

Ecole d'Ingénieurs du Canton de Vaud

VPN Solution

Christian Tettamanti

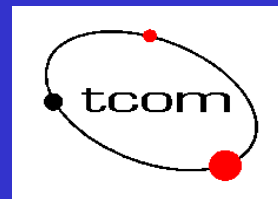
christian.tettamanti@eivd.ch

Stefano Ventura

stefano.ventura@eivd.ch

TCOM Institute

EIVD



VPN - Virtual Private Network

tcom

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

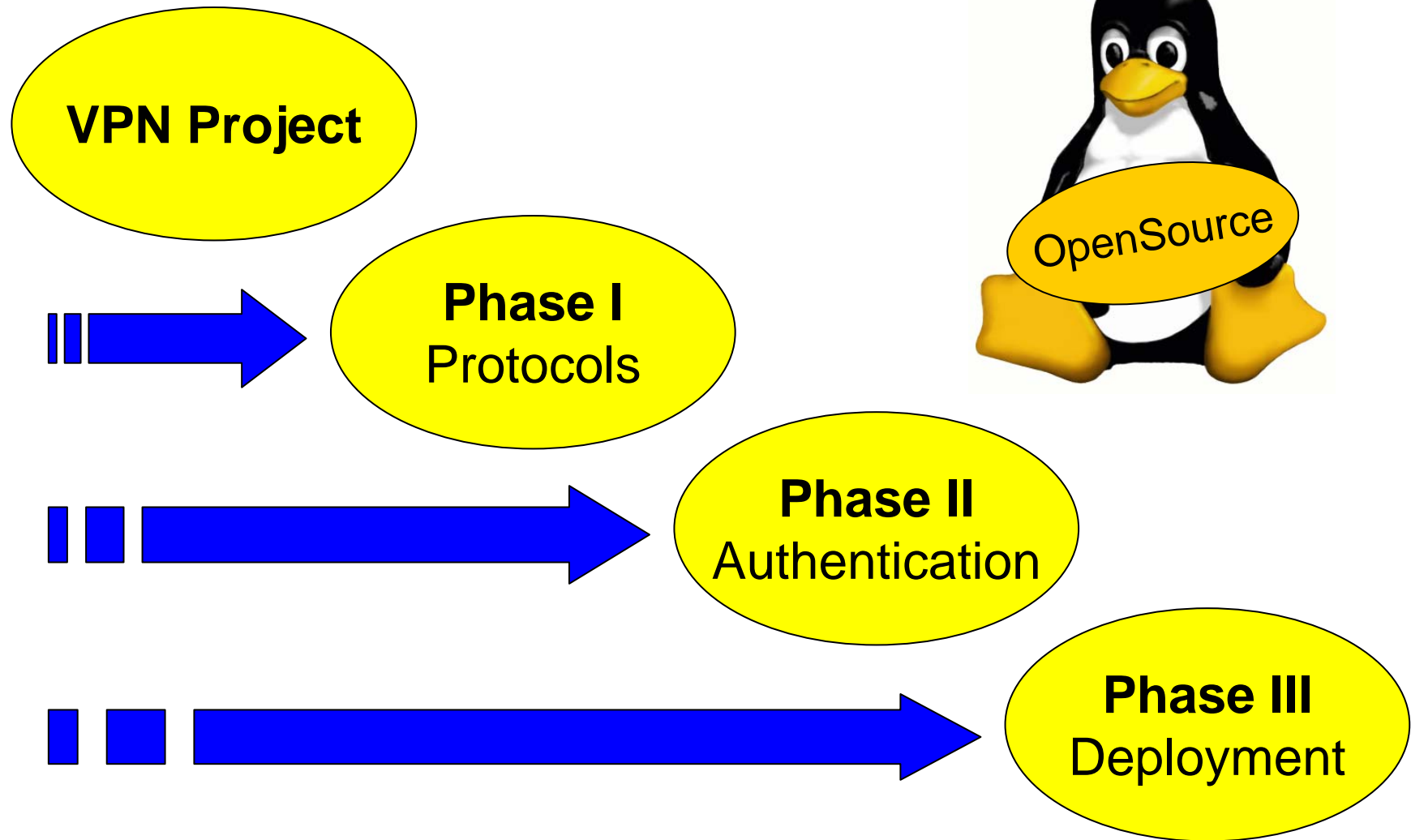
prof. HES
ing. HES
ing. HES



VPN - Goals Of The Project

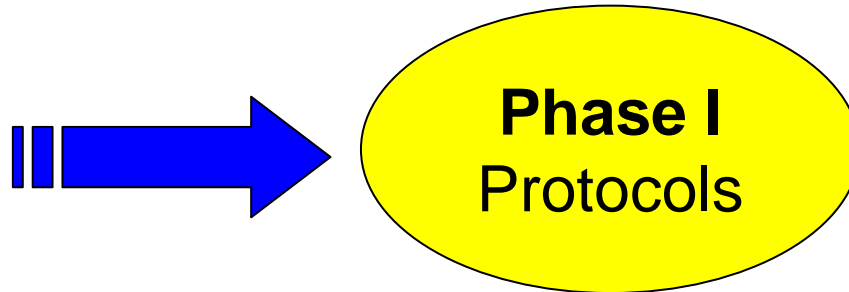
tcom

Christian Tettamanti, ing. HES



VPN - Goals Of The Project

tcom



- 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

tcom

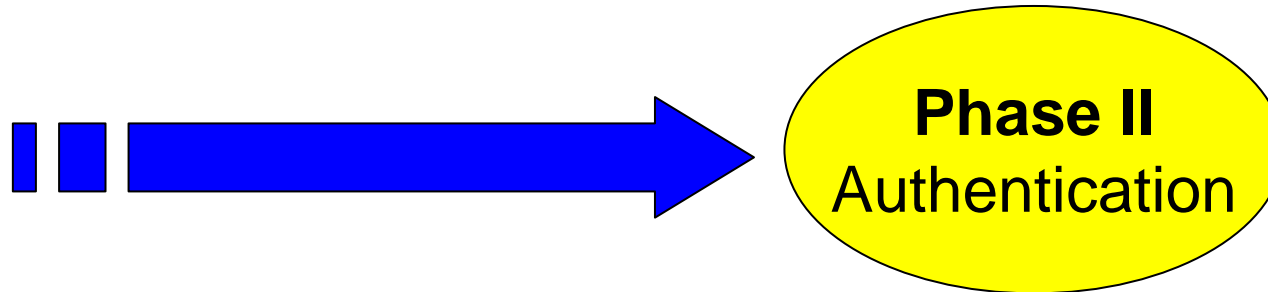
- Phase I

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

tcom



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



VPN - Goals Of The Project

tcom



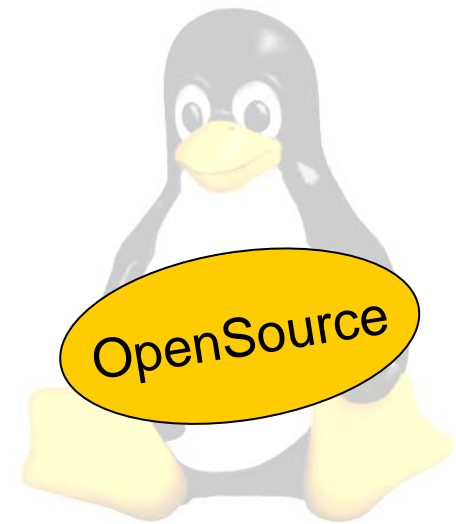
- Phase III
 - Deployment
 - LAN-to-LAN between EIG and TCOM
 - HOST-to-LAN at EIVD

VPN – Open Source Software

tcom

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



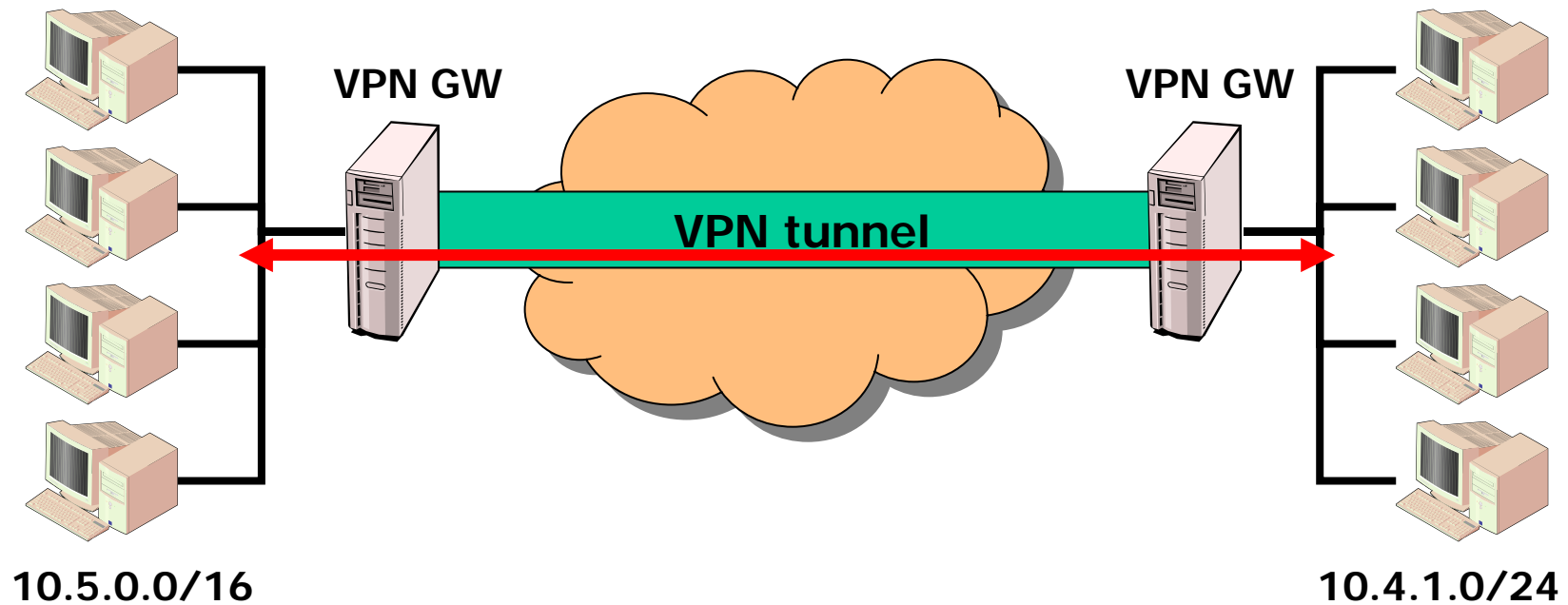
*Free License for universities

VPN – Scenario 1

tcom

EIG – Proprietary Solutions

EIVD – Open Source Solutions



VPN – Scenario 2

tcom

EIVD – Open Source Solutions

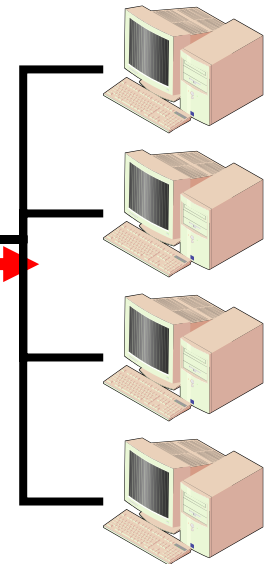
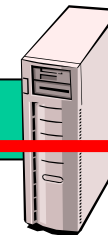
Remote Client



VPN Client
10.4.2.20

VPN tunnel

VPN GW



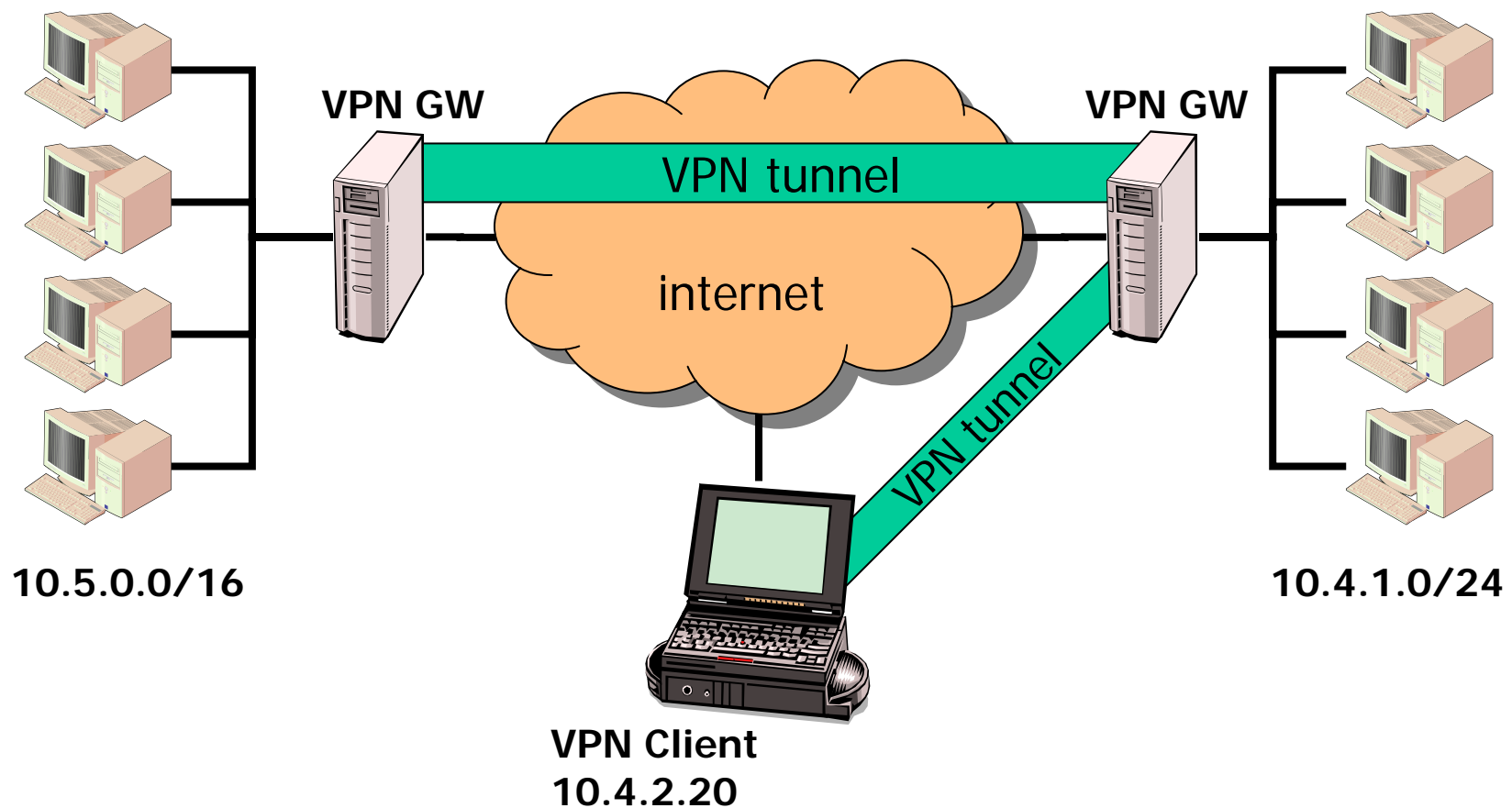
10.4.1.0/24

VPN – Scenario 3

tcom

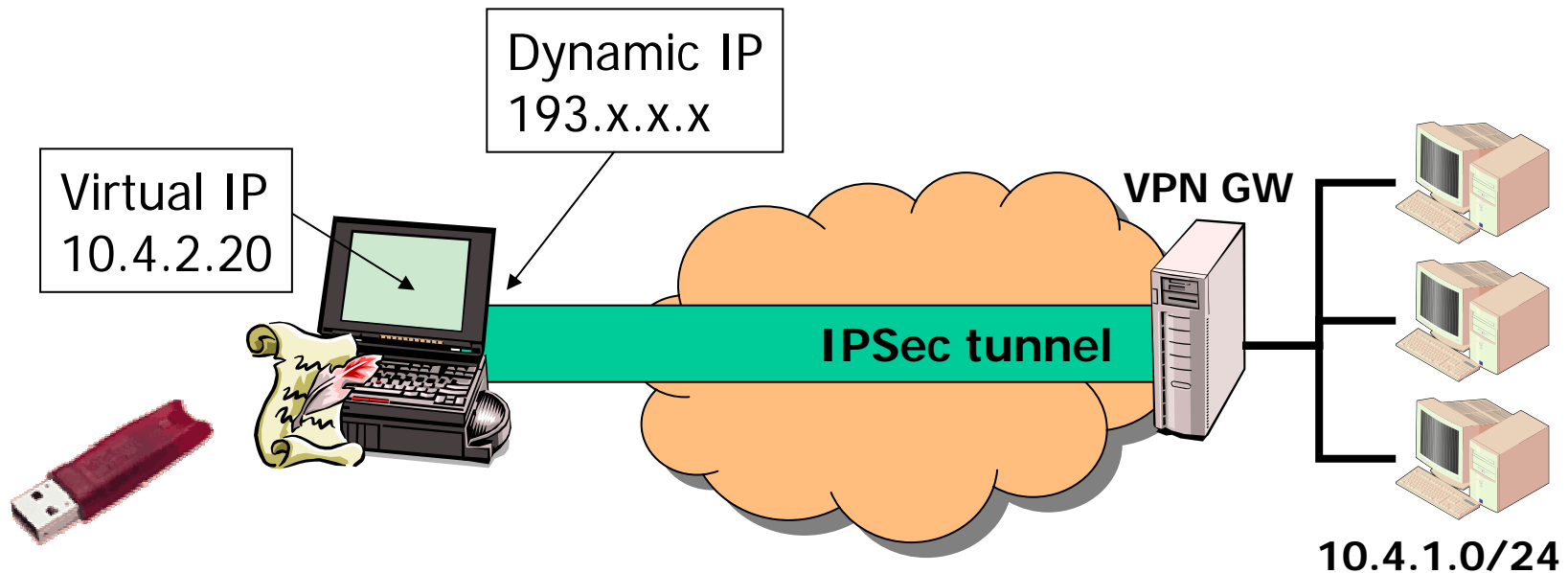
EIG – Proprietary Solutions

EIVD – Open Source Solutions



VPN – Remote Client Authentication

tcom

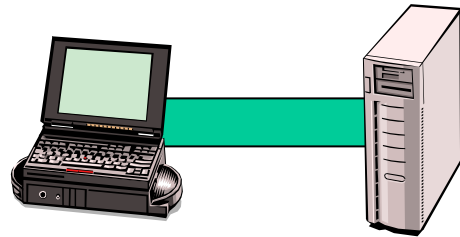


- The remote client authenticates himself on gw VPN
- The authentication is based on X.509 certificates
- The client acquire a private IP address with DCHP-over-IPSEC
- The remote client is part of the internal private network

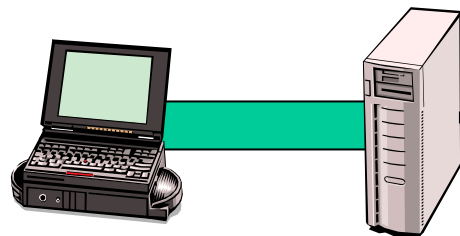
VPN – DHCP-over-IPSec

• tcom

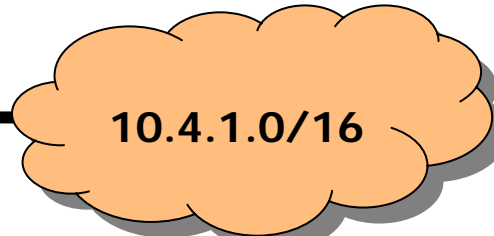
- Internet Draft: [draft-ietf-ipsec-dhcp-13.txt](#)



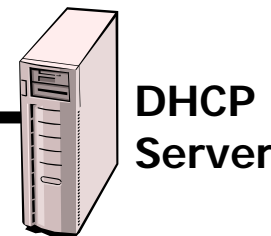
ISAKMP SA: Main Mode Auth.



DHCP
Relay



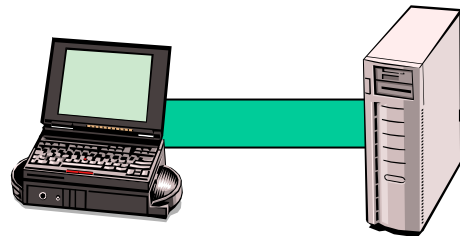
10.4.1.0/16



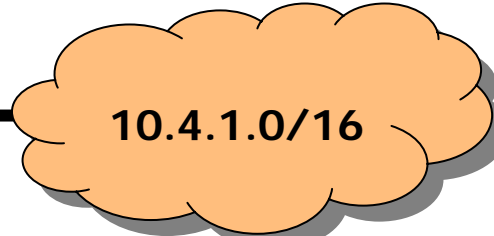
DHCP
Server

DHCP DISCOVER

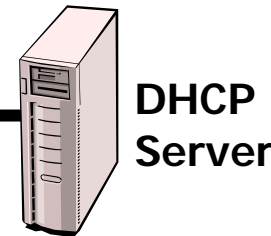
DHCP SA: Life Time = 20 sec.



10.4.2.20



10.4.1.0/16



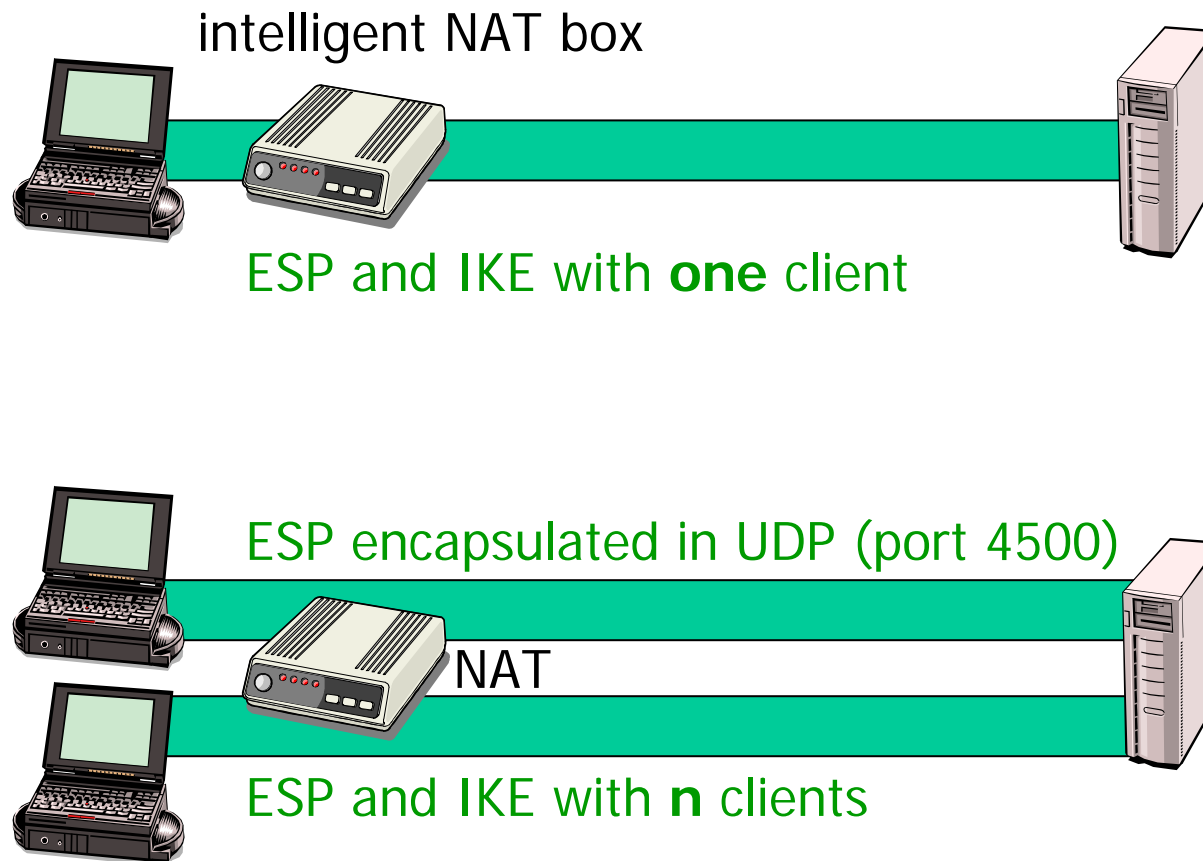
DHCP
Server

ESP SA: 10.4.2.20 ↔ 10.4.0.0/15

VPN – NAT-Traversal

tcom

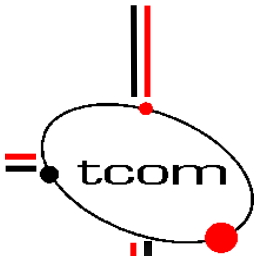
- Internet Drafts: [draft-ietf-ipsec-udp-encaps-03.txt](#)
[draft-ietf-ipsec-nat-t-03.txt](#)



VPN – Encountered Problems

tcom

- 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 |

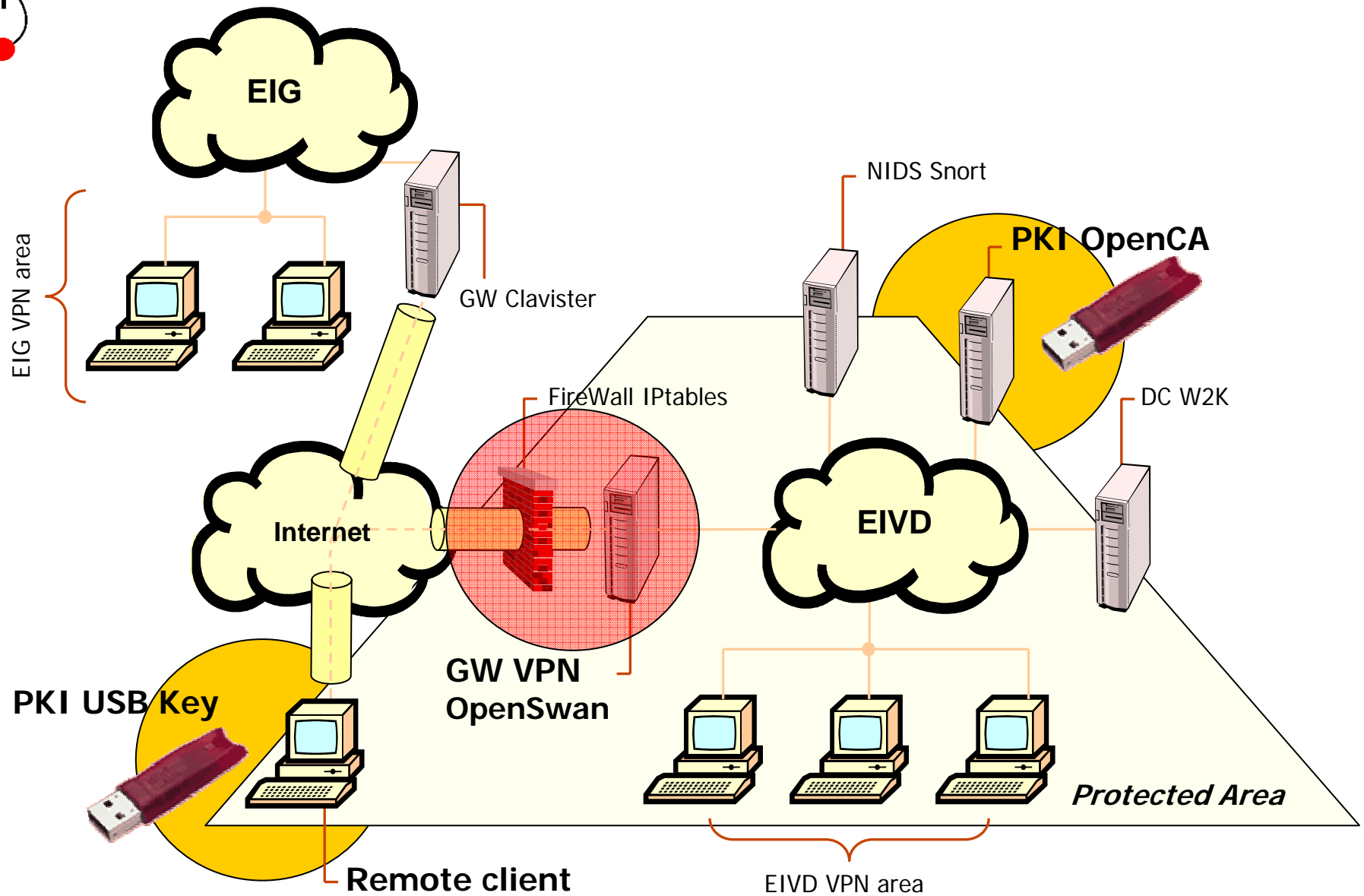
IPSEC – ESP (AH):

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

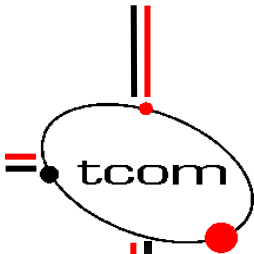
Other:

| | |
|-----------------|----|
| DHCP over IPSEC | OK |
| NAT-Traversal | OK |

VPN – Final Architecture

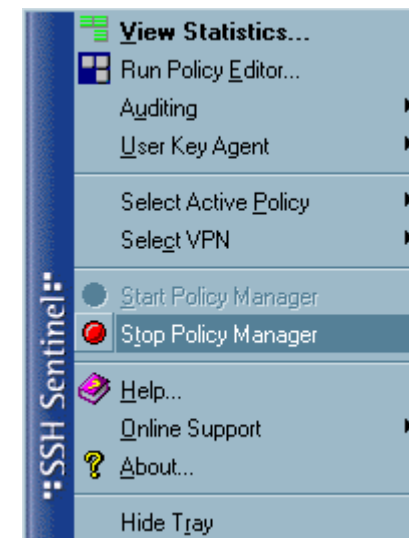
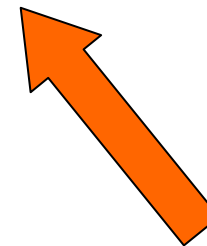
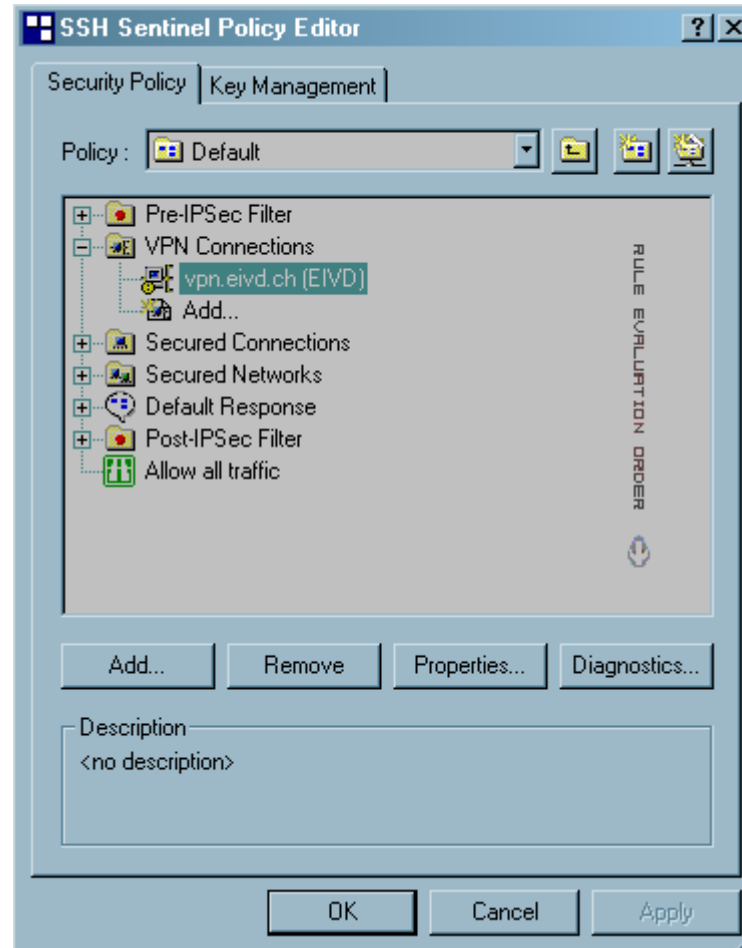


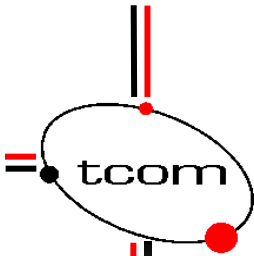
!!! Demonstration !!!



VPN – SSH Sentinel Configuration

Christian Tettamanti, ing. HES





VPN – PKI Certificate Configuration

Rule Properties [?] [X]

General | Advanced

Remote endpoint

Security gateway: vpn.eivd.ch [IP]

Remote network: EIVD [v] [...]

IPSec / IKE proposal

Authentication key: ca-eivd [v]

Proposal template: normal [v]

[Settings...]

Acquire virtual IP address

A virtual IP address is an address from the internal network. [Settings...]

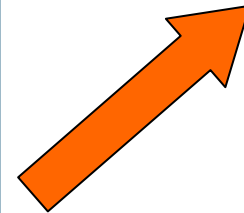
Extended authentication

The VPN gateway may require IKE XAuth, RADIUS or CHAP authentication. [Settings...]

Description

<no description> [Change...]

[OK] [Cancel]



Certificate Information [?] [X]

General | Details

The certificate is shown in X.509 format. You can verify that you are handling the same certificate as the other end by comparing the fingerprint.

Certification path: ca-eivd [v]

Certificate Information

Subject name: ca-eivd

Alternative names:

Issuer name: ca-eivd

Valid from: Mon Aug 09 2004 12:47:21

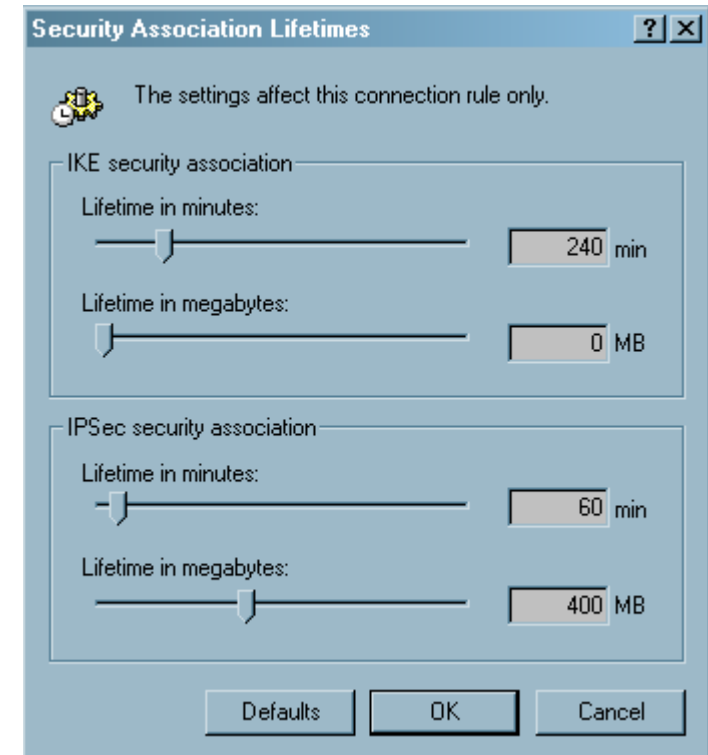
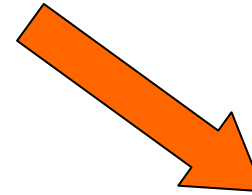
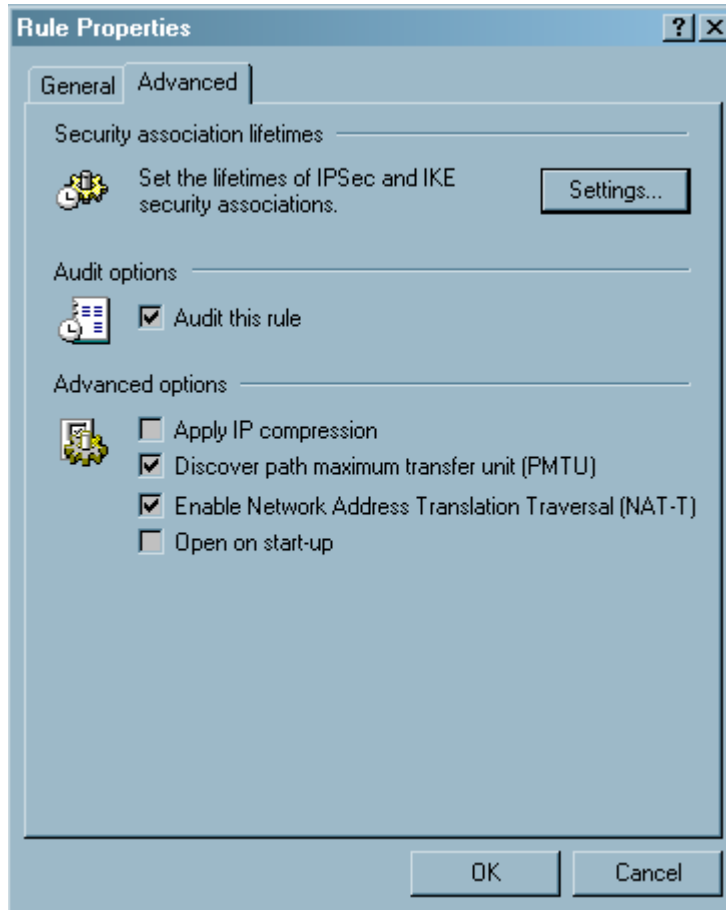
Valid to: Fri Aug 09 2024 12:47:21

Certificate fingerprint:

- 39E8 8A6E 9AE9 E247 6736 6747 BACD D261 5844 C2C6


[Export...] [Close]

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

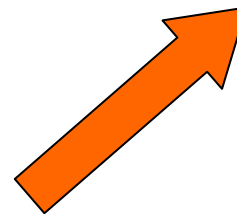
Integrity function: HMAC-SHA-1

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

The screenshot illustrates the process of establishing a VPN connection through the SSH Sentinel application. It shows three main windows:

- SSH Sentinel Main Window:** The 'Select VPN' menu item is highlighted, with a sub-menu showing 'vpn.eivd.ch (EIVD)' selected. An orange arrow points from this menu to the status window.
- VPN Connection Status Window:** Displays the progress of opening the VPN connection to 'vpn.eivd.ch (EIVD)'. A 'Passphrase query' dialog box is overlaid, asking for the passphrase for the key '(eTCAPI) Christian Tettamanti's ID'. An orange arrow points from this window to the statistics window.
- SSH Sentinel Statistics Window:** Shows the 'IPSec Statistics' tab with a table of active security associations.

| Remote | Type | KBytes in | KBytes out |
|-------------|------|-----------|------------|
| vpn.eivd.ch | ESP | 0 | 2 |

 Below the table, the 'Security association details' are shown: 'ESP, tunnel mode, rijndael-cbc (128 bits), hmac-sha1-96 life: 409600 kBytes'. Buttons for 'Terminate' and 'Close' are visible.

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 ???

???