

IPSec Tunnel

APPLICATION GUIDE





International Headquarters

B&B Electronics Mfg. Co. Inc.
707 Dayton Road
Ottawa, IL 61350 USA

Phone (815) 433-5100 -- **General Fax** (815) 433-5105
Website: www.bb-elec.com

European Headquarters

B&B Electronics Ltd.
Westlink Commercial Park
Oranmore, Co. Galway, Ireland

Phone +353 91-792444 -- **Fax** +353 91-792445
Website: www.bb-europe.com

Revision One – April 2013

Used symbols



Danger – important notice, which may have an influence on the user's safety or the function of the device.



Attention – notice on possible problems, which can arise in specific cases.



Information, notice – information, which contains useful advice or special interest.

©2013 B&B Electronics Mfg. Co. Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and does not represent a commitment on the part of B&B Electronics Mfg. Co. Inc.

GPL

B&B Electronics Mfg. Co. Inc. shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

License

Source codes under GPL license are available free of charge by sending an email to info@conel.cz.



**Declared quality system
ISO 9001**



Content

1. IPSEC PROTOCOL.....	6
1.1. Openswan.....	6
1.2. Restriction of the IPsec protocol with CISCO routers.....	6
1.3. Firewall changes.....	7
2. EXAMPLES OF USE THE IPSEC PROTOCOL.....	8
2.1. IPsec tunnel – initiator on the router.....	8
2.1.1. Router configuration via web browser.....	8
2.1.2. IPsec tunnel configuration in web interface.....	9
2.1.3. Detection of the successful establishment of an IPsec tunnel.....	10
2.2. IPsec tunnel – responder on the router.....	11
2.2.1. Router configuration via web browser.....	11
2.2.2. IPsec tunnel configuration in web interface.....	12
2.2.3. Detection of successful establishment of an IPsec tunnel.....	13
2.3. Using the IPsec tunnel – Linux server.....	14
2.4. Using the IPsec tunnel – CISCO router.....	15
2.4.1. Configuration – initiator on the router.....	15
2.4.2. Configuration – responder on the router.....	20
2.5. Using the IPsec tunnel – Windows.....	25
2.5.1. NCP Secure Entry Client program (version 9.23, build 18).....	25
2.5.2. Create a profile for IPsec tunnel establishing.....	26
2.5.3. IPsec tunnel configuration.....	26
2.5.4. Router setting.....	34
2.5.5. Connection successfully established.....	35
2.6. Using the IPsec tunnel – Mikrotik.....	36
2.6.1. Router setting.....	36
2.6.2. Mikrotik router setting.....	37
2.7. Using the IPsec tunnel – Lancom 1721.....	39
2.7.1. VPN – General.....	39
2.7.2. VPN – Defaults.....	41
2.7.3. VPN – IKE parameters.....	42
2.7.4. VPN – IKE Authorities.....	42
2.7.5. VPN – IPsec parameters.....	43
2.7.6. Router setting (Lancom 1721).....	44

Image list

Fig. 1: IPSec tunnel – initiator on the router.....	8
Fig. 2: Web interface for router configuration (initiator).....	8
Fig. 3: IPSec tunnel configuration (initiator)	9
Fig. 4: Information about IPSec tunnel (initiator).....	10
Fig. 5: IPSec tunnel – responder on the router.....	11
Fig. 6: Web interface for router configuration (responder)	11
Fig. 7: IPSec tunnel configuration (responder).....	12
Fig. 8: Information about IPSec tunnel (responder).....	13
Fig. 9: IPSec tunnel – Linux server	14
Fig. 10: Configuration file ipsec.conf.....	14
Fig. 11: Configuration file ipsec.secrets	14
Fig. 12: IPSec tunnel – CISCO router.....	15
Fig. 13: IPSec tunnel – Windows	25
Fig. 14: NCP Secure Entry Client.....	25
Fig. 15: Create a profile.....	26
Fig. 16: IPSec tunnel configuration.....	26
Fig. 17: Basic Settings	27
Fig. 18: Line Management	27
Fig. 19: IPSec General Settings.....	28
Fig. 20: Policy Editor I (IPSec Configuration).....	28
Fig. 21: Pre-shared Key (IPSec Configuration).....	29
Fig. 22: Policy Editor II (IPSec Configuration).....	29
Fig. 23: IPSec Policy (IPSec Configuration).....	30
Fig. 24: IPSec General Settings – final setting.....	30
Fig. 25: Advanced IPSec Options	31
Fig. 26: Identities.....	31
Fig. 27: IPSec Address Assignment.....	32
Fig. 28: Split Tunneling	32
Fig. 29: IP Network.....	33
Fig. 30: Split Tunneling – entered data.....	33
Fig. 31: Router setting (Windows).....	34
Fig. 32: Connection successfully established.....	35
Fig. 33: Ping 192.168.1.100.....	35

Fig. 34: Router setting (Mikrotik).....	36
Fig. 35: Mikrotik router setting.....	37
Fig. 36: IPSec Proposal.....	38
Fig. 37: IPSec – Installed Sas.....	38
Fig. 38: VPN – General.....	39
Fig. 39: Remote gateways.....	39
Fig. 40: Connection list – Edit Entry.....	40
Fig. 41: Connection parameters – Edit Entry.....	40
Fig. 42: VPN – Defaults.....	41
Fig. 43: VPN – IKE parameters.....	42
Fig. 44: IKE proposal lists.....	42
Fig. 45: VPN – IKE Authorities.....	42
Fig. 46: VPN – IPSec parameters.....	43
Fig. 47: IPSec proposal lists.....	43
Fig. 48: LANmonitor.....	43
Fig. 49: Router setting (Lancom 1721).....	44
Fig. 50: Information about IPSec tunnel (Lancom 1721).....	44

Table list

Tab. 1: IPSec tunnel setting (initiator)	10
Tab. 2: IPSec tunnel setting (responder).....	13

1. IPSec protocol

IPSec (Internet Protocol Security) is a protocol for securing IP communications by authenticating and/or encrypting each IP packet in the data flow.

- ⤴ **Authenticating** – Verifies whether the sent packet corresponds to the sender or whether the sender actually exists (Phase I, IKE phase, Main mode). In PSK 's case, an exchange of keys is performed at the end.
- ⤴ **Encrypting** – Both sides agree on the form of packet encrypting in advance. Then the entire packet will be encrypted, apart from the IP header. (Alternatively the entire packet is encrypted and then the new IP header is added). Phase II, IPSec phase, Quick mode. The tunnel is established at the end.

IPSec protocol includes protocols for secure exchange of keys. It works on the network layer of the OSI model.

NAT-T (or NAT-Traversal) is an acronym for Network Address Translation Traversal. It is a technology that is used to share one public IP address of a group of computers in the internal network with non-public IP range. NAT-T allows interconnection of private network using IPSec.

1.1. Openswan

Openswan Version 2.4.5 X.509-1.5.4 with Pluto daemon is implemented in the router. It offers the following parameters:

- ⤴ Simple and advanced options for configuring tunnels
- ⤴ Full RFC (AH, ESP, transport and tunnel mode)
- ⤴ Complete support for NAT-Traversal
- ⤴ Flexible encryption (based on public key in DNS/DNSSEC) with DHCP integration
- ⤴ Extended roadwarrior support (clients with dynamic IP)
- ⤴ The ability to run custom scripts
- ⤴ The original RSA keys (public keys are specified directly)
- ⤴ Extended use of X.509 certificates, CAs and intermediate CA treatment
- ⤴ Dynamic Certificate Revocation List (CRL) using FTP, HTTP or LDAP
- ⤴ Dead Peer Detection – check of accessibility of the other end of the tunnel
- ⤴ Aggressive mode support
- ⤴ Support for Windows L2TP via IPSec transport mode
- ⤴ Cooperation with many non-standard commercial implementations (software)
- ⤴ Implementation of all public known VENDOR-ID
- ⤴ Well portable source code fitting into many Linux platforms (MIPS, ARM, Sparc, Alpha)

1.2. Restriction of the IPSec protocol with CISCO routers



CISCO routers support IPSec protocol only, with IOS 7.1 and later. DH1 is not supported.

1.3. Firewall changes

- ⤴ V1.0.2 (14.2.2007):
IPSec tunnel configuration extended by parameters Rekey Margin and Rekey Fuzz (parameters of the keys expiration time)
- ⤴ v1.0.3 (22.3.2007):
Added support for entering the computer name in the configuration of the IPSec tunnel
- ⤴ v1.1.1 (27.5.2008)
Added support for IPSec X.509 certificates and NAT Traversal
- ⤴ v1.1.2 (25.8.2008)
Added support for three other IPSec tunnels
Added support for IPSec passthru (in transport mode)
- ⤴ v1.1.9 (15.5.2009)
Added support for aggressive mode at IPSec tunnel establishing
- ⤴ v2.0.0 (19.11.2009)
Added support for Dead Peer Detection for IPSec tunnels
- ⤴ v2.0.1 (27.1.2010)
Modified restart the IPSec tunnel and packets routing
- ⤴ v2.0.6 (26.10.2010)
Increased the limit for Rekey Margin parameter (this parameter determines the expiration time of keys)

2. Examples of use the IPSec protocol

2.1. IPSec tunnel – initiator on the router

The IP address of the SIM card inserted into the router can be static or dynamic, because IPSec tunnel connects to the initiator in the router. In this case the Linux/CISCO server offers services for IPSec tunnel. So it must be available on a static IP address or domain-name.

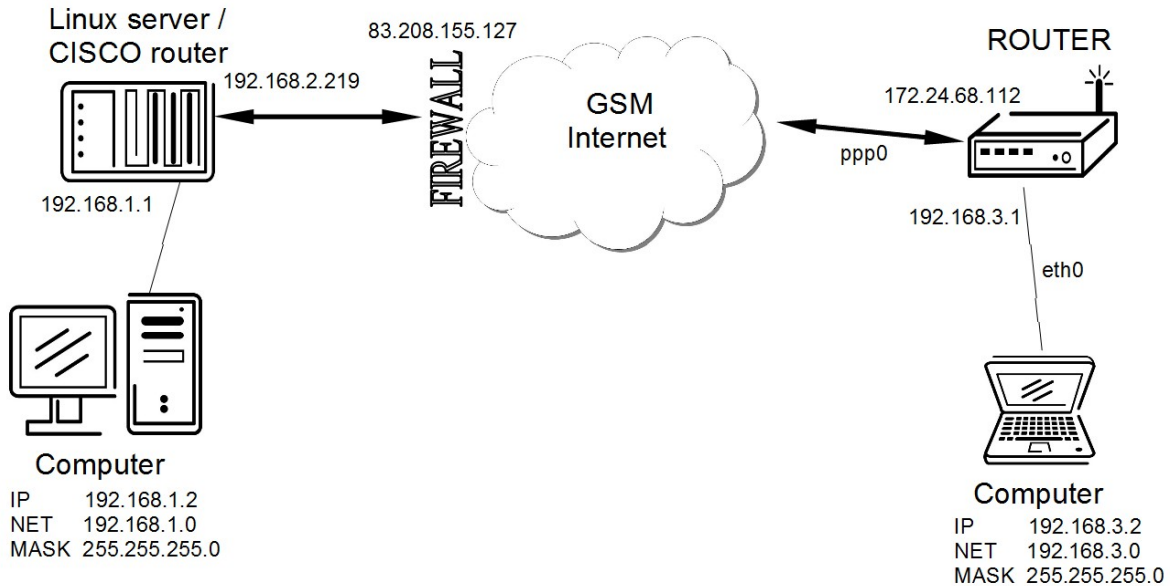


Fig. 1: IPSec tunnel – initiator on the router

2.1.1. Router configuration via web browser

Status Network DHCP GPRS IPsec DynDNS System Log Configuration LAN GPRS Firewall NAT IPsec GRE L2TP DynDNS NTP SMS PIN External Port Administration Change Password Set Real Time Clock Backup Configuration Restore Configuration Update Firmware Reboot	Network Status Interfaces eth0 Link encap:Ethernet HWaddr 00:CF:52:08:CF:01 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:236 errors:0 dropped:0 overruns:0 frame:0 TX packets:18 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:22767 (22.2 KB) TX bytes:6337 (6.1 KB)																
	Route Table <table border="1"> <thead> <tr> <th>Destination</th> <th>Gateway</th> <th>Genmask</th> <th>Flags</th> <th>Metric</th> <th>Ref</th> <th>Use</th> <th>Iface</th> </tr> </thead> <tbody> <tr> <td>192.168.1.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>0</td> <td>eth0</td> </tr> </tbody> </table>	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface										
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0										

Status information, configuration and administration of the router

Details of the selected function from the menu on the left. For example, information or configuration

Fig. 2: Web interface for router configuration (initiator)

2.1.2. IPSec tunnel configuration in web interface

IPsec Tunnel Configuration

Create 1st IPsec tunnel

Description *

Remote IP Address *

Remote ID *

Remote Subnet *

Remote Subnet Mask *

Local ID *

Local Subnet *

Local Subnet Mask *

Key Lifetime sec

IKE Lifetime sec

Rekey Margin sec

Rekey Fuzz %

DPD Delay * sec

DPD Timeout * sec

NAT Traversal

Aggressive Mode

Authenticate Mode

Pre-shared Key

CA Certificate

Remote Certificate

Local Certificate

Local Private Key

Local Passphrase *

Extra Options *

* can be blank

Fig. 3: IPSec tunnel configuration (initiator)

If addresses of tunnel ends are mutually visible, just set Remote IP address, Remote Subnet, Remote Subnet Mask, Local Subnet and Local Subnet Mask. If not (one end of the tunnel is in a private network), it is necessary to enable NAT Traversal.

It is also necessary to set Remote ID (if NAT-T is active). As the ID is usually filled FQDN, which is the designation for a fully specified domain-name of a computer (an acronym for the term **F**ully **Q**ualified **D**omain **N**ame). It is also possible to set up authentication using certificates, but then there is no need to enter the Remote ID.

There is an example of IPSec tunnel settings in the following table:

Item	Router
Remote External IP Address	83.208.155.127
Remote ID	ciscoasa@default.domain
Remote Subnet	192.168.1.0
Remote Subnet Mask	255.255.255.0
Local Subnet	192.168.3.0
Local Subnet Mask	255.255.255.0
Pre-shared Key	test
NAT Traversal	Enabled

Tab. 1: IPSec tunnel setting (initiator)

Other parameters can be left in default setting. If the parameter „Remote External IP Address“ on one side of the IPSec tunnel is empty, this side waits for a connection and doesn't attempt to establish a connection.

Items marked with * may be empty. These items are used to accurately identify the IPSec tunnel.

2.1.3. Detection of the successful establishment of an IPSec tunnel

```

IPsec Status
IPsec Tunnel Info

interface ipsec0/ppp0 172.24.68.112

"ipsec": 172.24.68.112...83.208.155.127===192.168.1.0/24
"ipsec": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec": policy: PSK+ENCRYPT+TUNNEL; interface: eth0; erouted
"ipsec": newest ISAKMP SA: #1; newest IPsec SA: #2; eroute owner: #2
"ipsec": IKE algorithms wanted: 5_000-1-5, 5_000-2-5, 5_000-1-2, 5_000-2-2, flags--strict
"ipsec": IKE algorithms found: 5_192-1_128-5, 5_192-2_160-5, 5_192-1_128-2, 5_192-2_160-2,
"ipsec": IKE algorithm newest: 3DES_CBC_192-MD5-MODP1024
"ipsec": ESP algorithms wanted: 3_000-1, 3_000-2, flags--strict
"ipsec": ESP algorithms loaded: 3/168-1/128, 3/168-2/160,
"ipsec": ESP algorithm newest: 3DES_0-HMAC_MD5; pfsgroup=

#2: "ipsec" STATE_QUICK_I2 (sent QI2, IPsec SA established); born:6790s; EVENT_SA_REPLACE in 2272s; newest IPSEC; eroute owner
#2: "ipsec" esp.f4609cc@83.208.155.127 esp.11286499@172.24.68.112 tun.1002@83.208.155.127 tun.1001@172.24.68.112
#1: "ipsec" STATE_MAIN_I4 (ISAKMP SA established); born:6788s; EVENT_SA_REPLACE in 2358s; newest ISAKMP

```

Fig. 4: Information about IPSec tunnel (initiator)

The previous figure shows the selected encryption in component stages for establishing the IPsec tunnel.

- ⤴ IKE: 3DES_CBC_192-MD5-MODP1536
- ⤴ IPsec: 3DES_0-HMAC_MD5, pfsgroup = none

In the highlighted part of this figure you can see that the tunnel is successfully established.

2.2. IPsec tunnel – responder on the router

If you are using dynamically assigned IP addresses for the DynDNS domain name, the router must have an available static IP address or dynamic IP address of inserted SIM card. In this case Linux/CISCO server is the initiator and it establishes an IPsec tunnel.

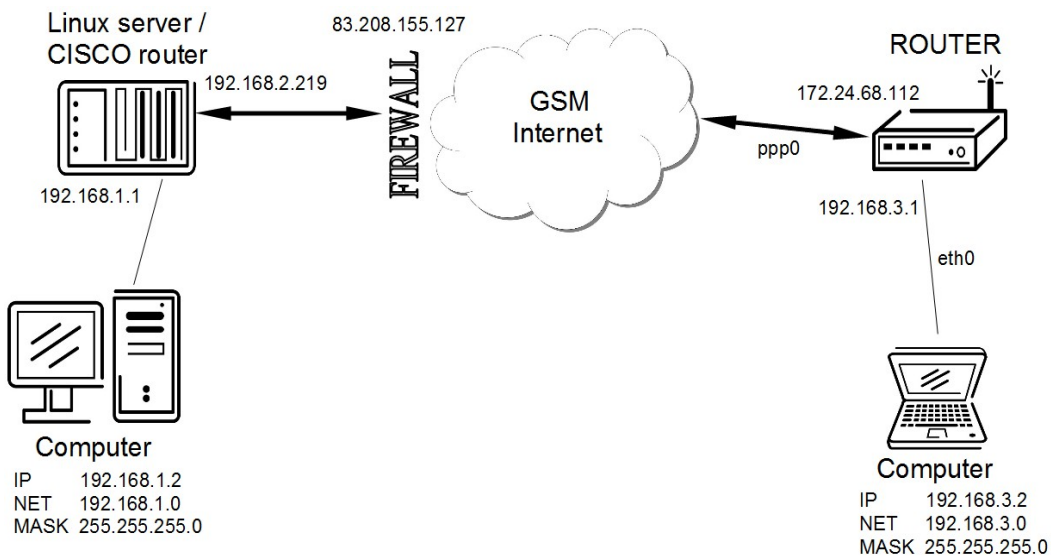


Fig. 5: IPsec tunnel – responder on the router

2.2.1. Router configuration via web browser

Status	Network Status
Network	Interfaces
DHCP	
GPRS	
IPsec	eth0 Link encap:Ethernet HWaddr 00:CF:52:08:CF:01 inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:236 errors:0 dropped:0 overruns:0 frames:0 TX packets:18 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:22767 (22.2 KB) TX bytes:6337 (6.1 KB)
DynDNS	Route Table
System Log	
Configuration	
LAN	
GPRS	
Firewall	
NAT	
IPsec	
GRE	
L2TP	
DynDNS	
NTP	
SMS	
PIN	
External Port	
Administration	
Change Password	
Set Real Time Clock	
Backup Configuration	
Restore Configuration	
Update Firmware	
Reboot	

Fig. 6: Web interface for router configuration (responder)

2.2.2. IPSec tunnel configuration in web interface

IPsec Tunnel Configuration

Create 1st IPsec tunnel

Description *

Remote IP Address *

Remote ID *

Remote Subnet *

Remote Subnet Mask *

Local ID *

Local Subnet *

Local Subnet Mask *

Key Lifetime sec

IKE Lifetime sec

Rekey Margin sec

Rekey Fuzz %

DPD Delay * sec

DPD Timeout * sec

NAT Traversal ▼

Aggressive Mode ▼

Authenticate Mode ▼

Pre-shared Key

CA Certificate

Remote Certificate

Local Certificate

Local Private Key

Local Passphrase *

Extra Options *

* can be blank

Fig. 7: IPSec tunnel configuration (responder)

If addresses of tunnel ends are mutually visible, just set Remote IP address, Remote Subnet, Remote Subnet Mask, Local Subnet and Local Subnet Mask. If not (one end of the tunnel is in a private network), it is necessary to enable NAT Traversal.

It is also necessary to set Remote ID (if NAT-T is active). As the ID is usually filled FQDN, which is the designation for a fully specified domain-name of a computer (an acronym for the term **Fully Qualified Domain Name**). It is also possible to set up authentication using certificates, but then there is no need to enter the Remote ID.

There is given an example of IPsec tunnel setting in the following table:

Item	Router
Remote ID	ciscoasa@default.domain
Remote Subnet	192.168.2.219
Remote Subnet Mask	255.255.255.255
Pre-shared Key	test
NAT Traversal	Enabled

Tab. 2: IPsec tunnel setting (responder)

Other parameters can be left in default setting. If the parameter „Remote External IP Address“ on one side of the IPsec tunnel is empty, this side waits for a connection and doesn't attempt to establish a connection.

Items marked with * may be empty. These items are used to accurately identify the IPsec tunnel.

2.2.3. Detection of successful establishment of an IPsec tunnel

```

IPsec Status
IPsec Tunnel Info

interface ipsec0/ppp0 172.24.68.112

"ipsec": 172.24.68.112...83.208.155.127===192.168.1.0/24
"ipsec": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec": policy: PSK+ENCRYPT+TUNNEL; interface: eth0; erouted
"ipsec": newest ISAKMP SA: #1; newest IPsec SA: #2; eroute owner: #2
"ipsec": IKE algorithms wanted: 5_000-1-5, 5_000-2-5, 5_000-1-2, 5_000-2-2, flags--strict
"ipsec": IKE algorithms found: 5_192-1_128-5, 5_192-2_160-5, 5_192-1_128-2, 5_192-2_160-2,
"ipsec": IKE algorithm newest: 3DES_CBC_192-MD5-MODP1024
"ipsec": ESP algorithms wanted: 3_000-1, 3_000-2, flags--strict
"ipsec": ESP algorithms loaded: 3/168-1/128, 3/168-2/160,
"ipsec": ESP algorithm newest: 3DES_0-HMAC_MD5; pfsgroup=

#2: "ipsec" STATE_QUICK_I2 (sent QI2, IPsec SA established); born:6790s; EVENT_SA_REPLACE in 2272s; newest IPSEC; eroute owner
#2: "ipsec" esp.f4609cc@83.208.155.127 esp.11286499@172.24.68.112 tun.1002@83.208.155.127 tun.1001@172.24.68.112
#1: "ipsec" STATE_MAIN_I4 (ISAKMP SA established); born:6788s; EVENT_SA_REPLACE in 2358s; newest ISAKMP

```

Fig. 8: Information about IPsec tunnel (responder)

The previous figure shows the selected encryption in component stages of establishing the IPsec tunnel.

- ⤴ IKE: 3DES_CBC_192-MD5-MODP1536
- ⤴ IPsec: 3DES_0-HMAC_MD5, pfsgroup = none

In the highlighted part of this figure you can see that the tunnel is successfully established.

2.3. Using the IPSec tunnel – Linux server

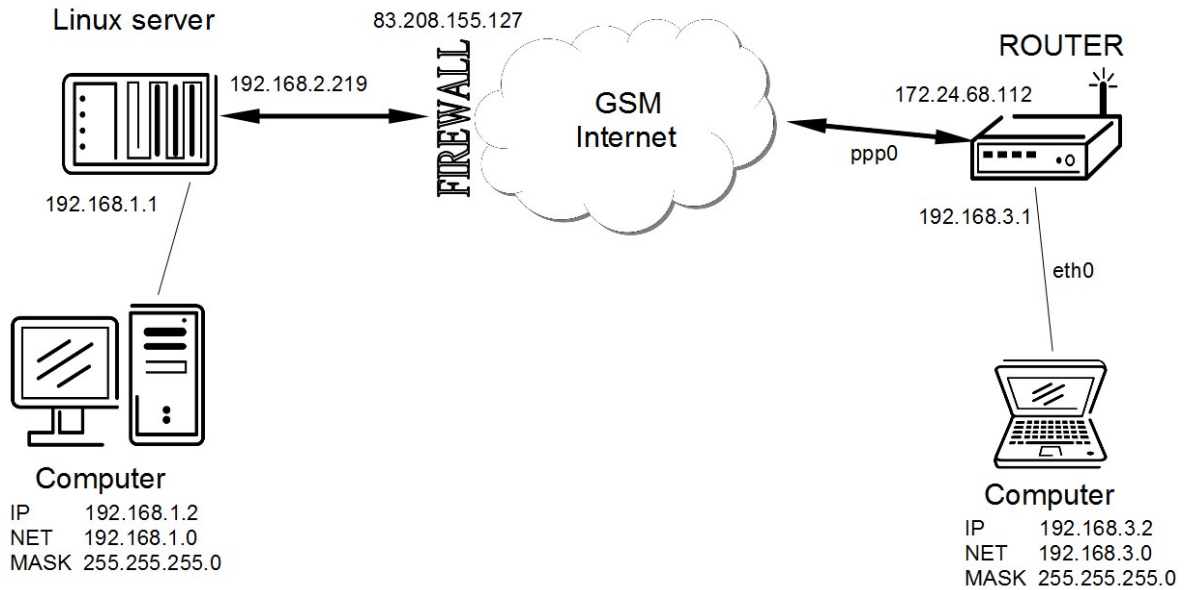


Fig. 9: IPSec tunnel – Linux server

It is necessary to set the configuration file *ipsec.conf*.

```
conn conelur
    authby=secret
    type=tunnel
    left=83.208.155.127
    leftsubnet=192.168.1.0/24
    right=172.24.68.112
    rightsubnet=192.168.3.0/24
    ikelifetime=3600s
    keylife=3600s
    pfs=no
    auto=add
```

Fig. 10: Configuration file ipsec.conf

It is also necessary to set the configuration file *ipsec.secrets*.

```
83.208.155.127 172.24.68.112 :PSK "test"
```

Fig. 11: Configuration file ipsec.secrets.

2.4. Using the IPSec tunnel – CISCO router

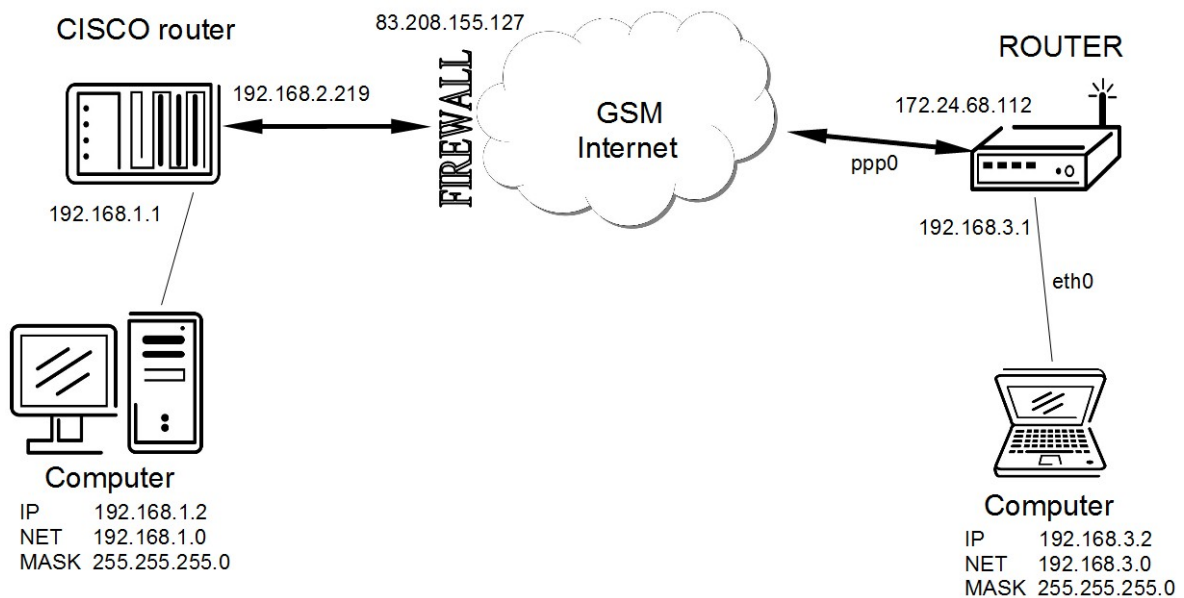


Fig. 12: IPSec tunnel – CISCO router



ATTENTION!!! CISCO routers support IPSec protocol only, with IOS 7.1 and later.

2.4.1. Configuration – initiator on the router

```
ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 100
 ip address 192.168.2.219 255.255.255.0
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
```

```

interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
passwd 2KFQnbNIdl.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain
same-security-traffic permit inter-interface
access-list outside_access_in extended permit ip any any
access-list outside_access_out extended permit ip any any
access-list inside_access_in extended permit ip any any
access-list inside_access_out extended permit ip any any
access-list outside_2_cryptomap extended permit ip 192.168.1.0 255.255.255.0
192.168.3.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
logging class auth asdm emergencies
logging class ip asdm critical
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-523.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
access-group inside_access_in in interface inside
access-group inside_access_out out interface inside
access-group outside_access_in in interface outside
access-group outside_access_out out interface outside
route outside 0.0.0.0 0.0.0.0 192.168.2.27 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

```

```

crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set UR1 esp-3des esp-none
crypto ipsec transform-set UR2 esp-des esp-none
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto map outside_map 1 match address outside_2_cryptomap
crypto map outside_map 1 set connection-type answer-only
crypto map outside_map 1 set peer 172.24.68.112
crypto map outside_map 1 set transform-set ESP-3DES-MD5
crypto map outside_map interface outside
crypto isakmp identity hostname
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 3600
crypto isakmp nat-traversal 20
vpn-sessiondb max-session-limit 1
telnet timeout 5
ssh timeout 5
console timeout 0
l2tp tunnel hello 300
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras

```

inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ipsec-pass-thru
!
service-policy global_policy global
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5
group-policy DfltGrpPolicy attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout none
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp enable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout none
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable

```
nac disable
nac-sq-period 300
nac-reval-period 36000
nac-default-acl none
address-pools none
smartcard-removal-disconnect enable
client-firewall none
client-access-rule none
webvpn
  functions none
html-content-filter none
  homepage none
  keep-alive-ignore 4
  http-comp gzip
  filter none
  url-list none
  customization value DfltCustomization
port-forward none
port-forward-name value Application Access
sso-server none
deny-message value Login was successful, but because certain criteria have not
been met or due to some specific group policy, you do not have permission to use
any of the VPN features. Contact your IT administrator for more information
svc none
svc keep-installer installed
svc keepalive none
svc rekey time none
svc rekey method none
svc dpd-interval client none
svc dpd-interval gateway none
svc compression deflate
tunnel-group DefaultL2LGroup ipsec-attributes
  pre-shared-key *
isakmp keepalive threshold 20 retry 10
tunnel-group 172.24.68.112 type ipsec-l2l
tunnel-group 172.24.68.112 ipsec-attributes
  pre-shared-key *
tunnel-group-map enable rules
tunnel-group-map default-group DefaultL2LGroup
prompt hostname context
no compression svc http-comp
zonelabs-integrity fail-timeout 20
Cryptochecksum:57784235ddef16872374b10e67a1415d
: end
```

2.4.2. Configuration – responder on the router

```
ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 100
 ip address 192.168.2.219 255.255.255.0
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
passwd 2KFQnbNIdl.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain
same-security-traffic permit inter-interface
access-list outside_access_in extended permit ip any any
access-list outside_access_out extended permit ip any any
access-list inside_access_in extended permit ip any any
access-list inside_access_out extended permit ip any any
access-list outside_2_cryptomap extended permit ip 192.168.1.0 255.255.255.0 192
.168.3.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
logging class auth asdm emergencies
logging class ip asdm critical
```

```

mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-523.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
access-group inside_access_in in interface inside
access-group inside_access_out out interface inside
access-group outside_access_in in interface outside
access-group outside_access_out out interface outside
route outside 0.0.0.0 0.0.0.0 192.168.2.27 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac crypto ipsec
transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac crypto ipsec
transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec
transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac crypto ipsec
transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac crypto ipsec
transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac crypto ipsec
transform-set UR1 esp-3des esp-none
crypto ipsec transform-set UR2 esp-des esp-none
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto map outside_map 1 match address outside_2_cryptomap
crypto map outside_map 1 set connection-type originate-only
crypto map outside_map 1 set peer 172.24.68.112
crypto map outside_map 1 set transform-set ESP-3DES-MD5
crypto map outside_map interface outside
crypto isakmp identity hostname
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 3600
crypto isakmp nat-traversal 20
vpn-sessiondb max-session-limit 1
telnet timeout 5

```

```

ssh timeout 5
console timeout 0
l2tp tunnel hello 300
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
!
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ipsec-pass-thru
!
service-policy global_policy global
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout none
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

```

password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp enable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout none
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
nac disable
nac-sq-period 300
nac-reval-period 36000
nac-default-acl none
address-pools none
smartcard-removal-disconnect enable
client-firewall none
client-access-rule none
webvpn
functions none
html-content-filter none
homepage none
keep-alive-ignore 4
http-comp gzip
filter none
url-list none
customization value DfltCustomization
port-forward none
port-forward-name value Application Access
sso-server none
deny-message value Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information
svc none
svc keep-installer installed
svc keepalive none
svc rekey time none

```
svc rekey method none
svc dpd-interval client none
svc dpd-interval gateway none
svc compression deflate
tunnel-group DefaultL2LGroup ipsec-attributes
pre-shared-key *
isakmp keepalive threshold 20 retry 10
tunnel-group 172.24.68.112 type ipsec-l2l
tunnel-group 172.24.68.112 ipsec-attributes
pre-shared-key *
tunnel-group-map enable rules
tunnel-group-map default-group DefaultL2LGroup
prompt hostname context
no compression svc http-comp
zonelabs-integrity fail-timeout 20
Cryptochecksum:3745a840258fc10269e066655f5b252e
: end
```

2.5. Using the IPSec tunnel – Windows



Recommended program for IPSec in Windows is NCP Secure Entry Client.

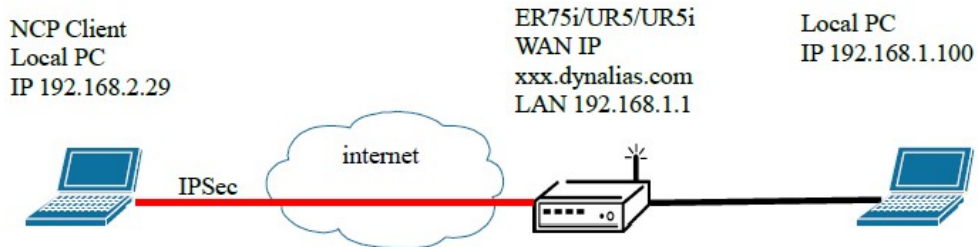


Fig. 13: IPSec tunnel – Windows

2.5.1. NCP Secure Entry Client program (version 9.23, build 18)



Obr. 14: NCP Secure Entry Client

2.5.2. Create a profile for IPsec tunnel establishing

Select *Configuration* item in the menu of the opening window of NCP Secure Entry Client (see previous figure) and then select *profiles*.

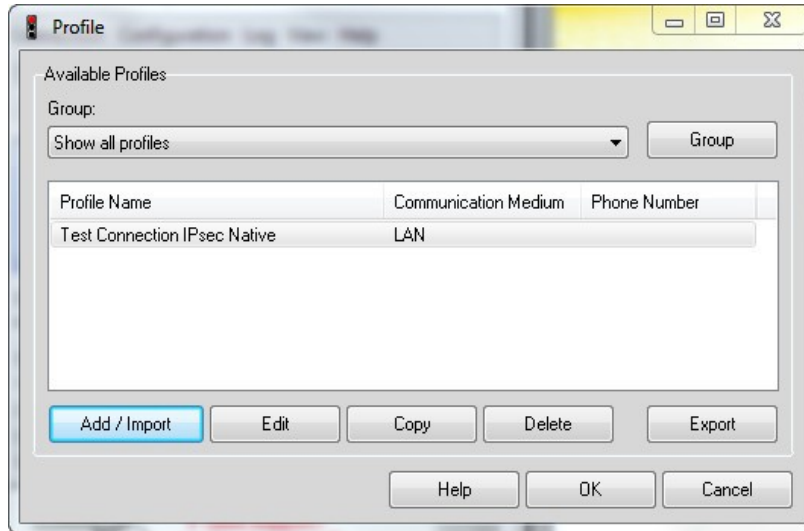


Fig. 15: Create a profile

Add a new profile by pressing the *Add/Import* button. Enter a profile name and on all screens only confirm by clicking on the *Next* (last on the *Finish*) button.

2.5.3. IPsec tunnel configuration

In the window that you used to creat the profile for IPsec tunnel establishing, click the *Edit* button.

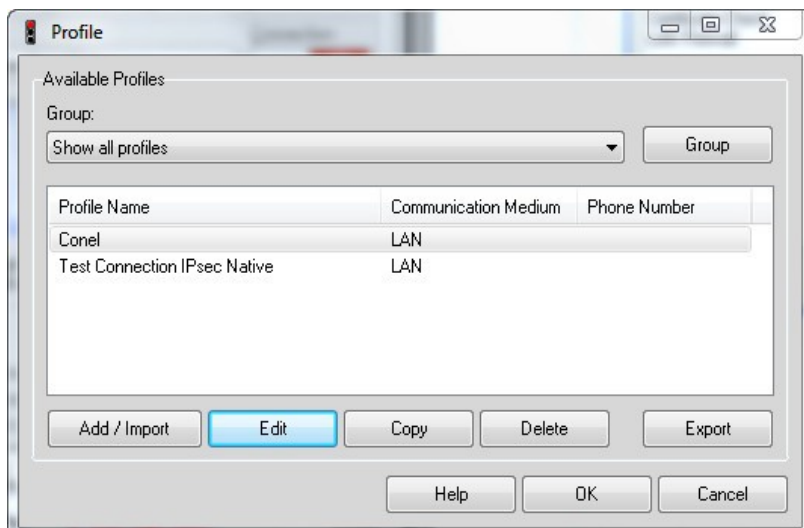


Fig. 16: IPsec tunnel configuration

Basic Settings

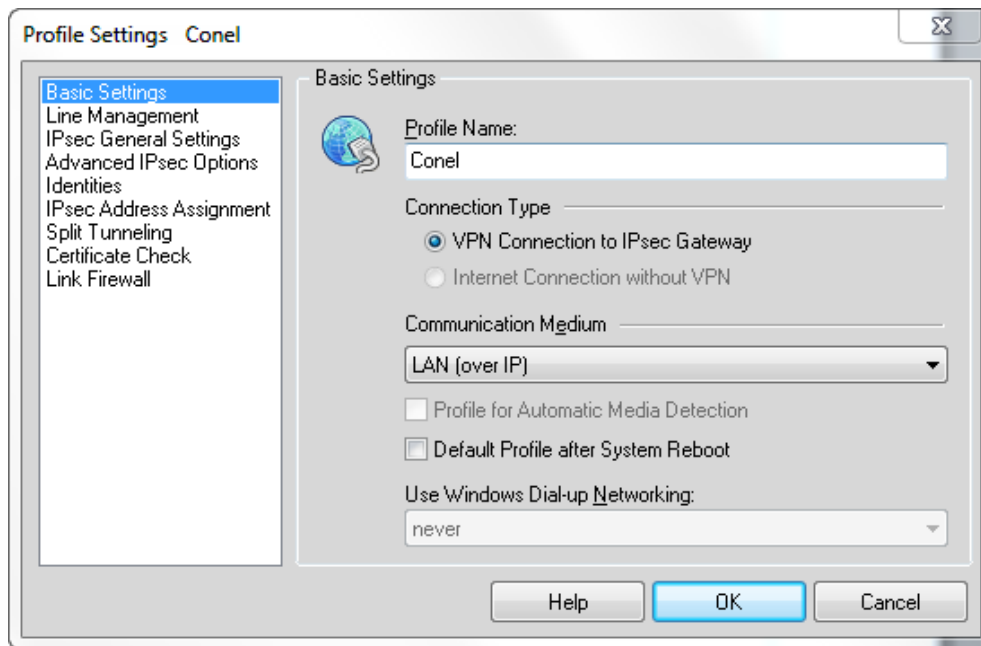


Fig. 17: Basic Settings

Line Management

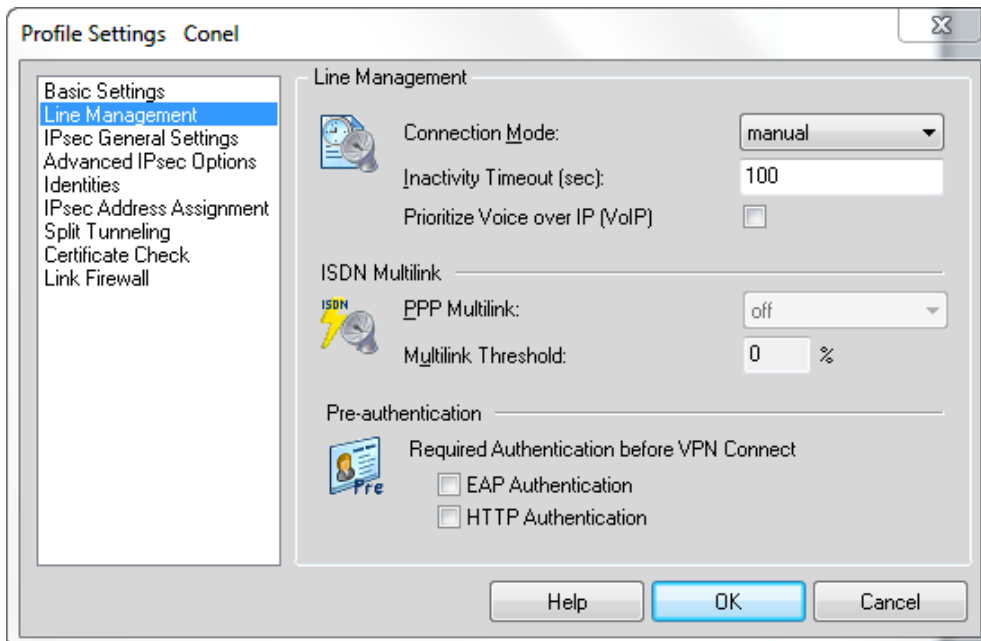


Fig. 18: Line Management

□ IPsec General Settings

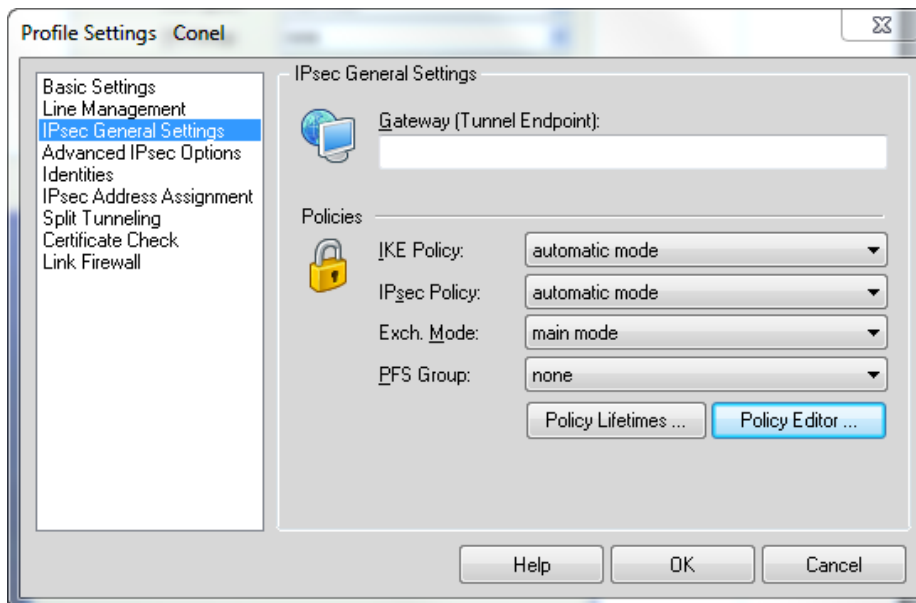


Fig. 19: IPsec General Settings

In this window press the *Police Editor...* button. Then, in the section named *IKE Policy* (in the new window) select *Pre-shared Key* item and click on the *Edit* button.

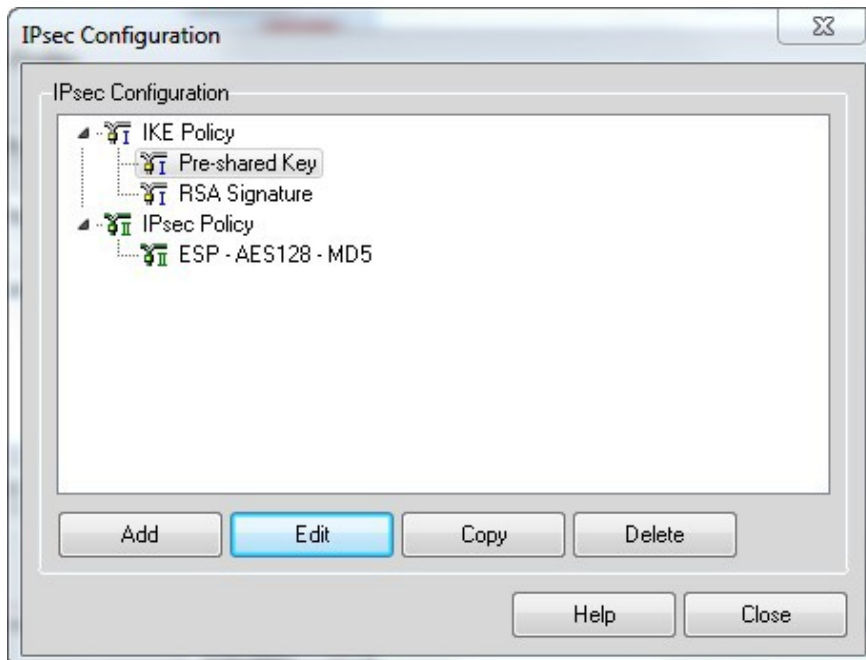


Fig. 20: Police Editor I (IPsec Configuration)

You will see the window shown in the figure below. Select *Pre-shared Key*, *Triple DES*, *MD5*, *DH-Group 2* and then press *OK*.

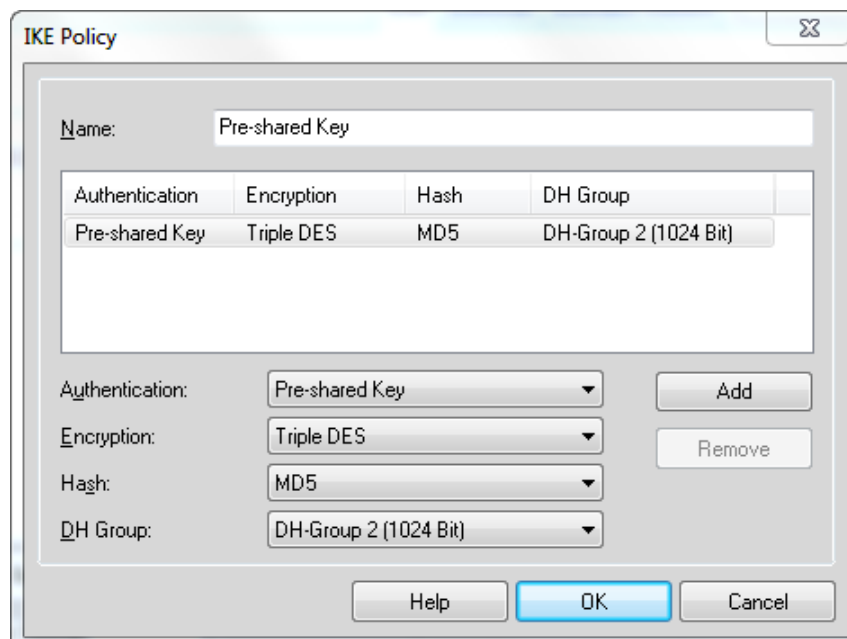


Fig. 21: Pre-shared Key (IPSec Configuration)

Now in the configuration window in *IPsec Policy* section select the only available item and click on the *Edit* button.

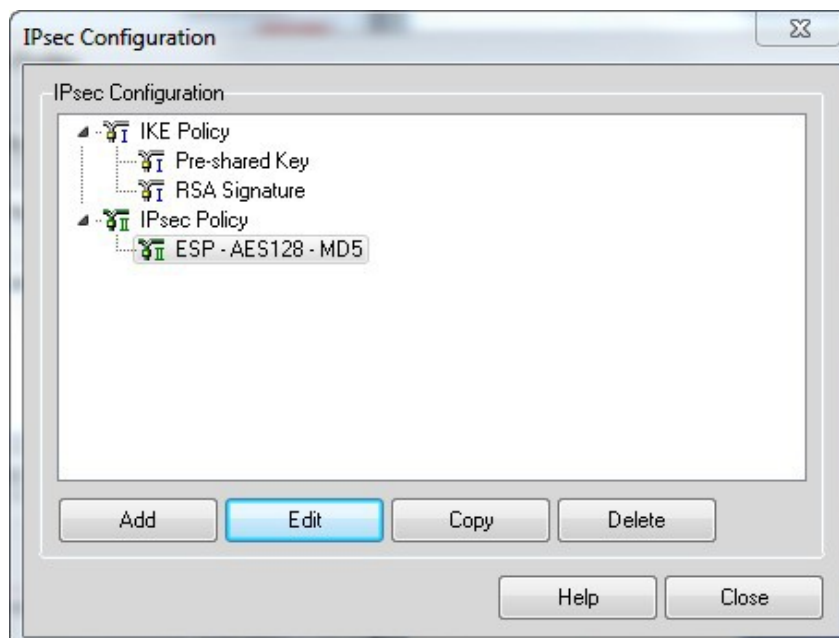


Fig. 22: Police Editor II (IPSec Configuration)

In the new window enter the name (e.g. ipsec) and select *Triple DES* and *MD5*. Then confirm by clicking *OK*.

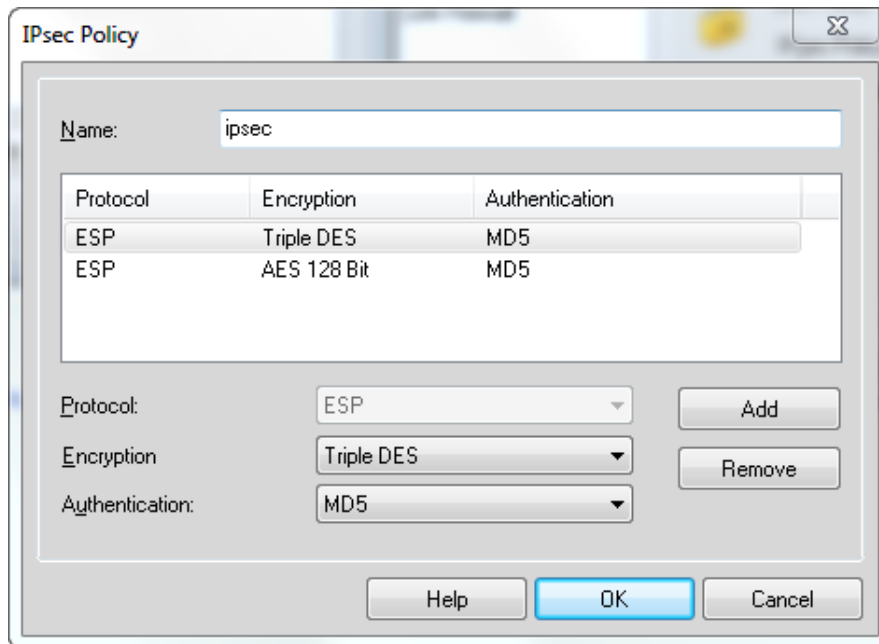


Fig. 23: IPsec Policy (IPsec Configuration)

Return to the main window of IPsec General Settings item and set the IKE Policy item and the IPsec Policy item on the basis of the previous configuration (see figure below).

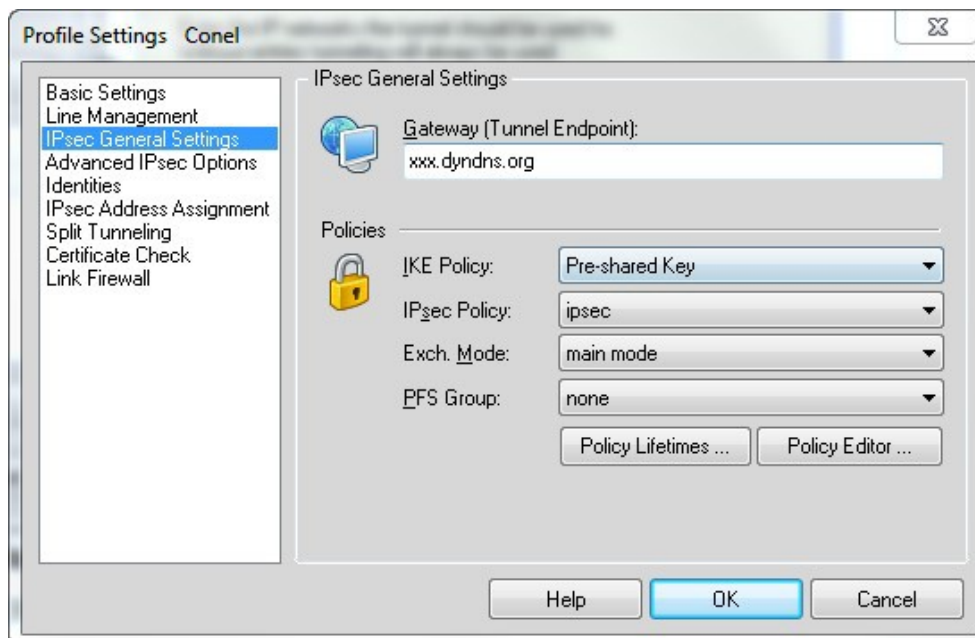


Fig. 24: IPsec General Settings – final setting

Advanced IPsec Options

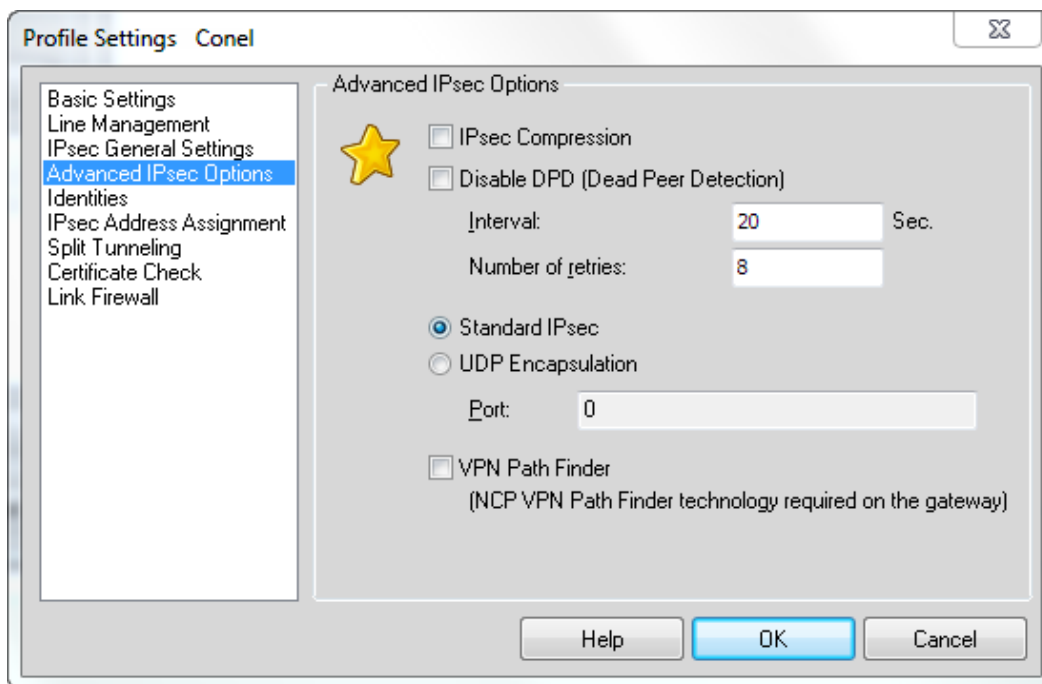


Fig. 25: Advanced IPsec Options

Identities

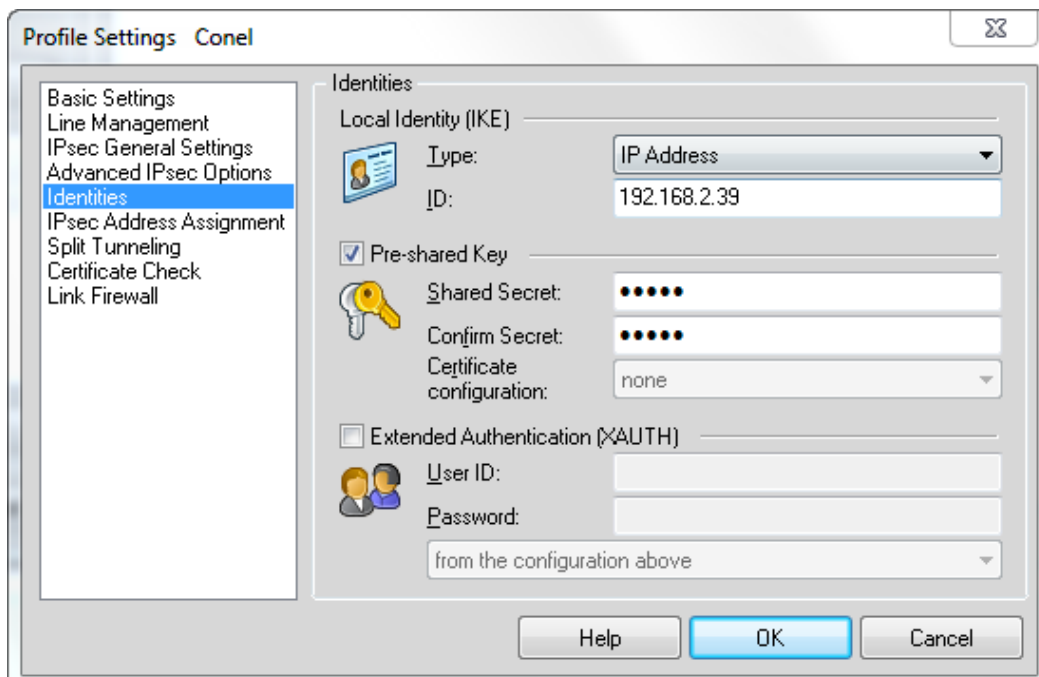


Fig. 26: Identities

IPSec Address Assignment

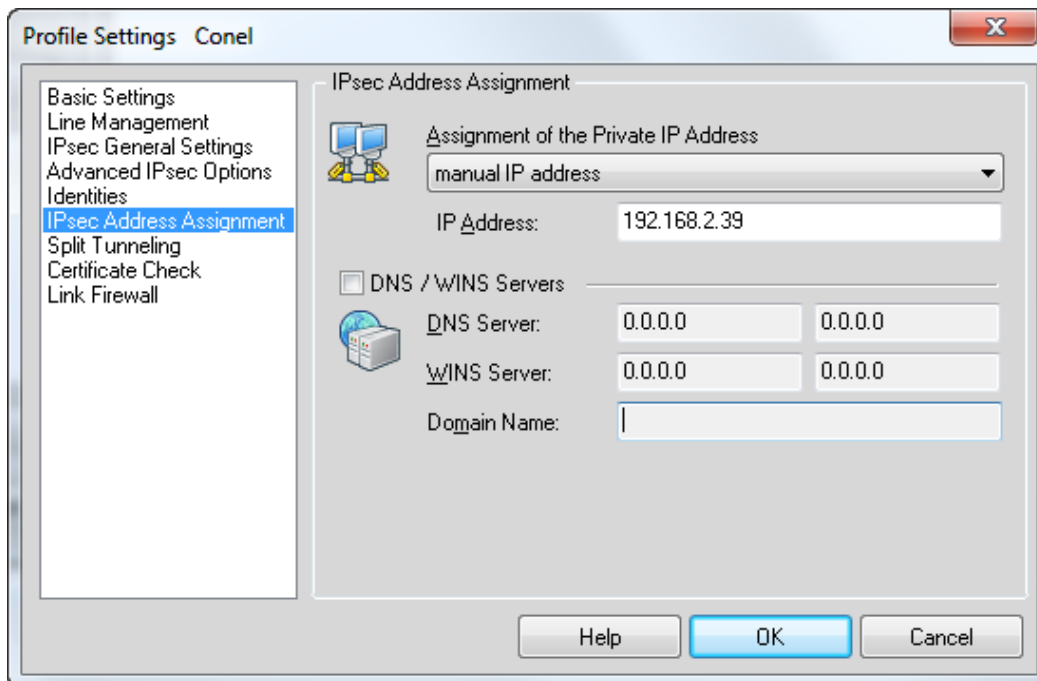


Fig. 27: IPSec Address Assignment

Split Tunneling

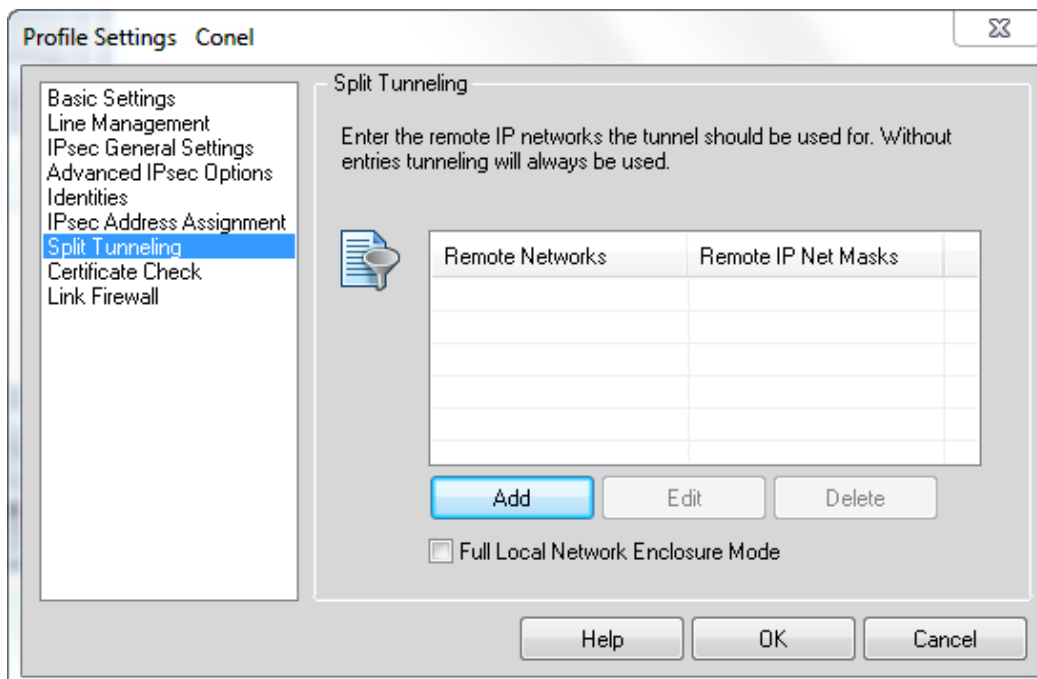


Fig. 28: Split Tunneling

Click the *Add* button and enter the subnet on the ETH port of the corresponding router.

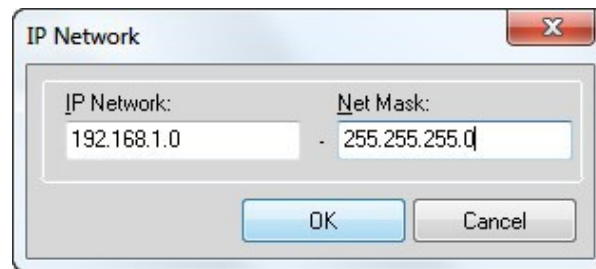


Fig. 29: IP Network

Confirm by clicking on the *OK* button. You will see the entered data in the original window of *Split Tunneling* item:

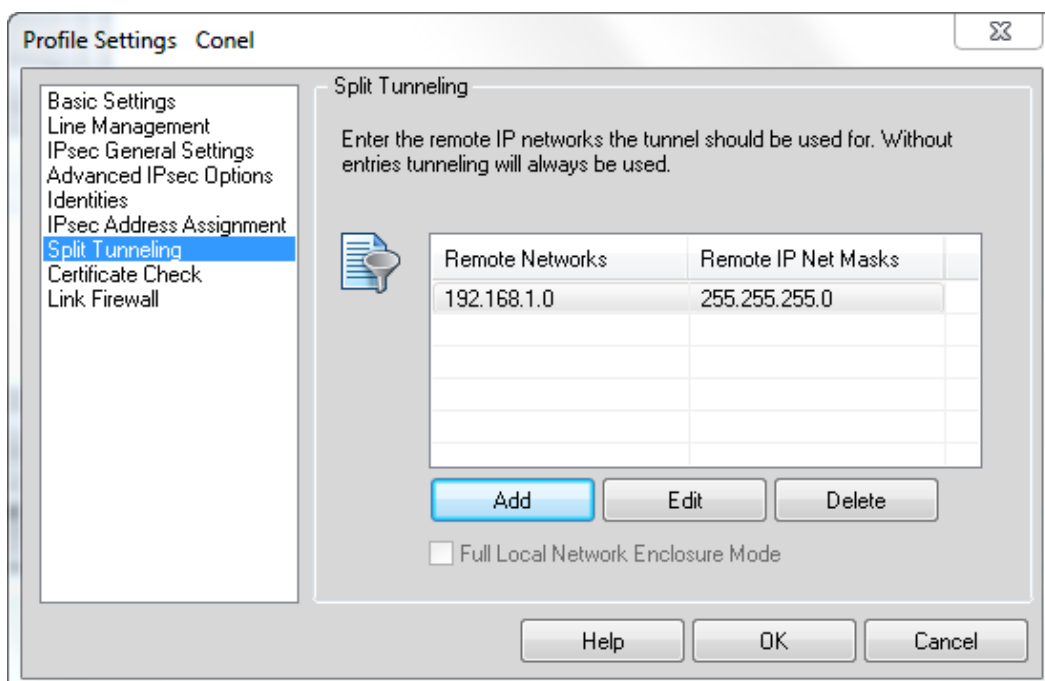


Fig. 30: Split Tunneling – entered data

Certificate Check and **Link Firewall** do not need to change.

Create 1st IPsec tunnel

Description '''	ncp
Remote IP Address x	
Remote ID x	192.1682.39
Remote Subnet '''	192.1682.39
Remote Subnet Mask '''	255.255255255
Local ID x	
Local Subnet '''	192.168.1.0
Local Subnet Mask x	255.255.255.0
Key Lifetime	3600 sec
KE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay x	sec
DPD Timeout '''	sec
NAT Traversal	enabled
Aggressive Mode	disabled
Authenticate Mode	pre-shared key
Pre-shared Key	test
CA Certificate	
Remote Certificate	
Local Certificate	
Local Private Key	
Local Passphrase '''	
Extra Options '''	

Fig. 31: Router setting (Windows)

2.5.5. Connection successfully established

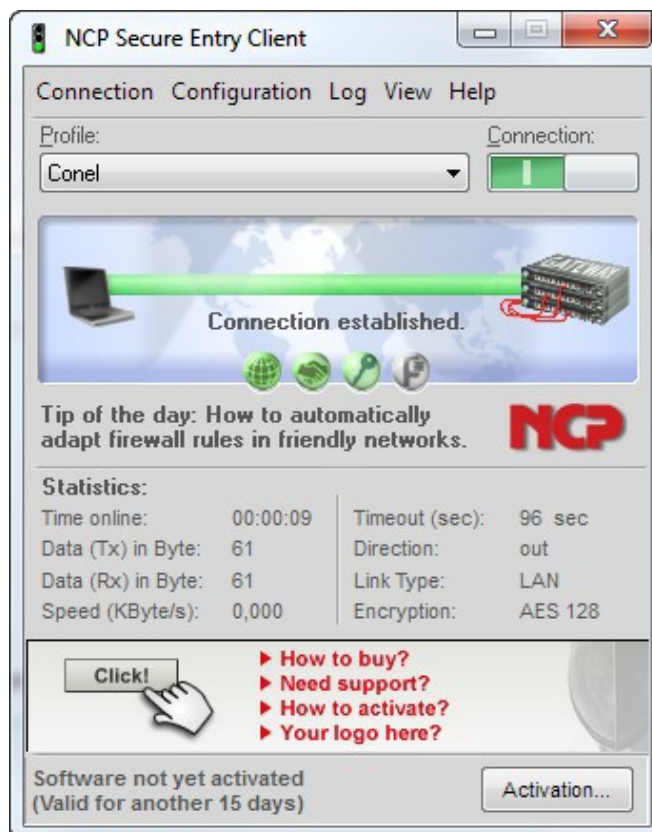


Fig. 32: Connection successfully established

Ping 192.168.1.100 (32 bytes):

```
Odpověď od 192.168.1.100: bajty=32 čas=651ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=287ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=305ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=326ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=324ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=321ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=299ms TTL=127
Odpověď od 192.168.1.100: bajty=32 čas=299ms TTL=127
```

Fig. 33: Ping 192.168.1.100

2.6. Using the IPsec tunnel- Mikrotik

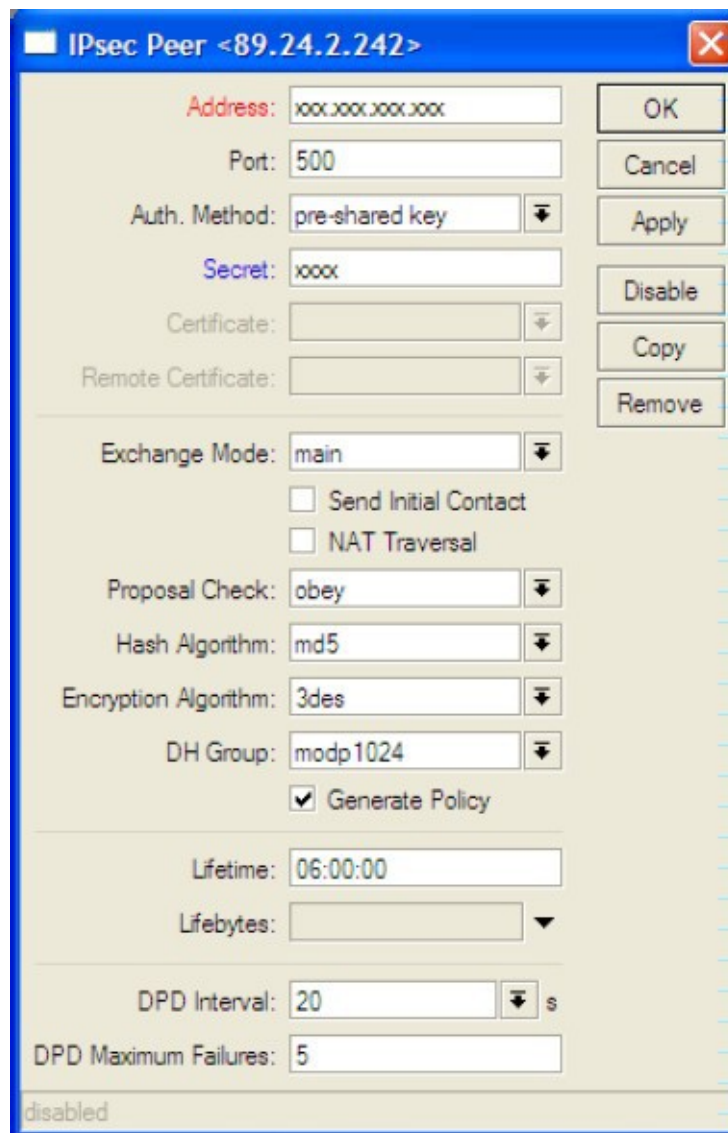
2.6.1. Router setting

Create 1st IPsec tunnel

Description ×	Mikrotik
Remote IP Address ""	IP adresa Mikrotiku
Remote ID ×	
Remote Subnet ""	192.168.1.0
Remote Subnet Mask ×	255.255.255.0
Local ID ×	
Local Subnet ""	192.168.10.0
Local Subnet Mask ""	255.255.255.0
Key Lifetime	3600 sec
IK E Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay""	sec
DPD Timeout ""	sec
NAT Traversal	disabled
Aggressive Mode	disabled
Authenticate Mode	pre-shared key
Pre-shared Key	conel
CA Certificate	
Remote Certificate	
Local Certificate	
Local Private Key	
Local Passphrase *	
Extra Options ×	

Fig. 34: Router setting (Mikrotik)

2.6.2. Mikrotik router setting



The screenshot shows the 'IPsec Peer <89.24.2.242>' configuration window. The fields are as follows:

- Address: xxx.xxx.xxx.xxx
- Port: 500
- Auth. Method: pre-shared key
- Secret: xxxx
- Certificate: (empty)
- Remote Certificate: (empty)
- Exchange Mode: main
 - Send Initial Contact
 - NAT Traversal
- Proposal Check: obey
- Hash Algorithm: md5
- Encryption Algorithm: 3des
- DH Group: modp1024
 - Generate Policy
- Lifetime: 06:00:00
- Lifebytes: (empty)
- DPD Interval: 20 s
- DPD Maximum Failures: 5

Buttons on the right: OK, Cancel, Apply, Disable, Copy, Remove.

Status: disabled

Fig. 35: Mikrotik router setting

In *Address* item you can enter 0.0.0.0/0 if the opposite side establishes the tunnel (it means router).

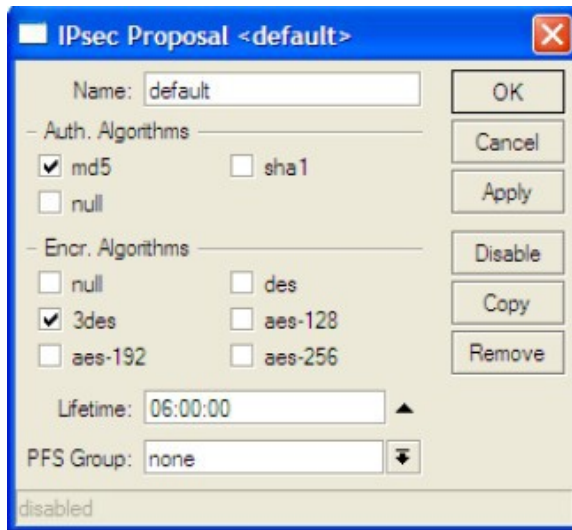


Fig. 36: IPsec Proposal

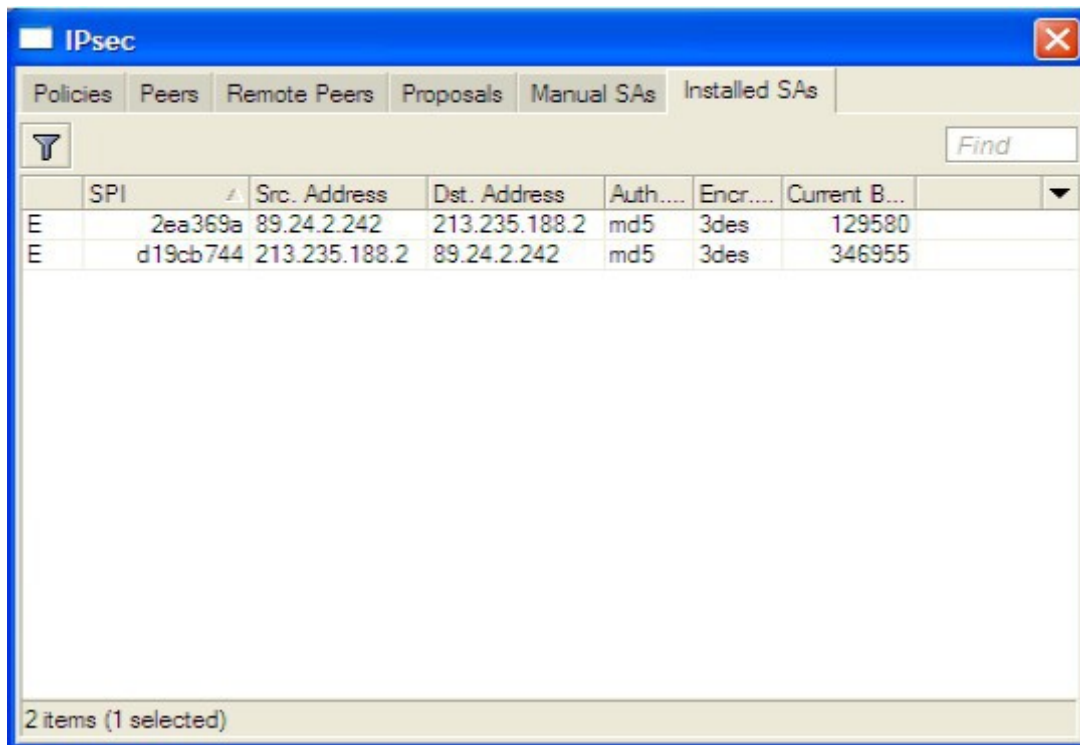


Fig. 37: IPsec – Installed SAs

2.7. Using the IPSec tunnel – Lancom 1721

2.7.1. VPN – General

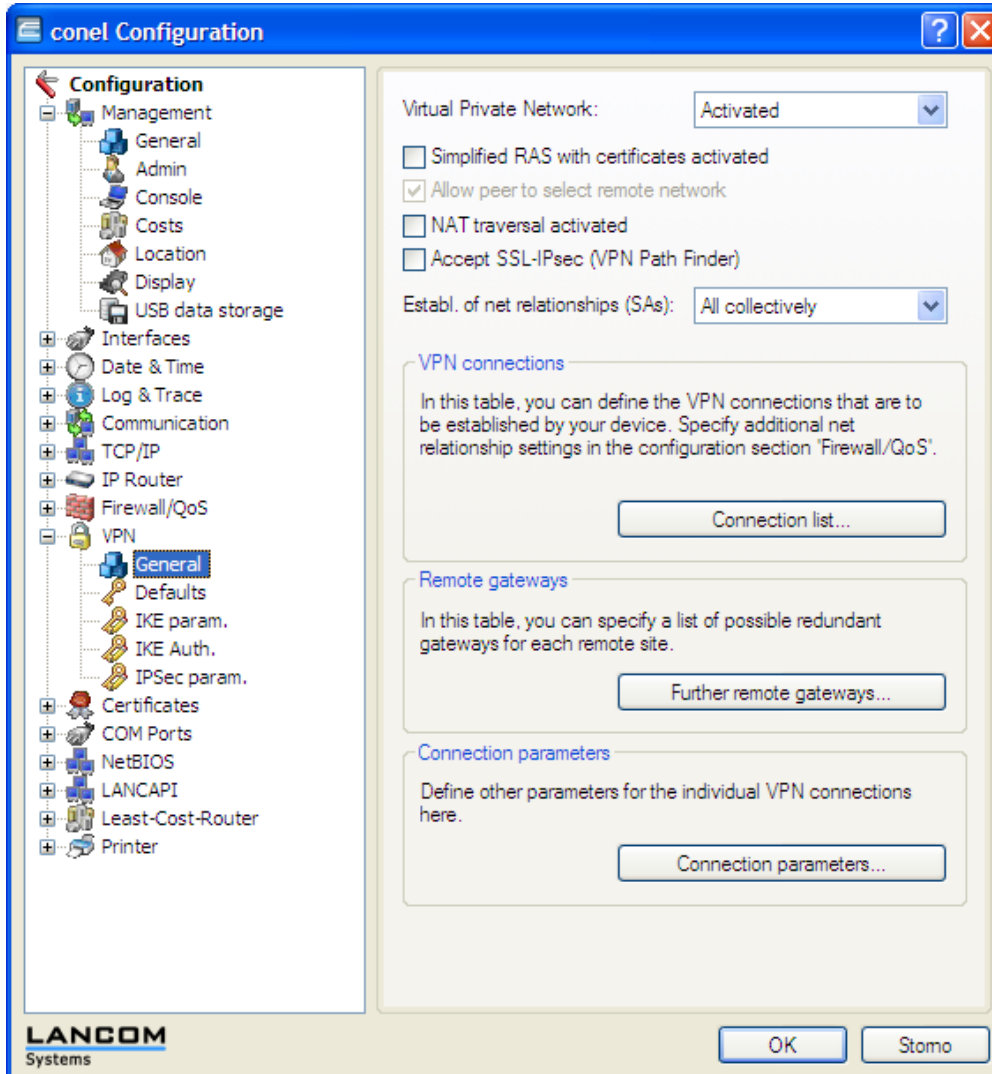


Fig. 38: VPN – General

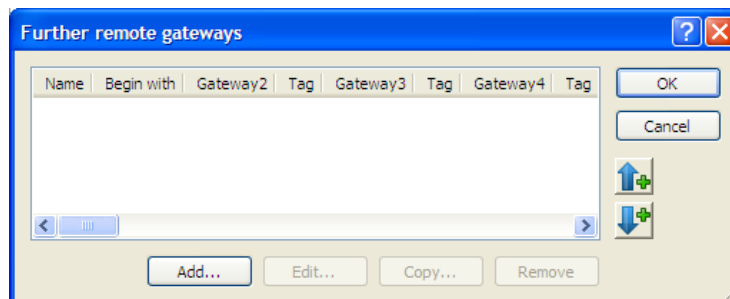


Fig. 39: Remote gateways

Connection list - Edit Entry

Name of connection:

Short hold time: seconds

Dead Peer Detection: seconds

Extranet address:

Gateway:

Connection parameters:

Rule Creation:

Dynamic VPN connection (only with compatible remote stations):

- No dynamic VPN
- Dynamic VPN (a connection is created to transmit IP addresses)
- Dynamic VPN (IP addresses are transmitted without establishing a connection if possible)
- Dynamic VPN (an ICMP packet will be sent to transmit IP addresses)
- Dynamic VPN (an UDP packet will be sent to transmit IP addresses)

IKE exchange (only in conjunction with "No dynamic VPN"):

- Main mode
- Aggressive mode

IKE-CFG:

XAUTH:

SSL-IPsec (Path Finder):

Routing tag:

Fig. 40: Connection list – Edit Entry

Connection parameters - Edit Entry

Identification:

PFS group:

IKE group:

IKE proposals:

IKE key:

IPsec proposals:

Fig. 41: Connection parameters – Edit Entry

2.7.2. VPN – Defaults

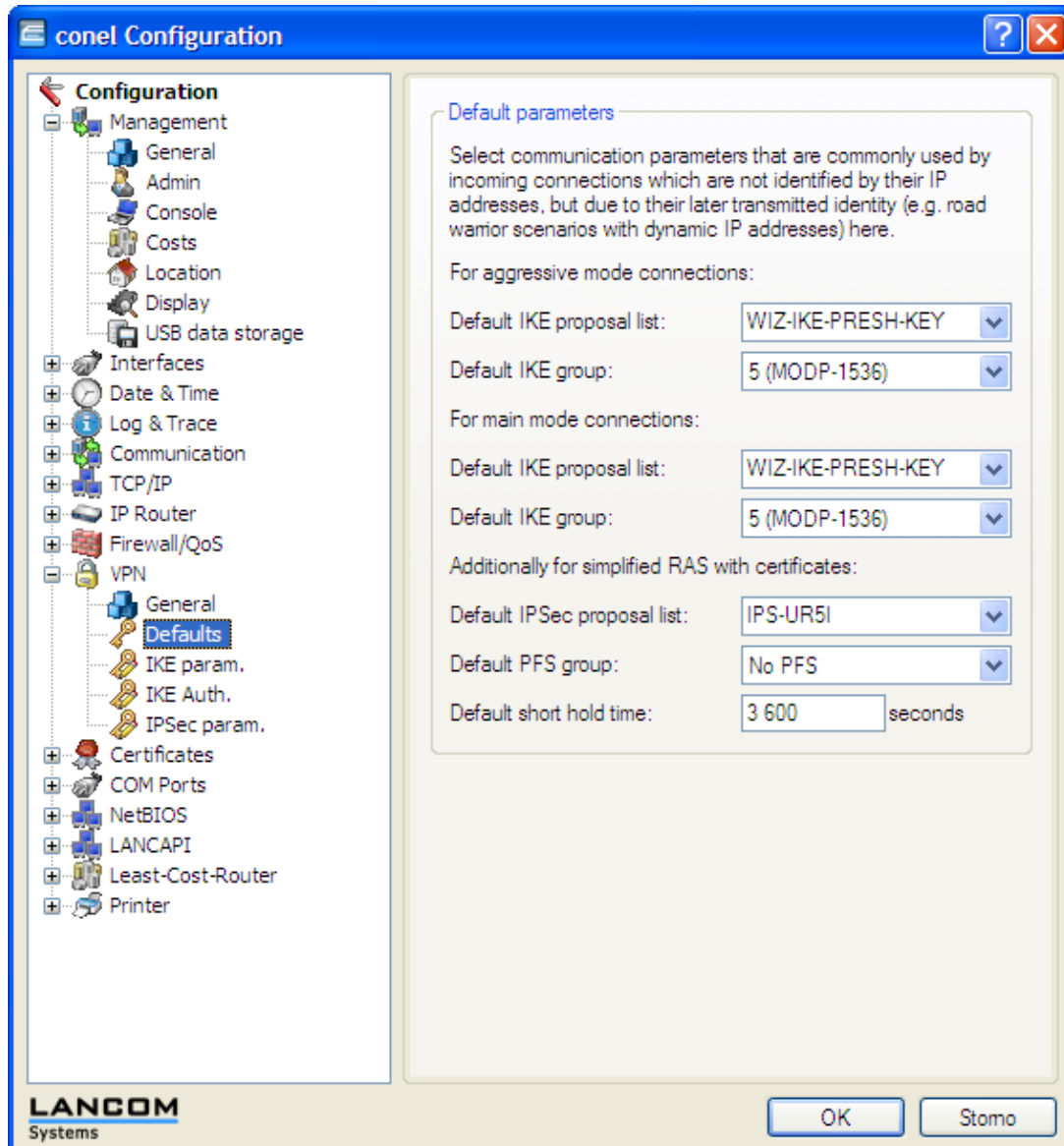


Fig. 42: VPN – Defaults

2.7.3. VPN – IKE parameters

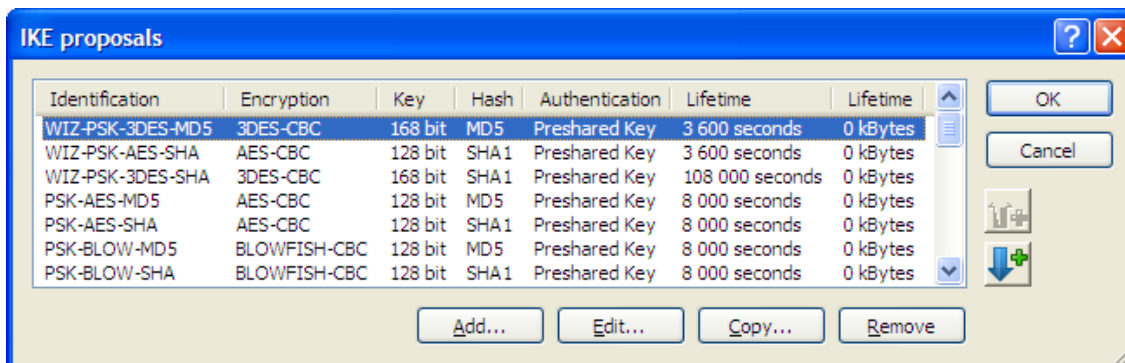


Fig. 43: VPN – IKE parameters

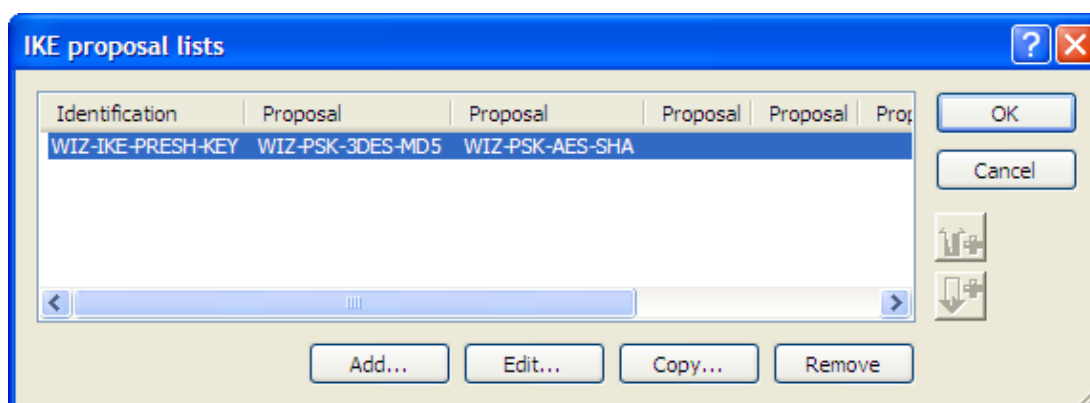


Fig. 44: IKE proposal lists

2.7.4. VPN – IKE Authorities

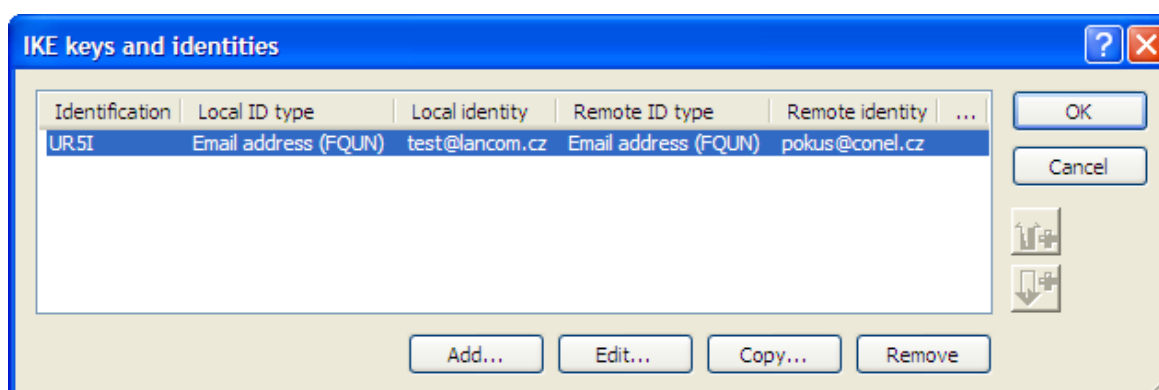


Fig. 45: VPN – IKE Authorities

2.7.5. VPN – IPsec parameters

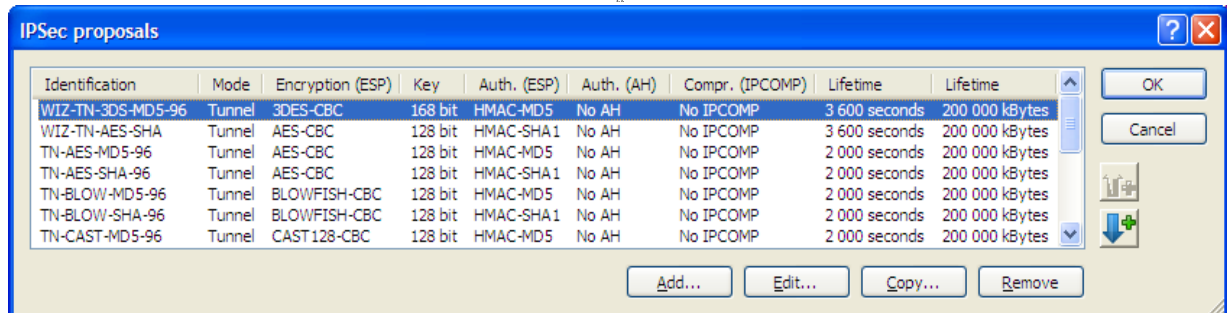


Fig. 46: VPN – IPsec parameters

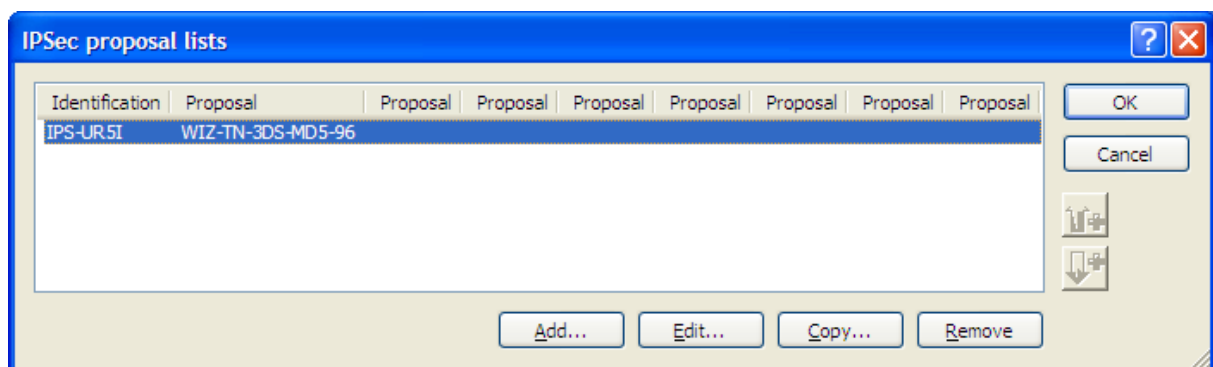


Fig. 47: IPsec proposal lists

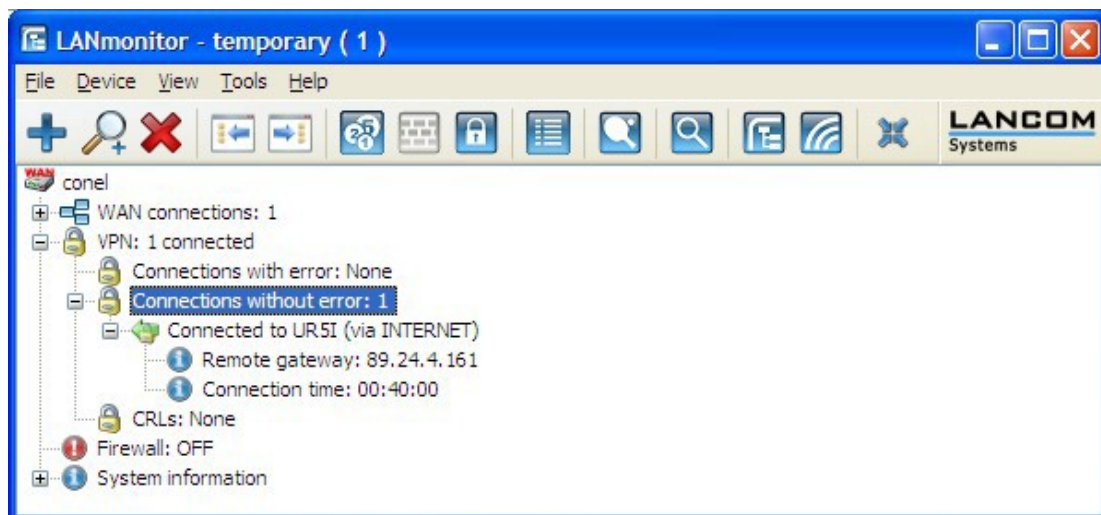


Fig. 48: LANmonitor

2.7.6. Router setting (Lancom 1721)

Create 1st IPsec tunnel

Description *	Lancom
Remote IP Address *	85.207.239.156
Remote ID *	test@lancom.cz
Remote Subnet *	192.168.11.0
Remote Subnet Mask *	255.255.255.0
Local ID *	pokus@conel.cz
Local Subnet *	192.168.2.0
Local Subnet Mask *	255.255.255.0
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	20 sec
DPD Timeout *	60 sec
NAT Traversal	enabled
Aggressive Mode	enabled
Authenticate Mode	pre-shared key
Pre-shared Key	test

Fig. 49: Router setting (Lancom 1721)

```

IPsec Tunnel Informations

interface eth0/eth0 192.168.2.1
interface eth0/eth0 192.168.2.1
interface ppp0/ppp0 10.169.175.215
interface ppp0/ppp0 10.169.175.215
%myid = (none)
debug none

"ipsec1": 192.168.2.0/24===10.169.175.215[pokus@conel.cz,S?C]...85.207.239.156[test@lancom.cz,S?C]===192.168.11.0/24; erouted; eroute owner: #2
"ipsec1":   srcip=unset; dstip=unset; srcup=/etc/scripts/updown; dstup=/etc/scripts/updown;
"ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
"ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP+AGGRESSIVE; prio: 24,24; interface: ppp0;
"ipsec1":   dpd: action:restart_by_peer; delay:20; timeout:60;
"ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #2;
"ipsec1":   IKE algorithms wanted: 5_000-1-5, flags=strict
"ipsec1":   IKE algorithms found: 5_192-1_128-5,
"ipsec1":   IKE algorithm newest: 3DES_CBC_192-MD5-MODP1536

#2: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 489s; newest IPSEC; eroute owner
#2: "ipsec1" esp.5a4396d3@85.207.239.156 esp.22a66bd5@10.169.175.215 tun.0@85.207.239.156 tun.0@10.169.175.215
#1: "ipsec1":500 STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 542s; newest ISAKMP; lastdpd=19s(seq in:30797 out:0)

```

Fig. 50: Information about IPsec tunnel (Lancom 1721)