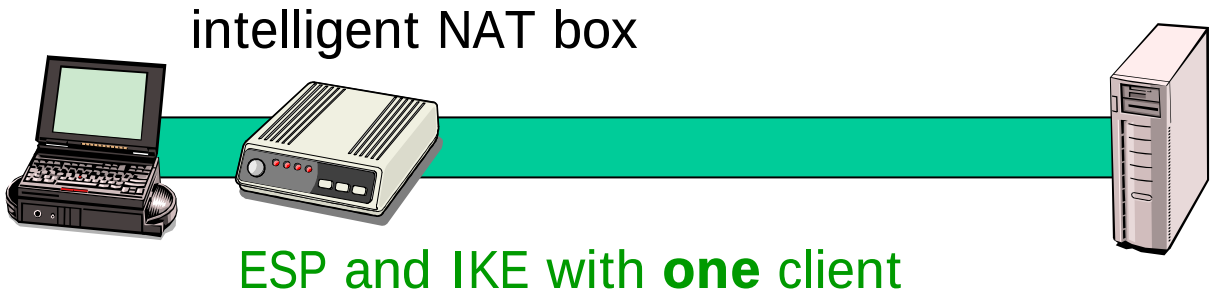
- Internet Draft: draft-ietf-ipsec-dhcp-13.txt

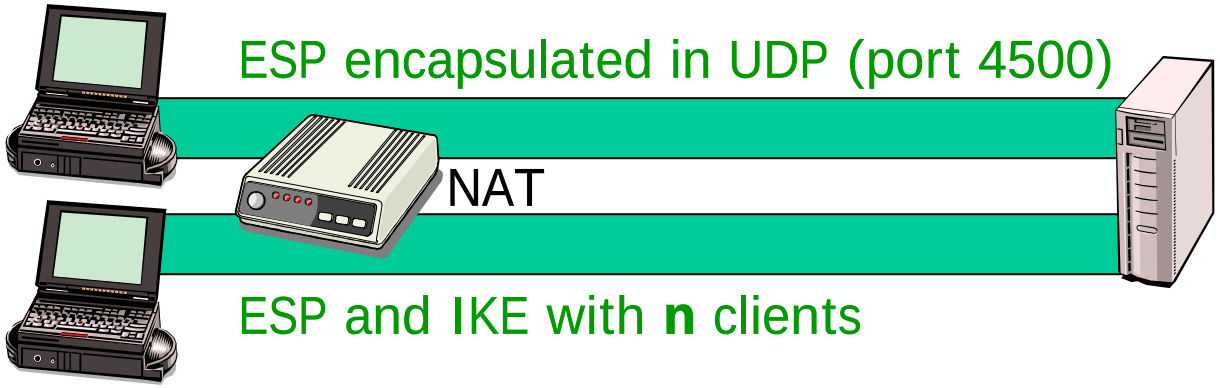


Christian Tettamanti, ing. HES

VPN – NAT-Traversal

- Internet Drafts: draft-ietf-ipsec-udp-encaps-03.txt
  draft-ietf-ipsec-nat-t-03.txt





Christian Tettamanti, ing. HES

VPN – Encountered Problems

- PKI
  - Token Integration
- Internet Service Provider (ISP)
  - Firewalls
  - Routing
- NAT routers
  - Intelligent Box
  - Stupid Box
    - NAT-Traversal
    - ESP→UDP Encapsulation

VPN – Gateway VPN Capabilities

IKE:

Encryption algorithm:	aes-256bit
Integrity function:	SHA-2
DF Group:	MODP 1536 (group 5)
PKI authentication	OK

IPSEC – ESP (AH):

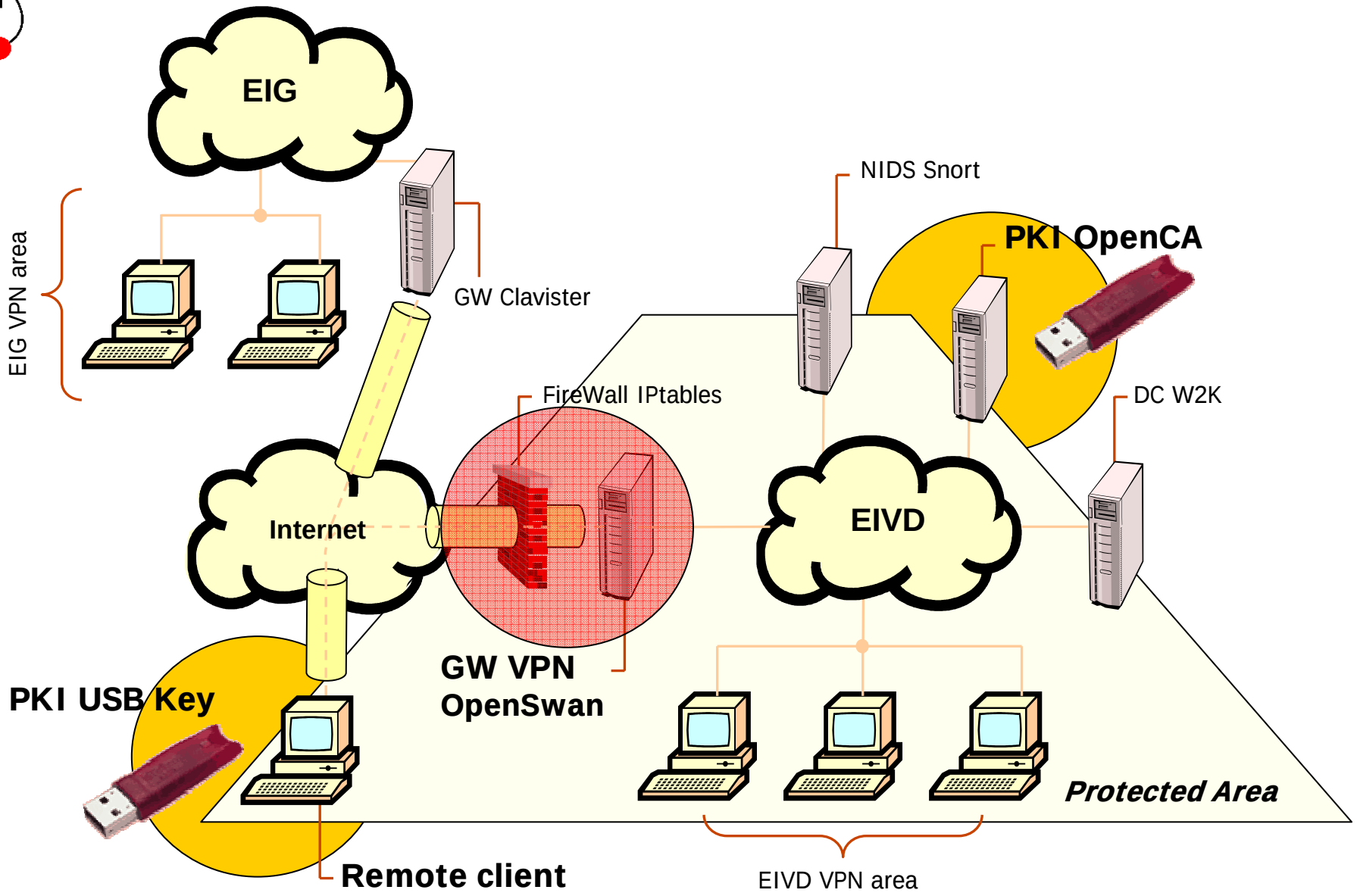
Encryption algorithm:	aes-256bit
Integrity function:	HMAC-SHA-2
DF Group:	MODP 1536 (group 5)

Other:

DHCP over IPSEC	OK
NAT-Traversal	OK

Christian Tettamanti, ing. HES

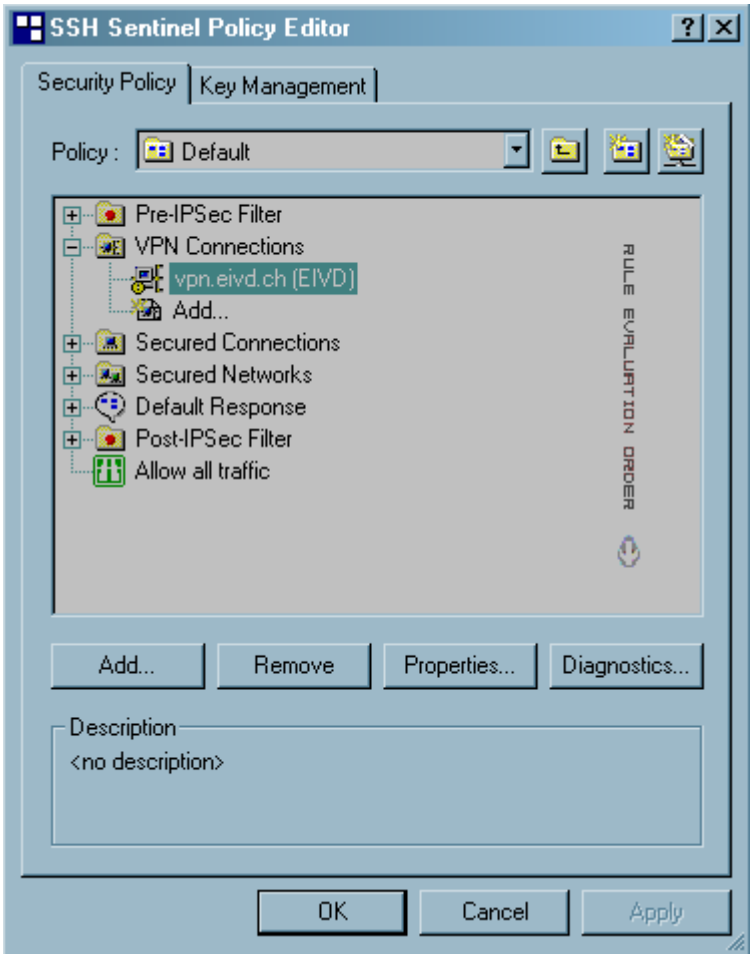
VPN – Final Architecture



Christian Tettamanti, ing. HES

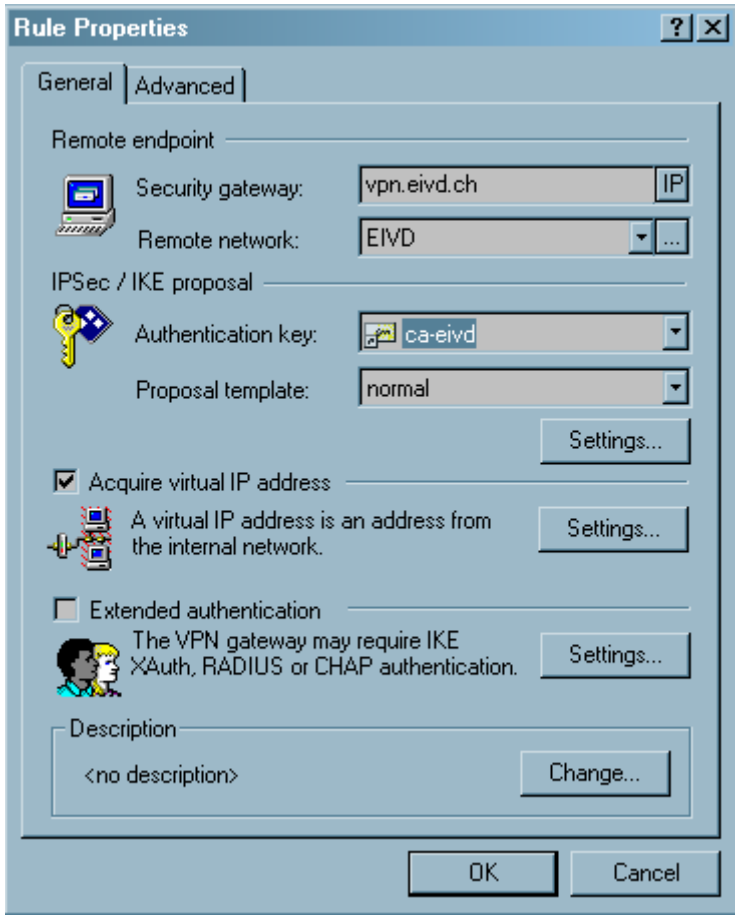
!!! Demonstration !!!

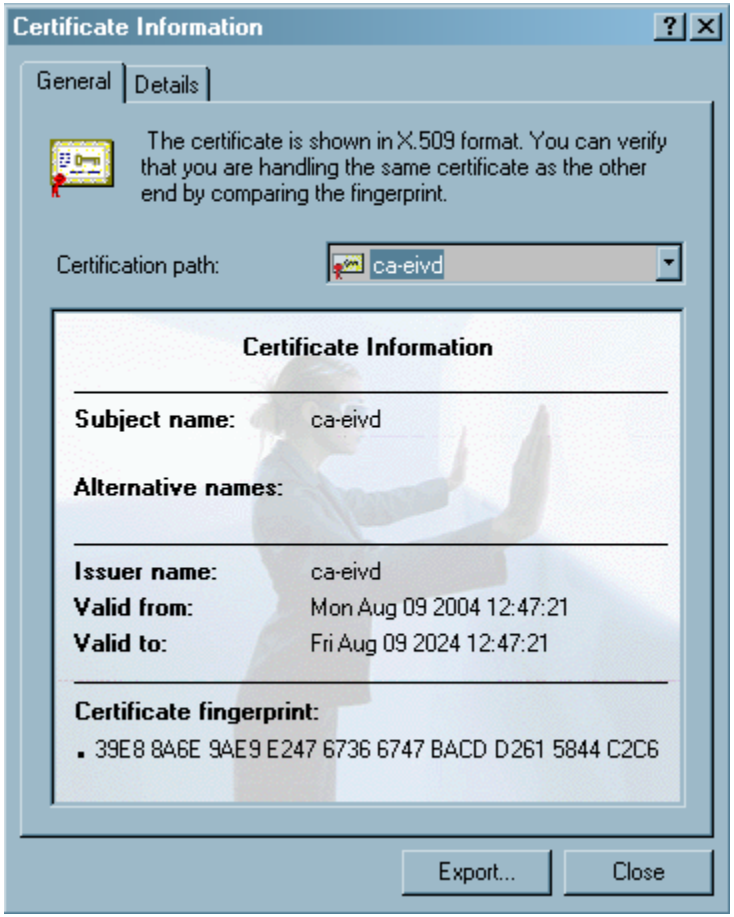
VPN – SSH Sentinell Configuration



Christian Tettamanti, ing. HES

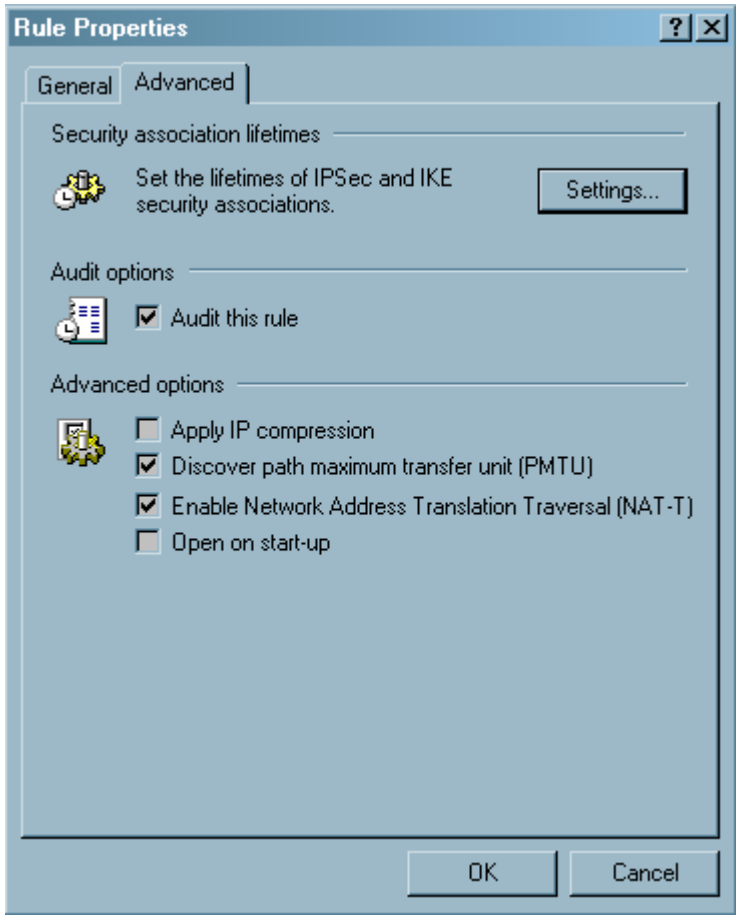
VPN – PKI Certificate Configuration

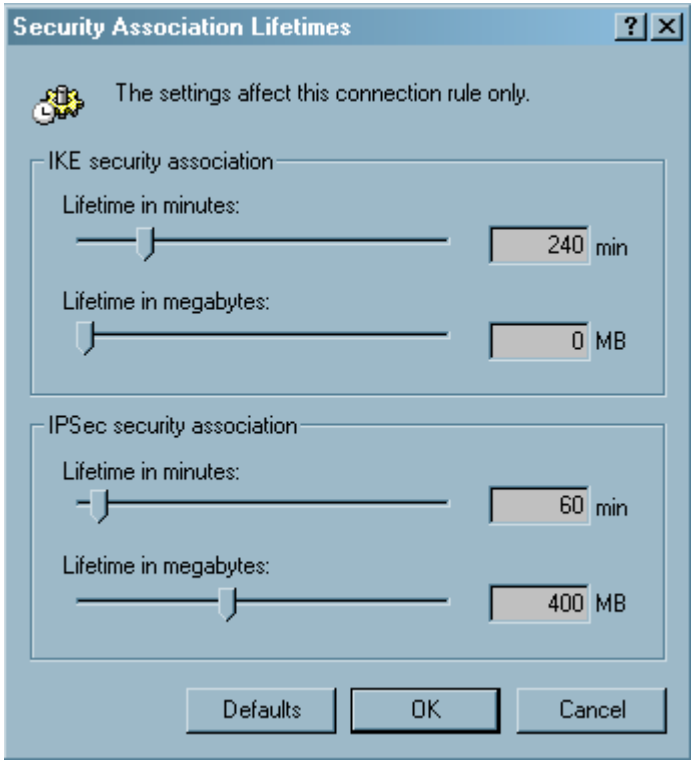




Christian Tettamanti, ing. HES

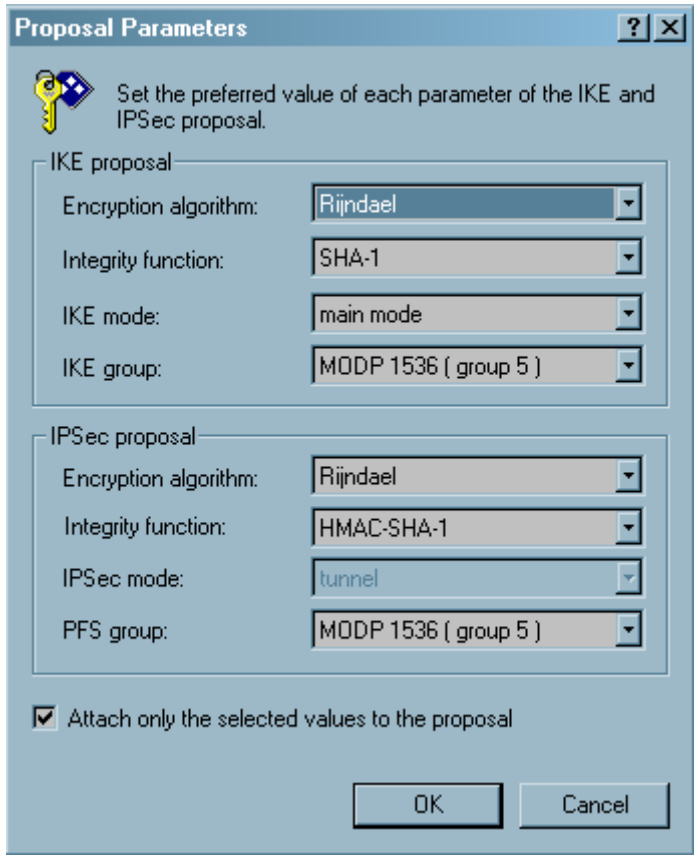
VPN – SA Life & NAT Configuration

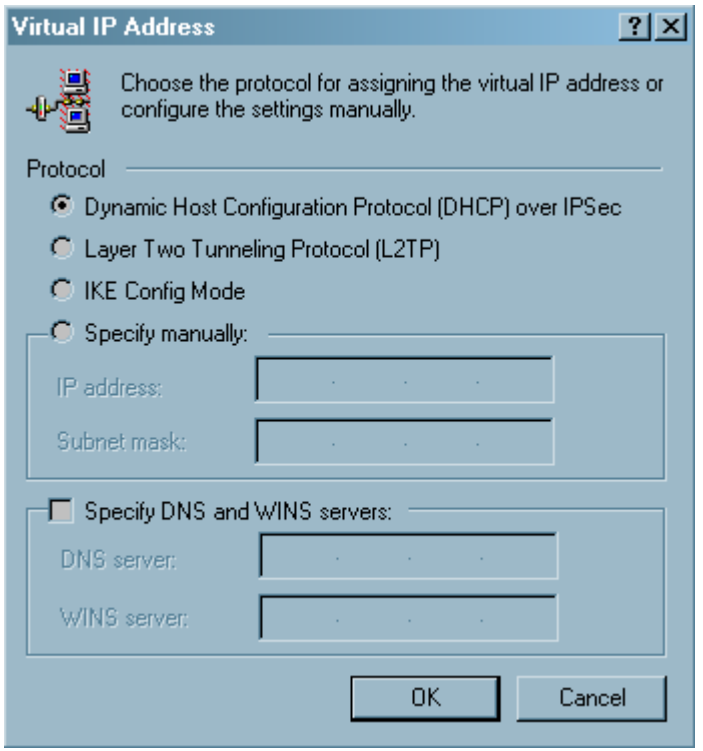




Christian Tettamanti, ing. HES

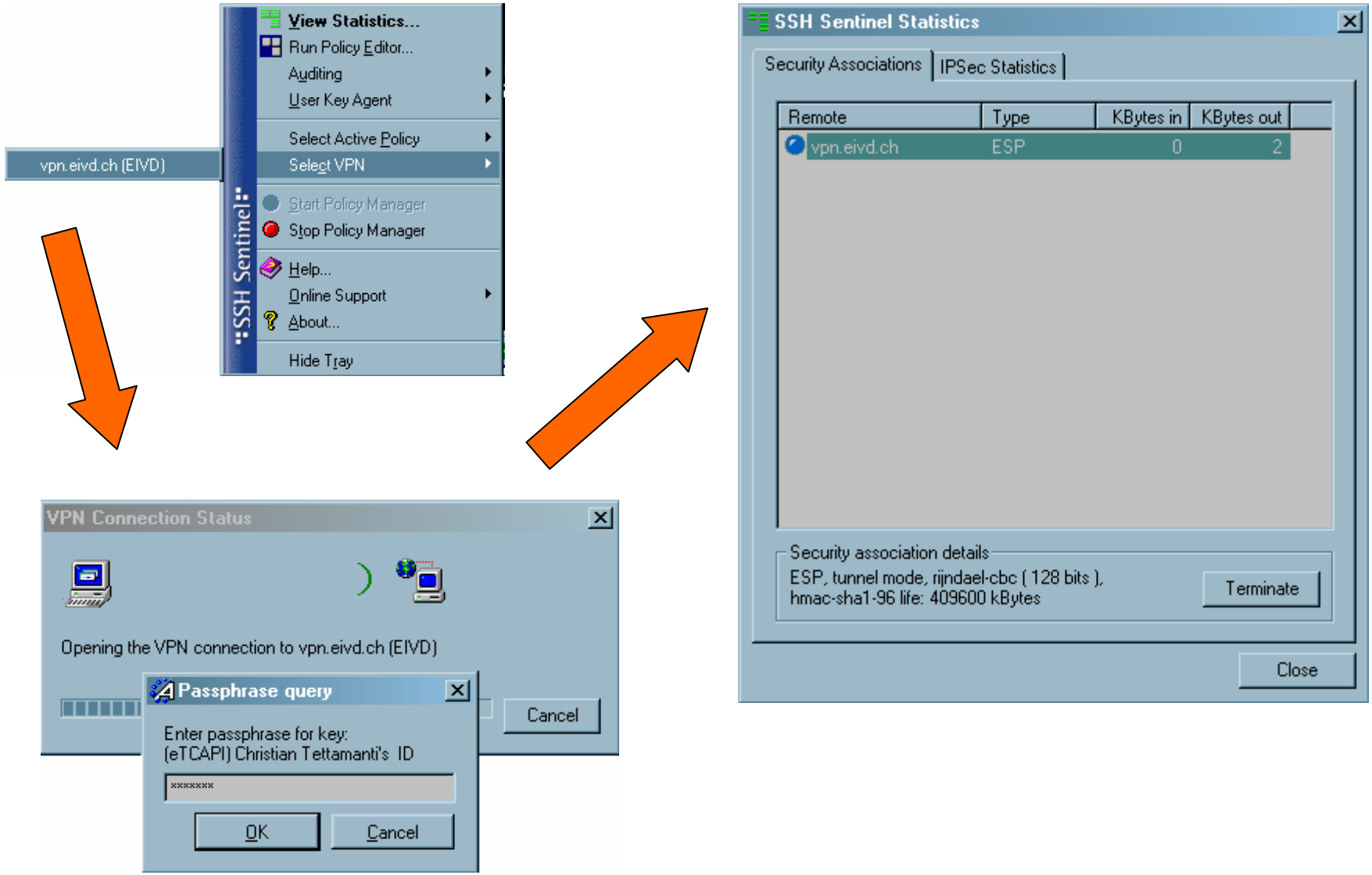
VPN – IKE & ESP Configuration





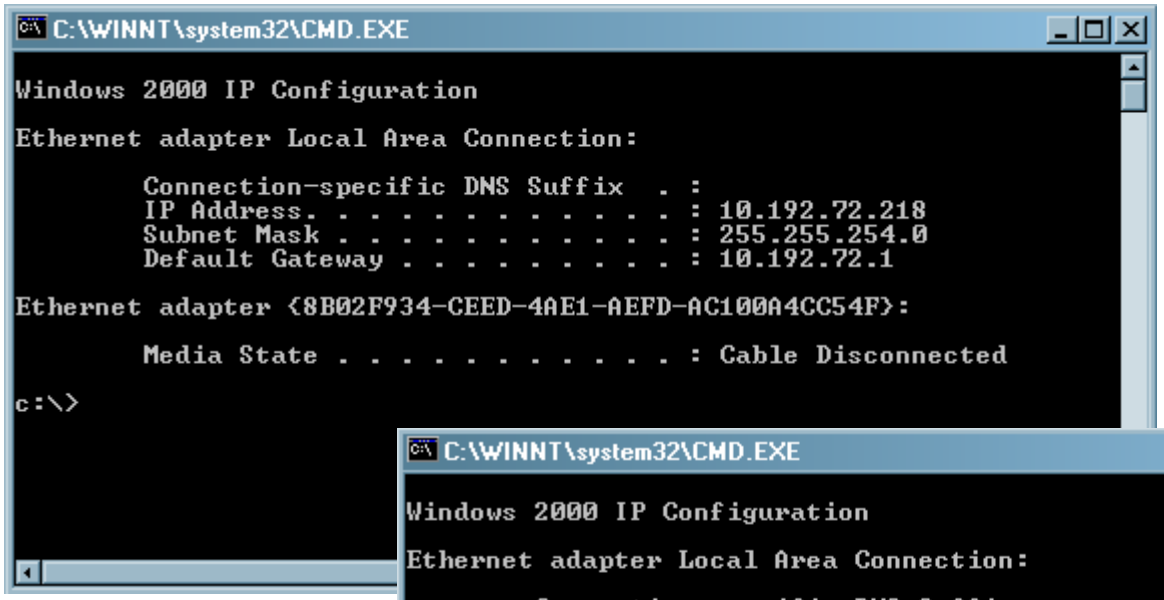
Christian Tettamanti, ing. HES

VPN – Connection example

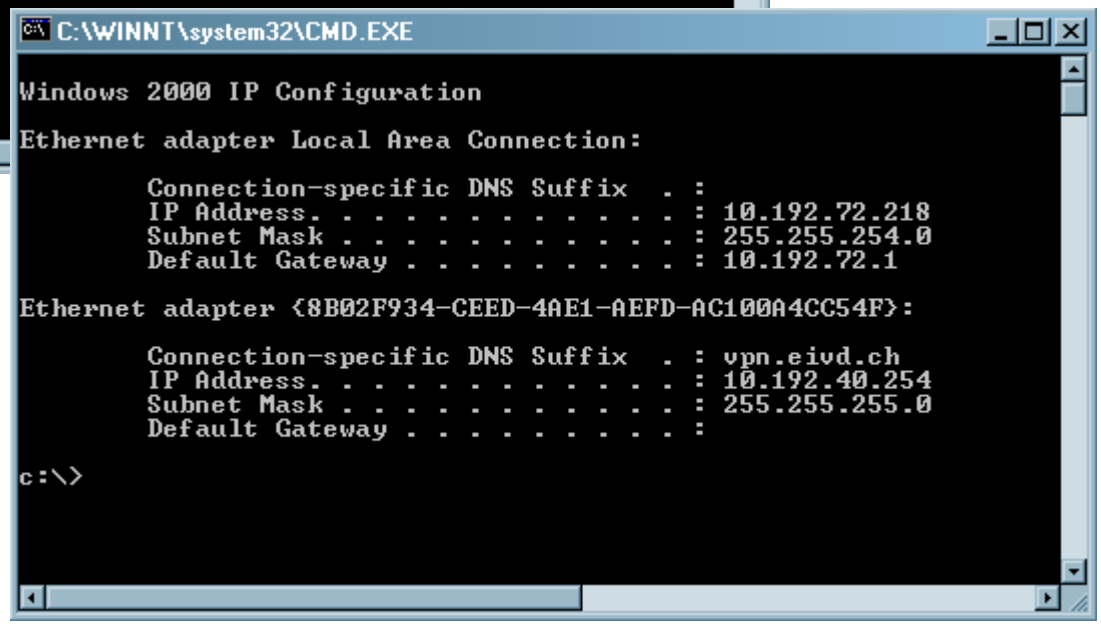


Christian Tettamanti, ing. HES

VPN – Network Interfaces



Before VPN Connection



After VPN Connection

Christian Tettamanti, ing. HES

??? Questions ???