

Ecole d'Ingénieurs du Canton de Vaud

VPN Solution

Christian Tettamanti

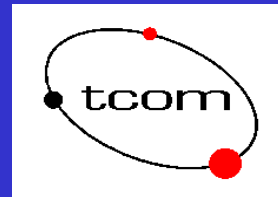
christian.tettamanti@eivd.ch

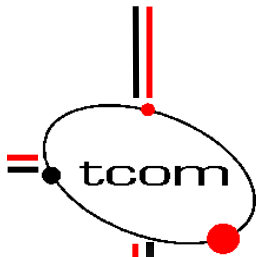
Stefano Ventura

stefano.ventura@eivd.ch

TCOM Institute

EIVD





VPN - Virtual Private Network

Start date : 01.02.2002

Duration : 1+1 years



Stefano Ventura
Christian Tettamanti
Pascal Gachet

prof. HES
ing. HES
ing. HES

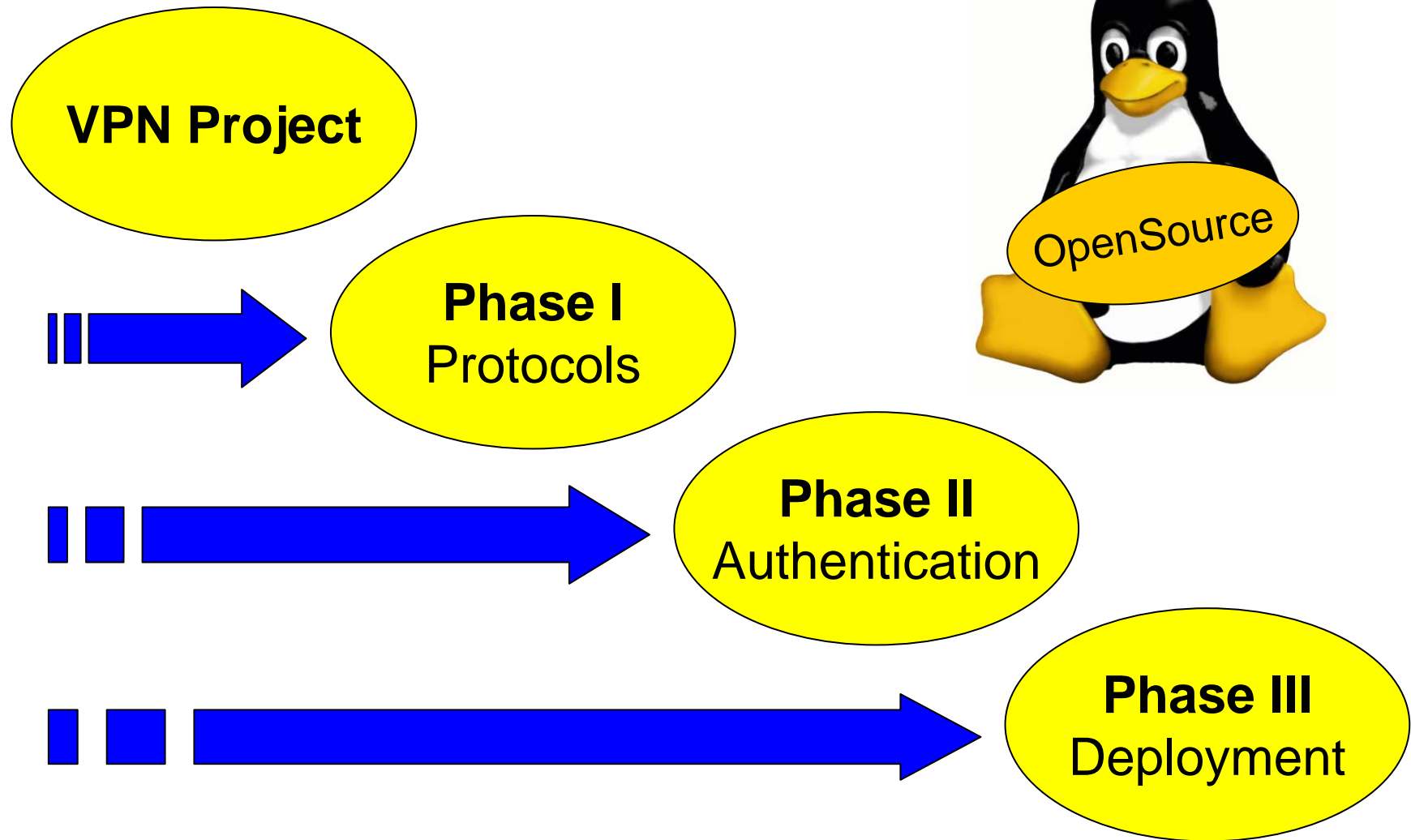


Gérald Litzistorf
Philippe Logean
Nicolas Sadeg

prof. HES
ing. HES
ing. HES



VPN - Goals Of The Project



VPN - Goals Of The Project



Phase I Protocols

- 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

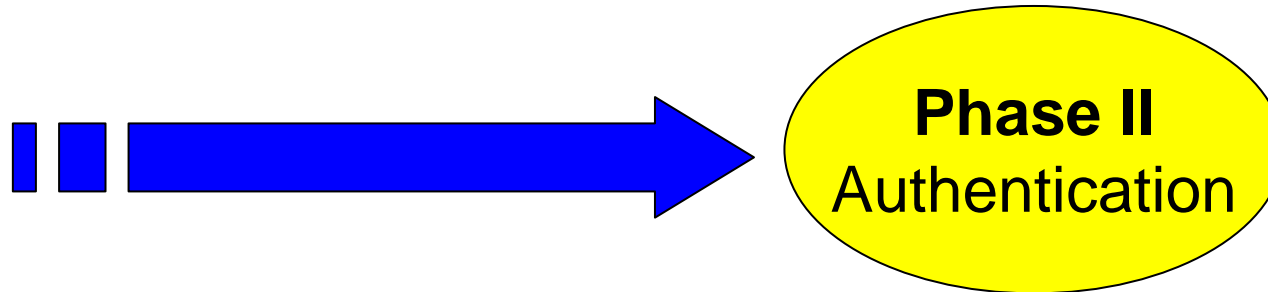
VPN - Goals Of The Project

- 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

VPN - Goals Of The Project



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



VPN - Goals Of The Project

tcom



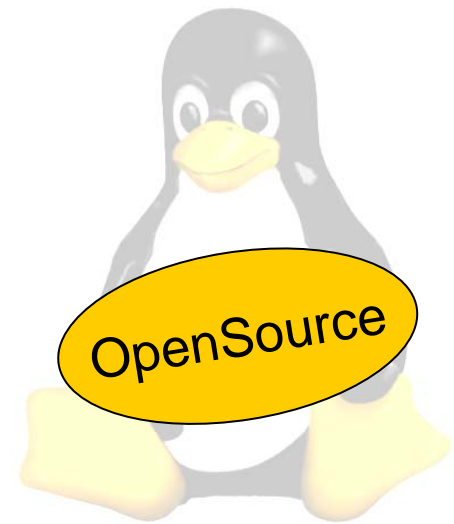
**Phase III
Deployment**

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

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

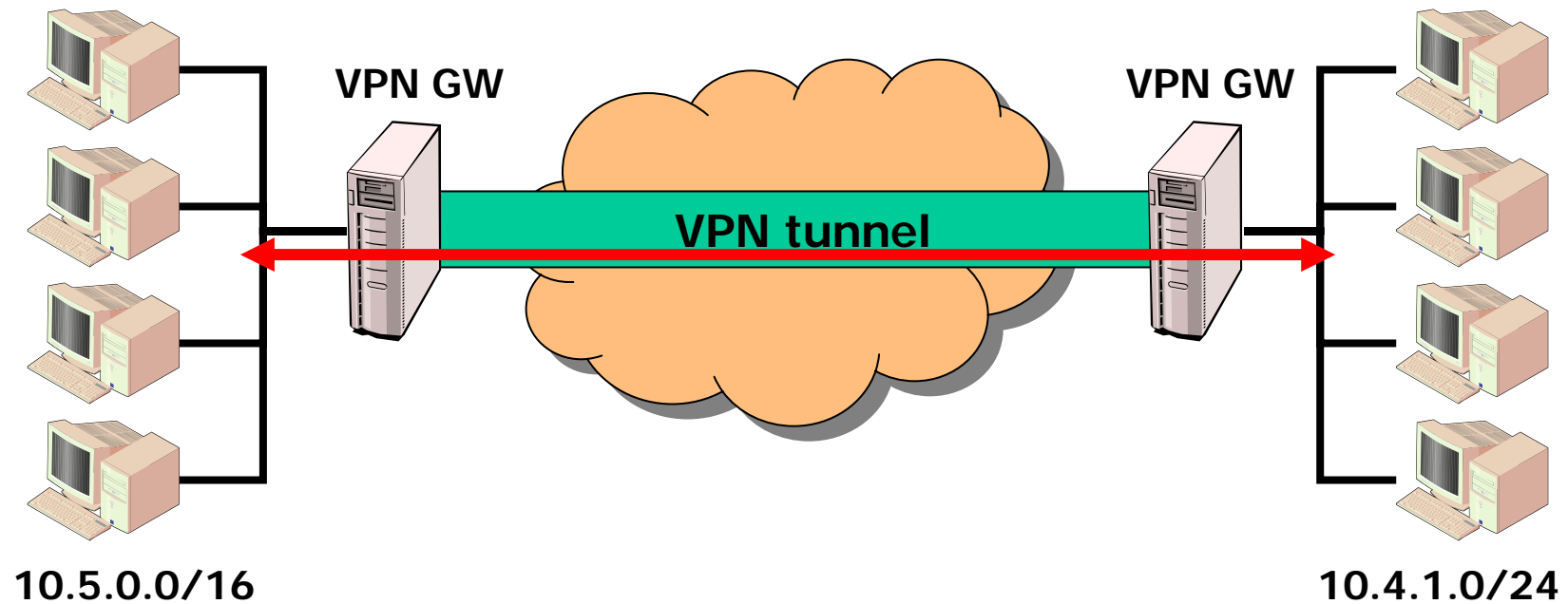


*Free License for universities

VPN – Scenario 1

EIG – Proprietary Solutions

EIVD – Open Source Solutions



VPN – Scenario 2

EIVD – Open Source Solutions

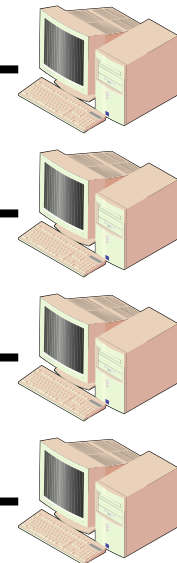
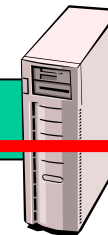
Remote Client

VPN Client
10.4.2.20



VPN tunnel

VPN GW

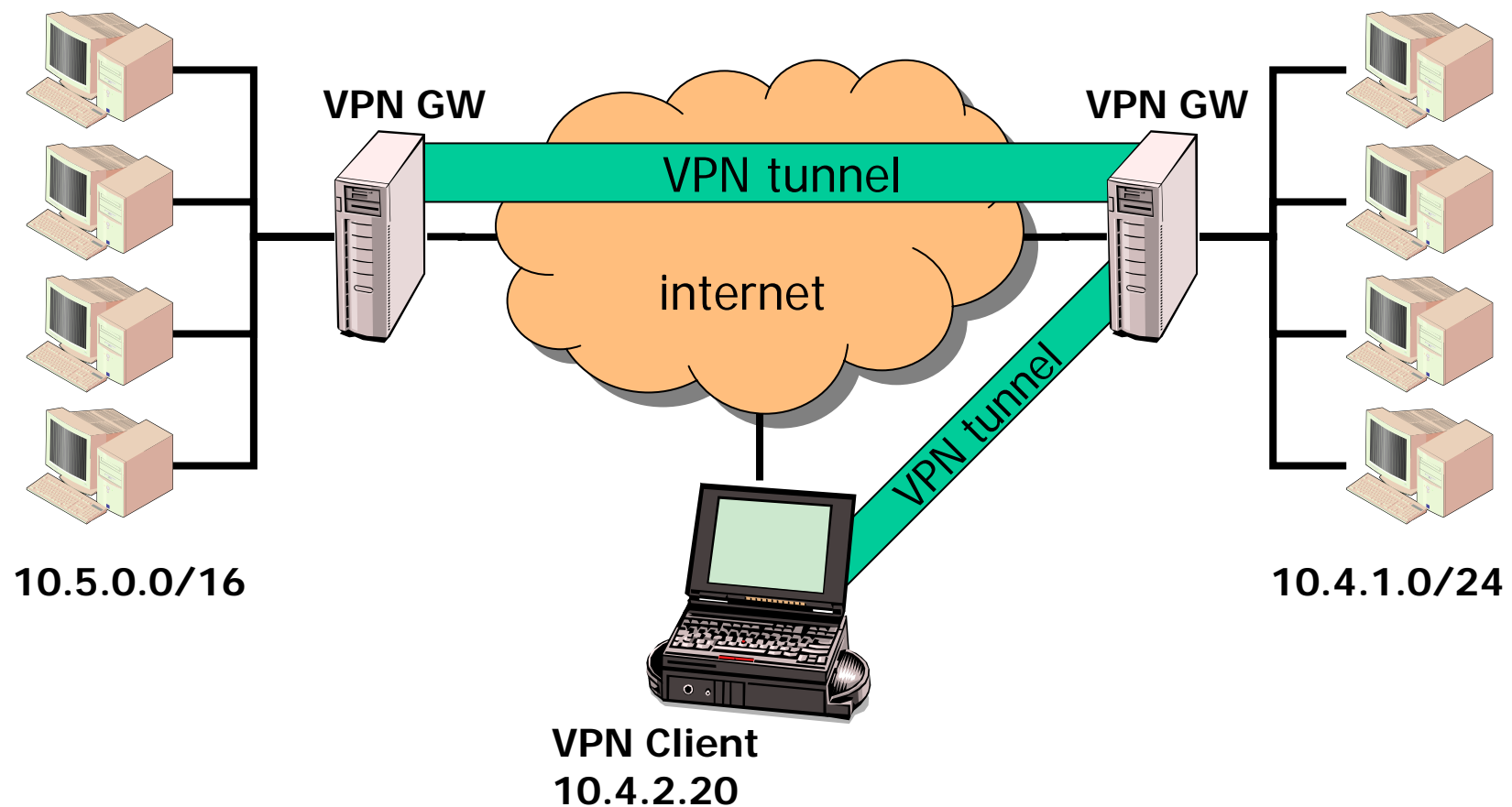


10.4.1.0/24

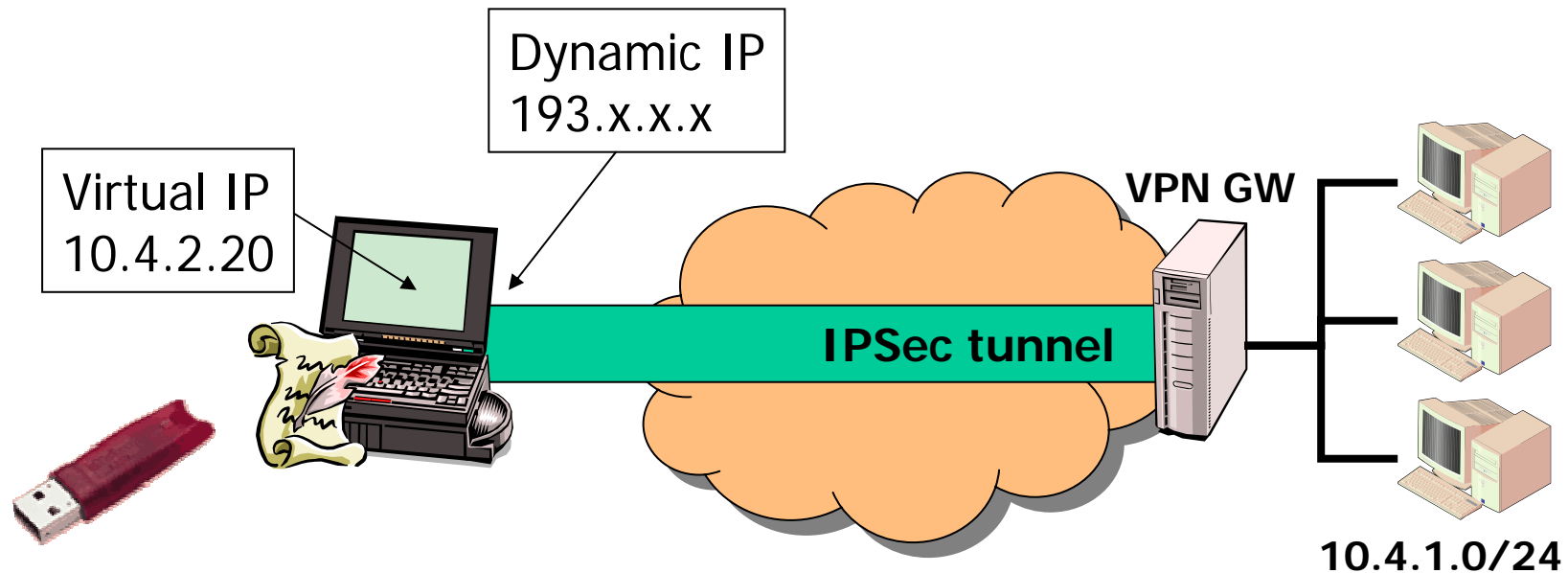
VPN – Scenario 3

EIG – Proprietary Solutions

EIVD – Open Source Solutions



VPN – Remote Client Authentication

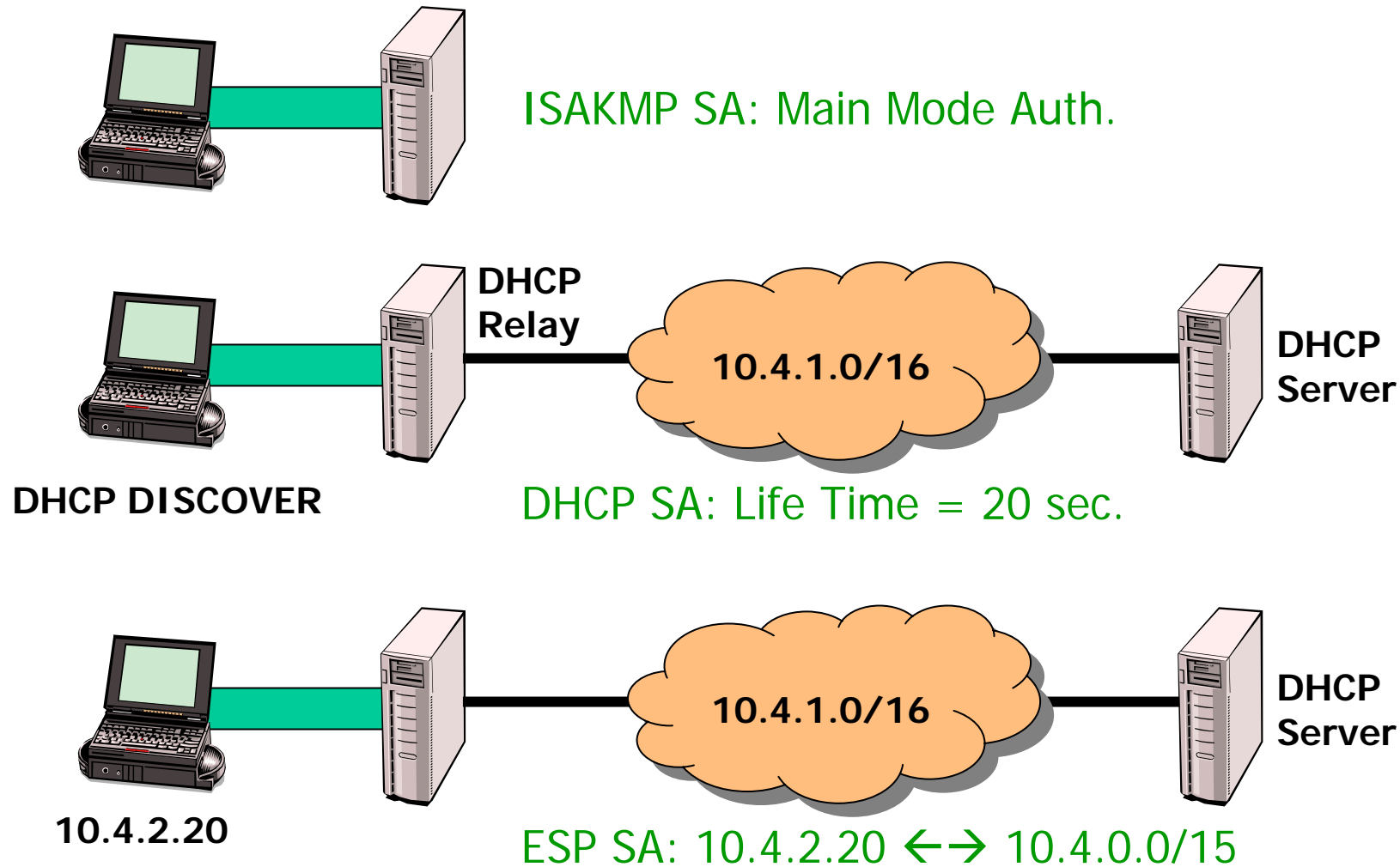


- The remote client authenticates himself on gw VPN
- The authentication is based on X.509 certificates
- The client acquire a private IP address with DCHP-over-IPSEC
- The remote client is part of the internal private network

VPN – DHCP-over-IPSec

tcom

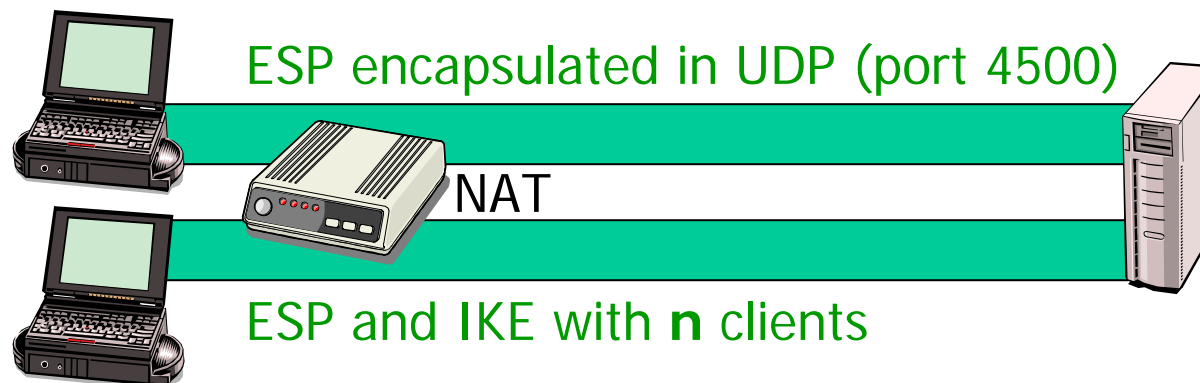
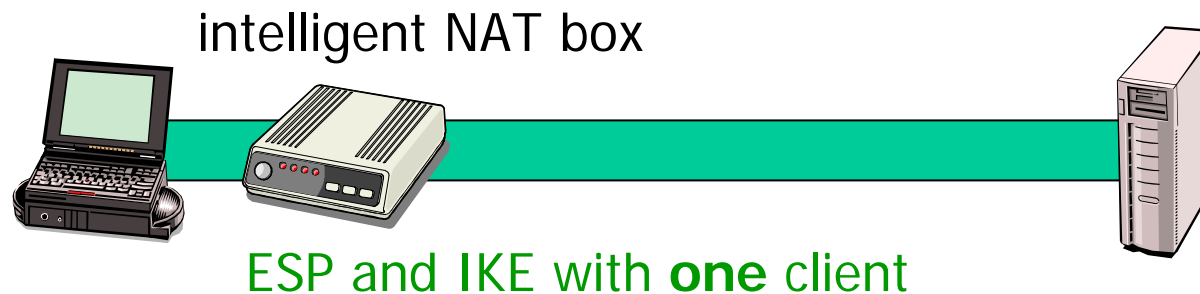
- Internet Draft: [draft-ietf-ipsec-dhcp-13.txt](#)

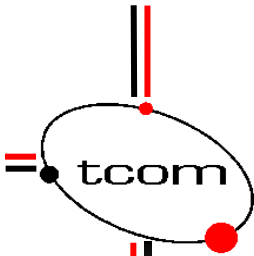


VPN – NAT-Traversal

tcom

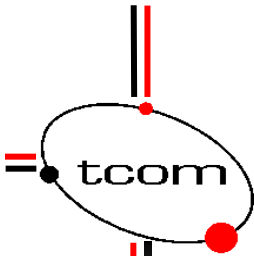
- Internet Drafts: [draft-ietf-ipsec-udp-encaps-03.txt](#)
[draft-ietf-ipsec-nat-t-03.txt](#)





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

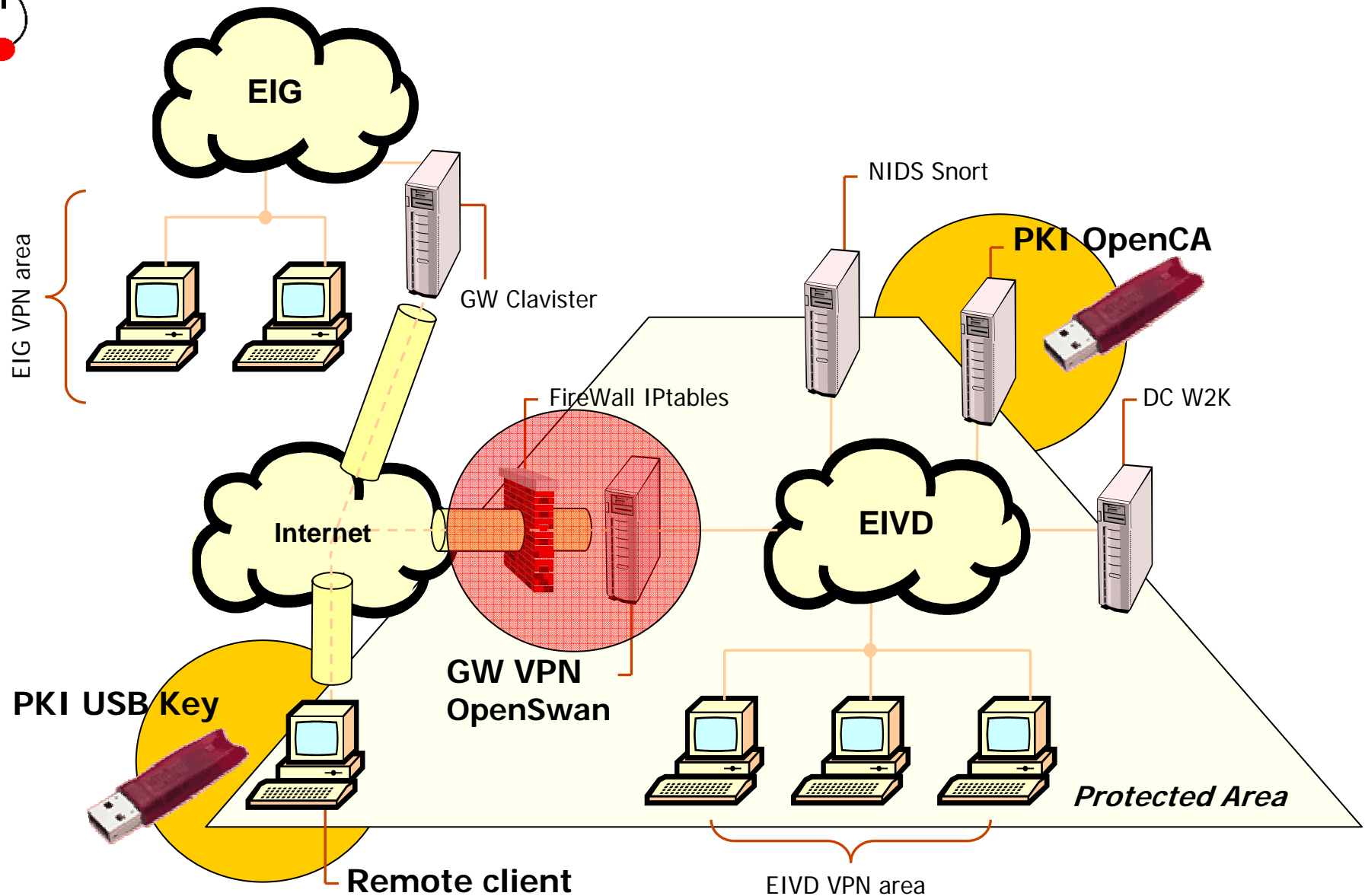
IPSEC – ESP (AH):

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

Other:

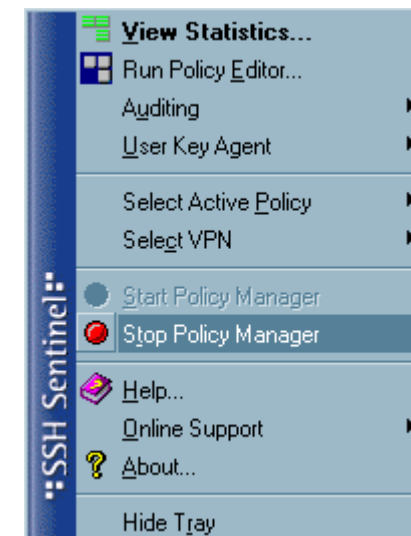
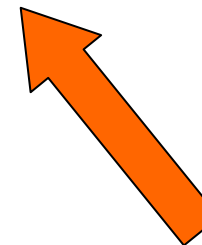
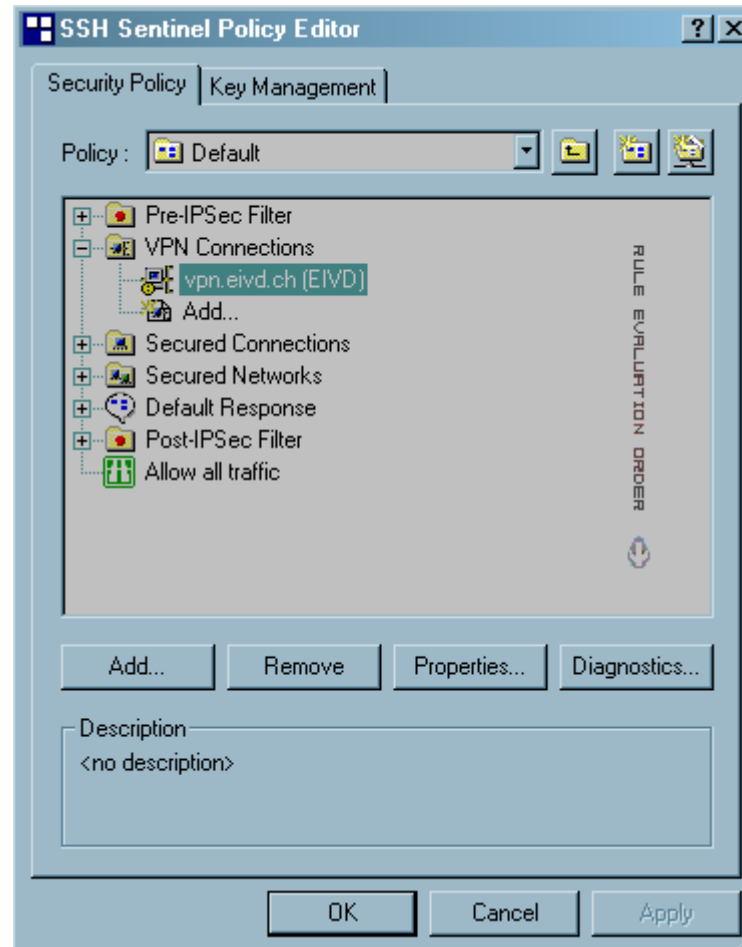
DHCP over IPSEC	OK
NAT-Traversal	OK

VPN – Final Architecture

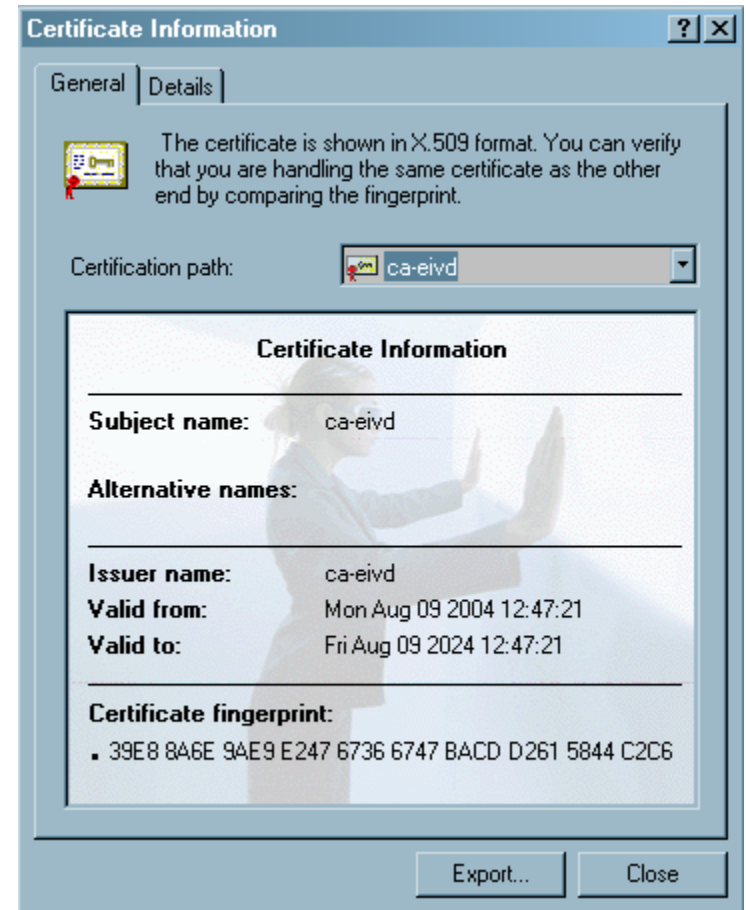
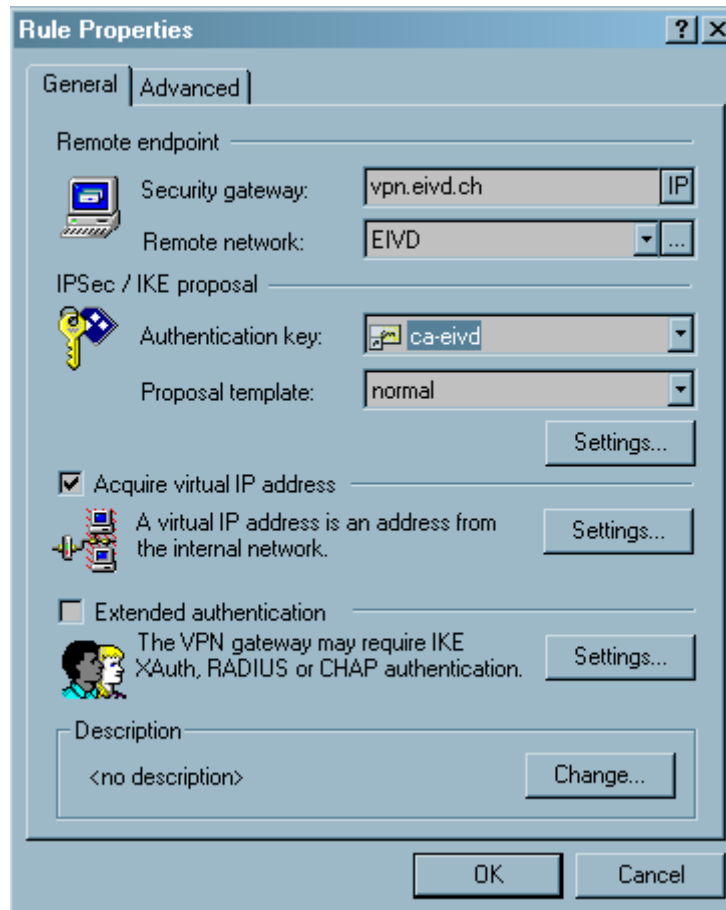


!!! Demonstration !!!

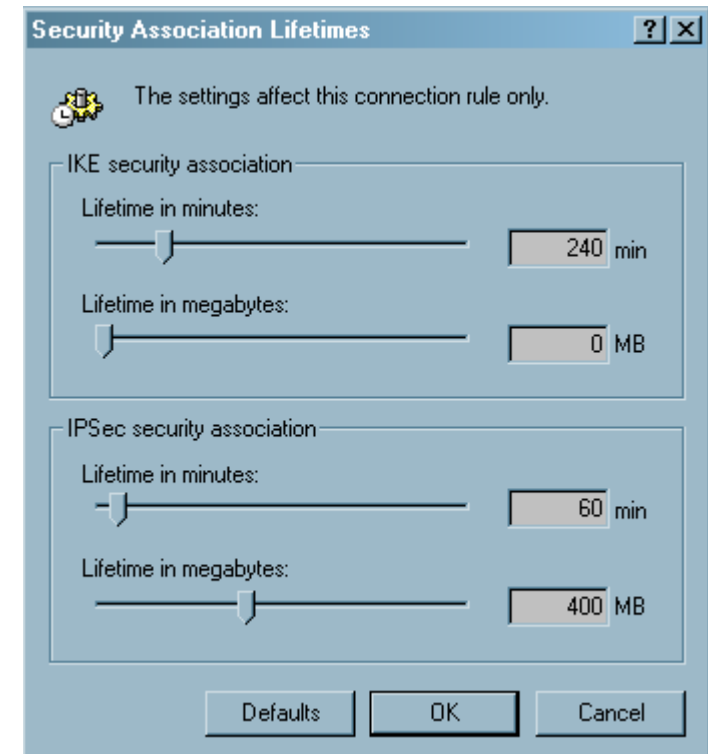
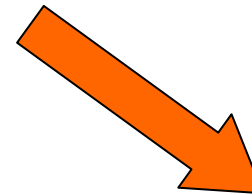
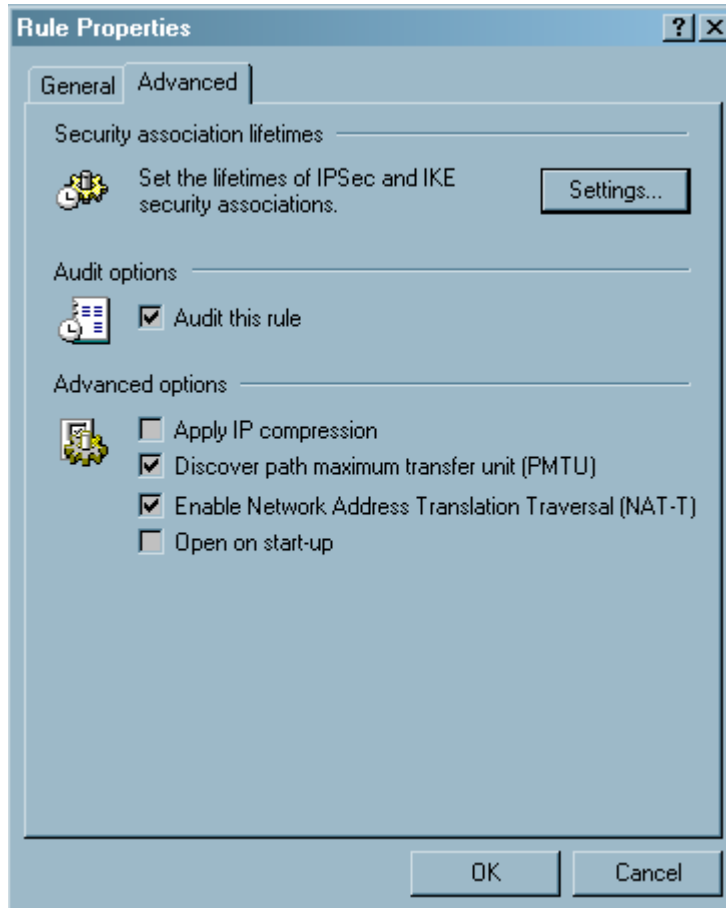
VPN – SSH Sentinel Configuration



VPN – PKI Certificate Configuration



VPN – SA Life & NAT Configuration



VPN – IKE & ESP Configuration

Proposal Parameters [?] [X]

Set the preferred value of each parameter of the IKE and IPSec proposal.

IKE proposal

Encryption algorithm: Rijndael

Integrity function: SHA-1

IKE mode: main mode

IKE group: MODP 1536 (group 5)

IPSec proposal

Encryption algorithm: Rijndael

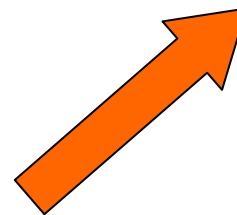
Integrity function: HMAC-SHA-1

IPSec mode: tunnel

PFS group: MODP 1536 (group 5)

☒ Attach only the selected values to the proposal

OK Cancel



Virtual IP Address [?] [X]

Choose the protocol for assigning the virtual IP address or configure the settings manually.

Protocol

☒ Dynamic Host Configuration Protocol (DHCP) over IPSec

☐ Layer Two Tunneling Protocol (L2TP)

☐ IKE Config Mode

☐ Specify manually:

IP address: . . .

Subnet mask: . . .

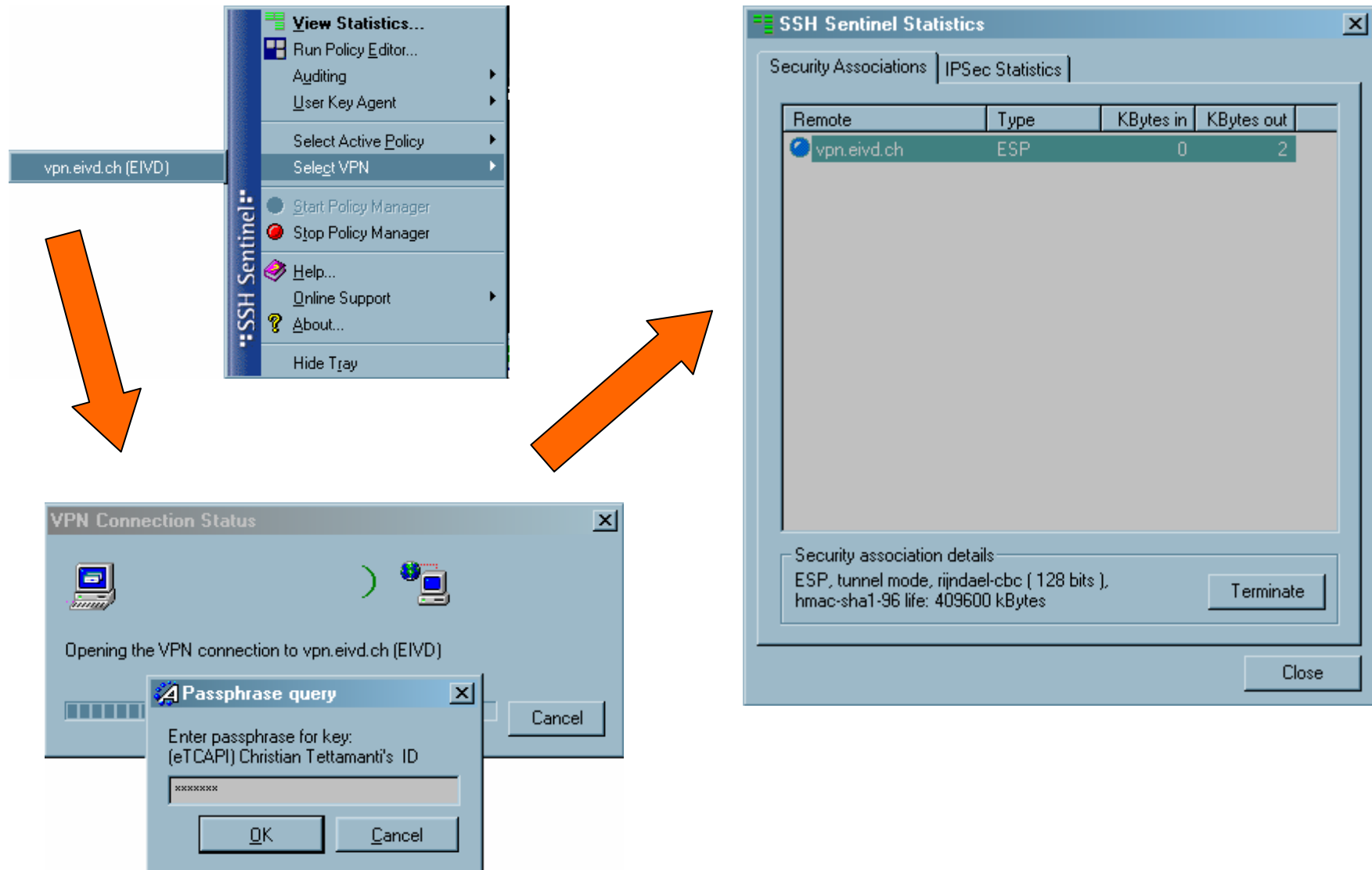
☐ Specify DNS and WINS servers:

DNS server: . . .

WINS server: . . .

OK Cancel

VPN – Connection example



VPN – Network Interfaces

Before VPN
Connection

```
C:\WINNT\system32\CMD.EXE

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.192.72.218
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.192.72.1

Ethernet adapter {8B02F934-CEED-4AE1-AEFD-AC100A4CC54F}:

    Media State . . . . . : Cable Disconnected

c:\>
```

After VPN
Connection

```
C:\WINNT\system32\CMD.EXE

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.192.72.218
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.192.72.1

Ethernet adapter {8B02F934-CEED-4AE1-AEFD-AC100A4CC54F}:

    Connection-specific DNS Suffix  . : vpn.eivd.ch
    IP Address. . . . . : 10.192.40.254
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

c:\>
```


??? Questions ???