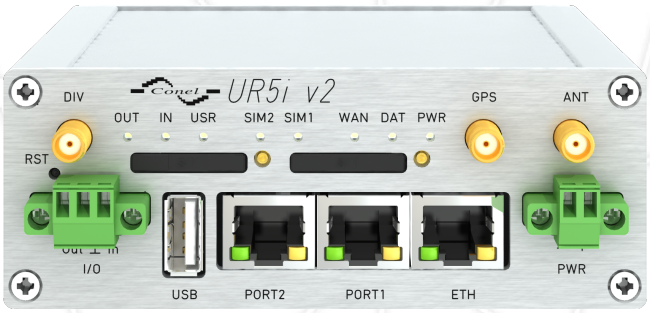
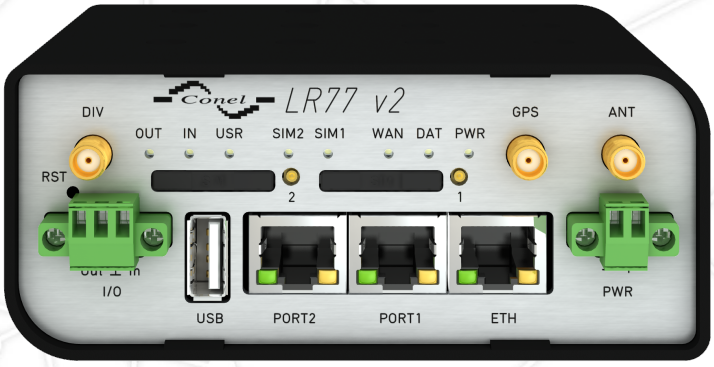
B+B SmartWorx®

+ CONEL CELLULAR ROUTERS

IPsec tunel

APPLICATION NOTE





ENABLING CONNECTED INTELLIGENCE

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.

Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Manual issued in CZ, February 17, 2015

Contents

List of Figures

List of Tables

1. IPsec and its protocols

IPsec (Internet Protocol Security) is a security extension of IP protocol based on authentication and encryption of every IP datagram. Within the OSI architecture, it is security at the network layer, which means that IPsec provides security for any transfer (any network application).

IPsec pay attention to these major security issues:

- **Authenticating** – Allows to verify the origin of the data, so if a packet is received, it is possible to verify that the transmitted packet corresponds to the sender or whether the sender exists at all (Phase I, IKE phase, Main mode). At PSK ends with key exchange.
- **Encrypting** – Both of sides agree on the form of packet encryption in advance. Thereafter the entire packet apart from the IP header will be encrypted, alternatively the entire packet will be encrypted and a new IP header will be added (Phase II, IPsec phase, Quick mode). Ends with establishing of a tunnel.

IPsec consists of two basic protocols – *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*. Protocols are complementary, so they are usually used simultaneously. A significant advantage of the simultaneous use of these two protocols is a higher level of security. Increased overhead when processing may eliminate this advantage. Part of IPsec is also *IKE (Internet Key Exchange)* protocol (key management). IKE creates logical channels which are called *Security Associations (SA)*. These channels are always unidirectional therefore it is necessary to use two separate channels (SA) for duplex. IKE also supports automatic generation and recovery of encryption keys.

1.1 Authentication Header (AH)

It provides authentication of sender and recipient, integrity of data in the header and protection against reverse queries. However, AH protocol does not provide confidentiality of data. This means that sent data are unencrypted and can be eavesdropped.

When using the Authentication Header protocol, each packet contains a special header which contains authentication information followed by data of the protocol itself. Authentication information consists of the result of a cryptographic checksum (it's used the SHA-1 or MD5 algorithm), security parameters (Security Parameter Index, SPI) and pointer to the header of higher level protocol. Items, which are changing in header of higher level protocol during a packet transmission (such as TTL item, for example), are ignored in the calculation of authentication information.

1.1.1 Usage of Authentication Header protocol

Authentication Header protocol can be used in two ways – in *transport mode* or in *tunnel mode*. Transport mode allows data protection using a header of AH protocol, which is inserted by the sender of the datagram between other extension headers. This mode requires less overhead when processing than the tunnel mode, but does not provide such security of data protection.

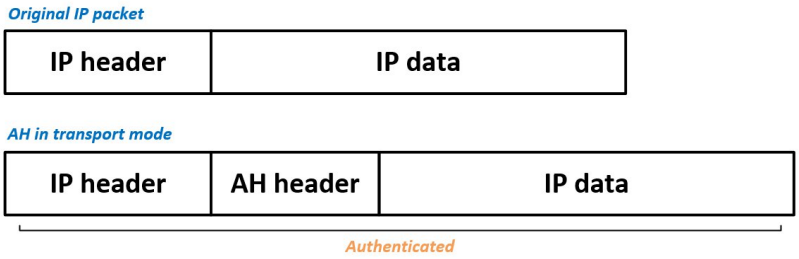


Figure 1: AH – transport mode

Tunnel mode (sometimes tunneling mode) creates a new IP header which is followed by header of Authentication Header protocol. This is followed by the entire original datagram packaged as new data datagram. In this mode, the AH protocol authenticates the entire datagram, which means that it is possible to determine whether the datagram has changed during transmission. The main advantage of the tunnel mode is perfect protection of an encapsulated IP datagram. Furthermore, it allows the use of private addresses.

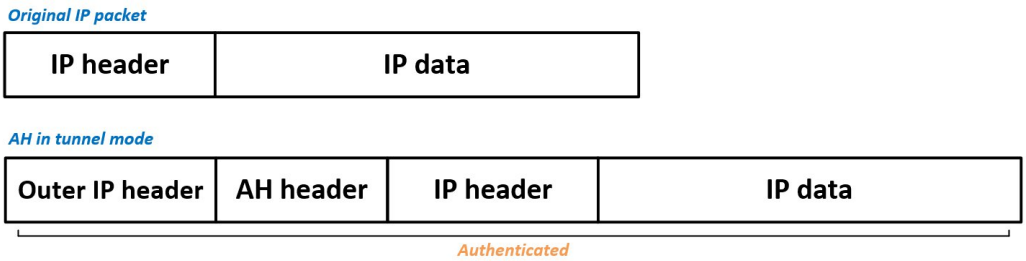


Figure 2: AH – tunnel mode

1.2 Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) protocol ensures the confidentiality of transmitted data (encrypts packets) and optionally the original authentication, data integrity and protection against reverse queries. As with the Authentication Header (AH) protocol, additional header is attached to an IP packet. This header contains the security parameters which are followed by encrypted data. However, the outer header is not protected and its integrity is not guaranteed.

In case of requirement for encryption and authentication, system which responds first authenticates packet and if the first step is successful, continues with encryption. This type of configuration reduces both overhead of processing and vulnerability in case of attack when denial of service.

1.2.1 Usage of Encapsulating Security Payload protocol

ESP protocol can be used in two ways – in *transport mode* or in *tunnel mode*. Transport mode inserts ESP header behind the IP header of the original IP datagram. ESP trailer and optional authentication data follow data of the original datagram. Transport mode requires less overhead when processing than the tunnel mode, but does not provide such security of data protection.

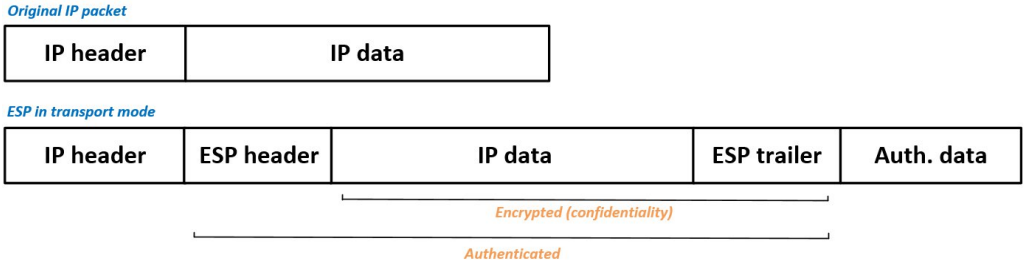


Figure 3: ESP – transport mode

Tunnel mode (sometimes tunneling mode) creates a new IP header which is followed by header of Encapsulating Security Payload protocol. This is followed by the entire original datagram packaged as new data datagram. This allows to completely protect original datagram (in case that encryption and authentication are used). ESP trailer and optional authentication data follow data of the original datagram.

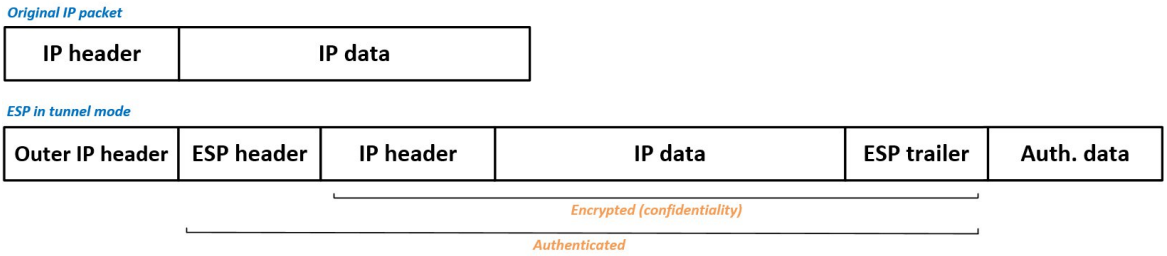


Figure 4: ESP – tunnel mode

2. Configuration of IPsec tunnel

IPsec tunnel creates a secure (encrypted) connection between two LANs into one that looks like a homogeneous. Conel Routers allow user to create up to four IPsec tunnels whose configuration can be called up by selecting the *IPsec* menu item. There are four lines in the *IPsec Tunnels Configuration* window, each line corresponds to the configuration of one tunnel.

Item	Description
Create	Enables (activates) individual tunnels (*yes* or *no*)
Description	Name or description of the tunnel specified in the configuration form of IPsec tunnel
Edit	Displays the configuration form of the IPsec tunnel

Table 1: Overview of IPsec tunnels

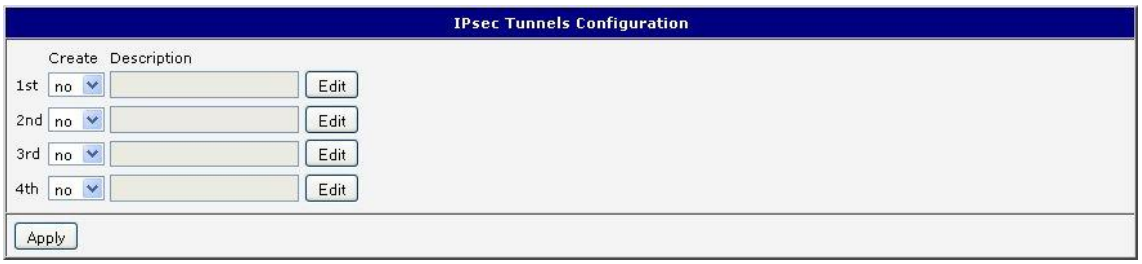


Figure 5: Overview of IPsec tunnels

Item	Description
Description	Name (description) of the tunnel
Remote IP Address	IP address of remote side of the tunnel. It is also possible to enter the domain name.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: *hostname* and *domain-name*.
Remote Subnet	IP address of a network behind remote side of the tunnel
Remote Subnet Mask	Subnet mask of a network behind remote side of the tunnel
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: *hostname* and *domain-name*.
Local Subnet	IP address of a local network
Local subnet mask	Subnet mask of a local network
Encapsulation Mode	IPsec mode (according to the method of encapsulation) – You can choose *tunnel* (entire IP datagram is encapsulated) or *transport* (only IP header).

Continued on next page

Continued from previous page

Item	Description
NAT traversal	If address translation is used between two end points of the tunnel, it needs to enable *NAT Traversal*.
IKE Mode	Defines mode for establishing connection (*main* or *aggressive*). If the aggressive mode is selected, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5.
IKE Algorithm	Way of algorithm selection: • **auto** – encryption and hash alg. are selected automatically • **manual** – encryption and hash alg. are defined by the user
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256
IKE Hash	Hash algorithm – MD5 nebo SHA1
IKE DH Group	Diffie-Hellman groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key. Group with higher number provides more security, but requires more processing time.
ESP Algorithm	Way of algorithm selection: • **auto** – encryption and hash alg. are selected automatically • **manual** – encryption and hash alg. are defined by the user
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hash algorithm – MD5 nebo SHA1
PFS	Ensures that derived session keys are not compromised if one of the private keys is compromised in the future
PFS DH Group	Diffie-Hellman group number (see *IKE DH Group*)
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before connection expiry should attempt to negotiate a replacement begin. Maximum value must be less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage extension of Rekay Margin time
DPD Delay	Time after which the IPsec tunnel functionality is tested
DPD Timeout	The period during which device waits for a response

Continued on next page

Continued from previous page

Item	Description
Authenticate Mode	Using this parameter can be set authentication: • **Pre-shared key** – sets the shared key for both sides of the tunnel • **X.509 Certificate** – allows X.509 authentication in multi-client mode
Pre-shared Key	Shared key for both sides of the tunnel to Pre-shared key authenticate
CA Certificate	Certificate for X.509 authentication
Remote Certificate	Certificate for X.509 authentication
Local Certificate	Certificate for X.509 authentication
Local Private Key	Private key for X.509 authentication
Local Passphrase	Passphrase for X.509 authentication
Extra Options	Use this parameter to define additional parameters of the IPsec tunnel, for example secure parameters etc.

Table 2: Configuration of IPsec tunnel

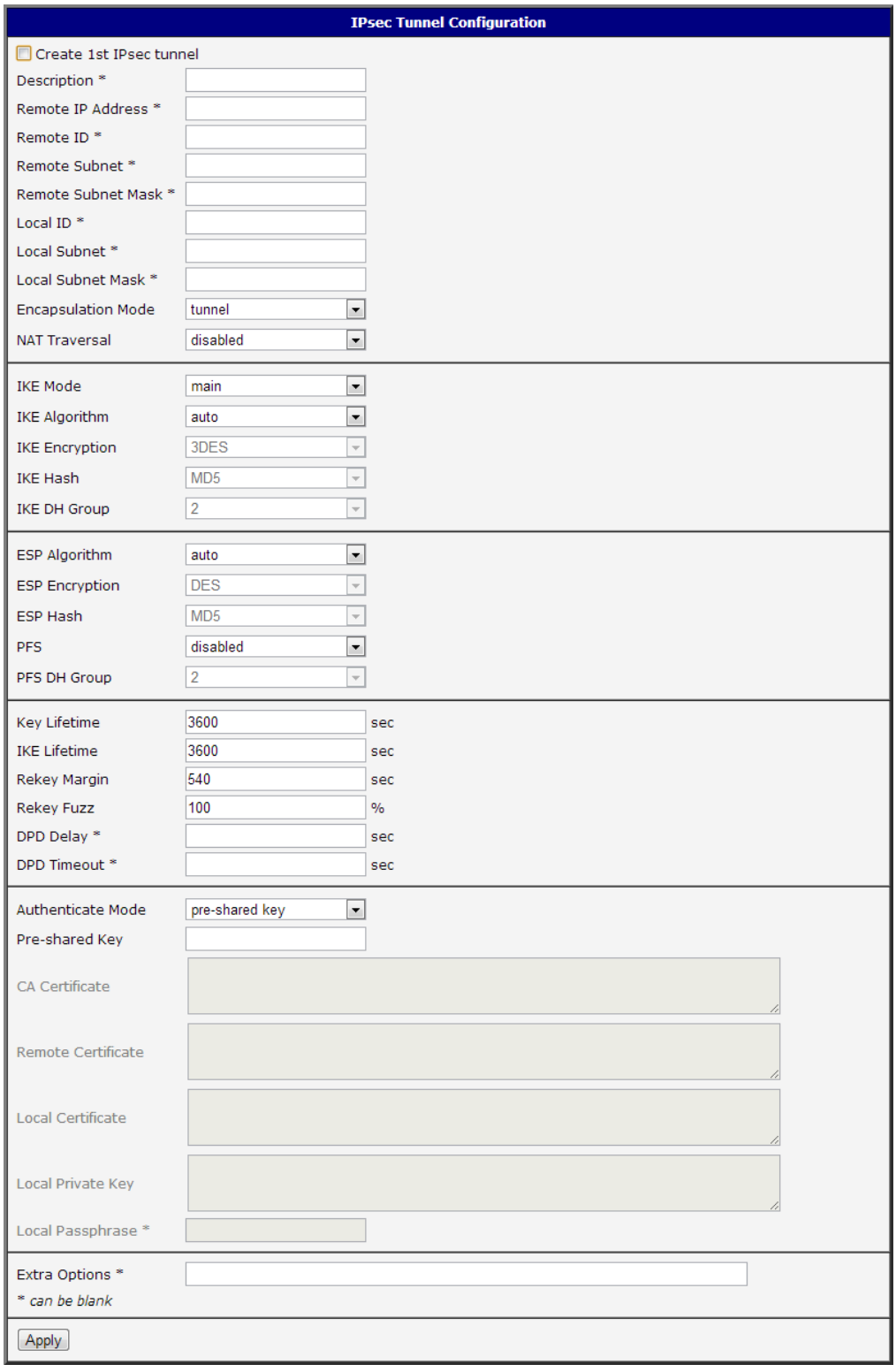


Figure 6: Configuration form of IPsec tunnel

3. Examples of use

3.1 IPsec tunnel – initiator on the router

IP address of the SIM card inserted into Conel router can be static or dynamic, because IPsec tunnel is established by initiator on the router. In this case, Linux server (CISCO router) offers services for IPsec tunnel therefore it must always be available on a static IP address or on a domain name.

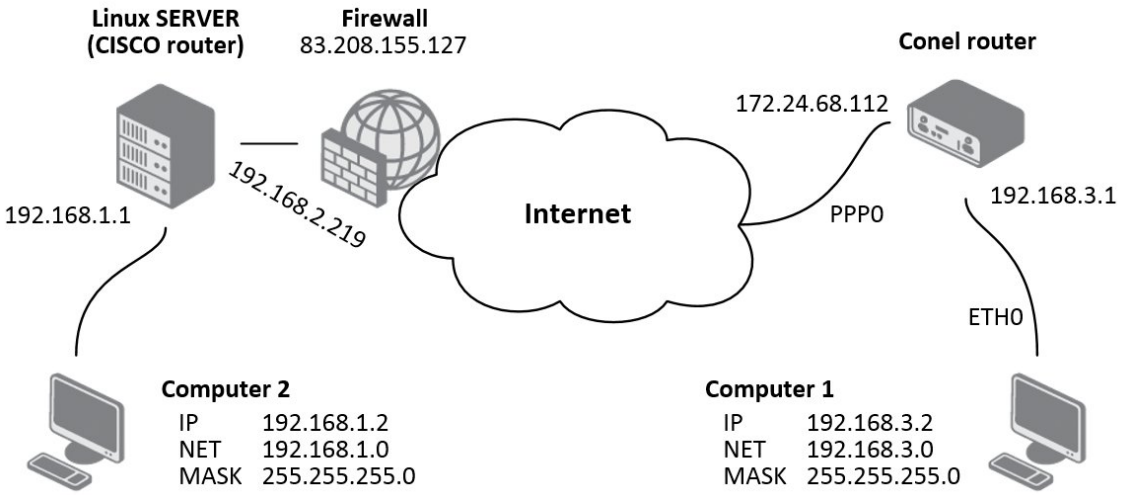


Figure 7: IPsec tunnel – initiator on the router

3.1.1 Configuration via web interface

If addresses of tunnel ends are visible to one another, all you have to do is specify these items: *Description*, *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*.

If *NAT Traversal* is active, it is also necessary to set *Remote ID*. As the ID has to be filled FQDN (Fully Qualified Domain Name), which is the designation for a fully specified domain name of the computer. It is also possible to set authentication using certificates, but then there is no need to enter *Remote ID*.

The following table provides an example of IPsec tunnel settings which correspond to the figure from the beginning of this chapter:

Item	Value
Remote 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

Table 3: IPsec tunnel settings (initiator)

Other parameters can be left in default settings. If the *Remote IP Address* parameter is empty on one side of IPsec tunnel, then this side will wait for a connection and will not attempt to establish a connection.

All items that are not mentioned in the sample settings and are marked with an asterisk (*) may not be filled in. They are used to accurate identification of the tunnel.

3.1.2 Detection of the successful establishment of the tunnel

Information about the active IPsec tunnel can be found in the *Status* section on the *IPsec* page of the router web interface.

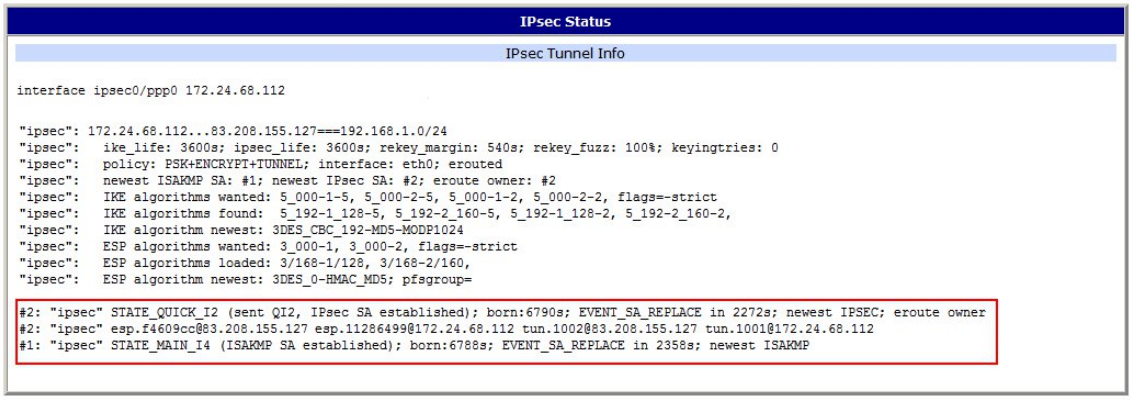


Figure 8: Information about IPsec tunnel (initiator)

It is possible to read the selected encryption in various stages of establishing the tunnel from the figure above:

- IKE: 3DES_CBC_192-MD5-MODP1024
- ESP: 3DES_0-HMAC_MD5, pfsgroup = none

The highlighted part shows information about the successful establishment of IPsec tunnel.

3.2 IPsec tunnel – responder on the router

Conel router must have an available static IP address or dynamic IP address of the SIM card in case of using translation of dynamically assigned IP addresses to DynDNS domain name. In this case, Linux server (CISCO router) is initiator and establishes IPsec tunnel.

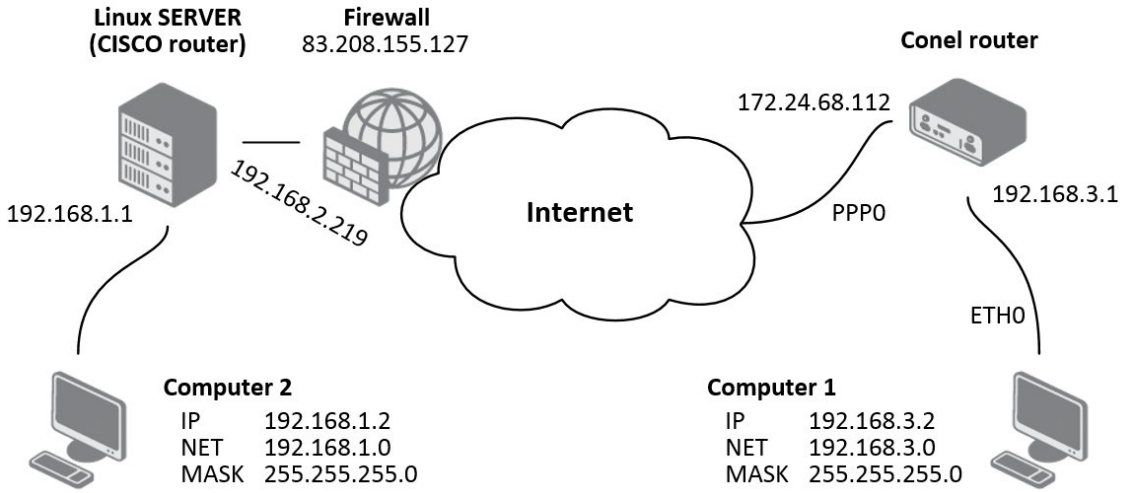


Figure 9: IPsec tunnel – responder on the router

3.2.1 Configuration via web interface

If addresses of tunnel ends are visible to one another, all you have to do is specify these items: *Description*, *Remote Subnet* and *Remote Subnet Mask*. If not (one end of the tunnel is in a private network), it is necessary to enable *NAT Traversal*.

If *NAT Traversal* is active, it is also necessary to set *Remote ID*. As the ID has to be filled FQDN (Fully Qualified Domain Name), which is the designation for a fully specified domain name of the computer. It is also possible to set authentication using certificates, but then there is no need to enter *Remote ID*.

The following table provides an example of IPsec tunnel settings which correspond to the figure from the beginning of this page:

Item	Value
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

Table 4: IPsec tunnel settings (responder)

Other parameters can be left in default settings. If the *Remote IP Address* parameter is empty on one side of IPsec tunnel, then this side will wait for a connection and will not attempt to establish a connection.

All items that are not mentioned in the sample settings and are marked with an asterisk (*) may not be filled in. They are used to accurate identification of the tunnel.

3.2.2 Detection of the successful establishment of the tunnel

Information about the active IPsec tunnel can be found in the *Status* section on the *IPsec* page of the router web interface.

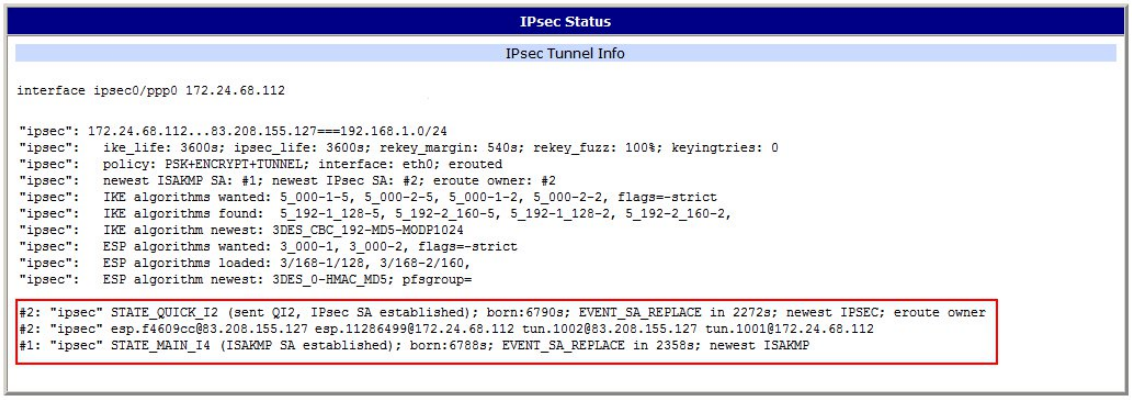


Figure 10: Information about IPsec tunnel (responder)

It is possible to read the selected encryption in various stages of establishing the tunnel from the figure above:

- IKE: 3DES_CBC_192-MD5-MODP1024
- ESP: 3DES_0-HMAC_MD5, pfsgroup = none

The highlighted part shows information about the successful establishment of IPsec tunnel.

3.3 IPsec tunnel – Linux server

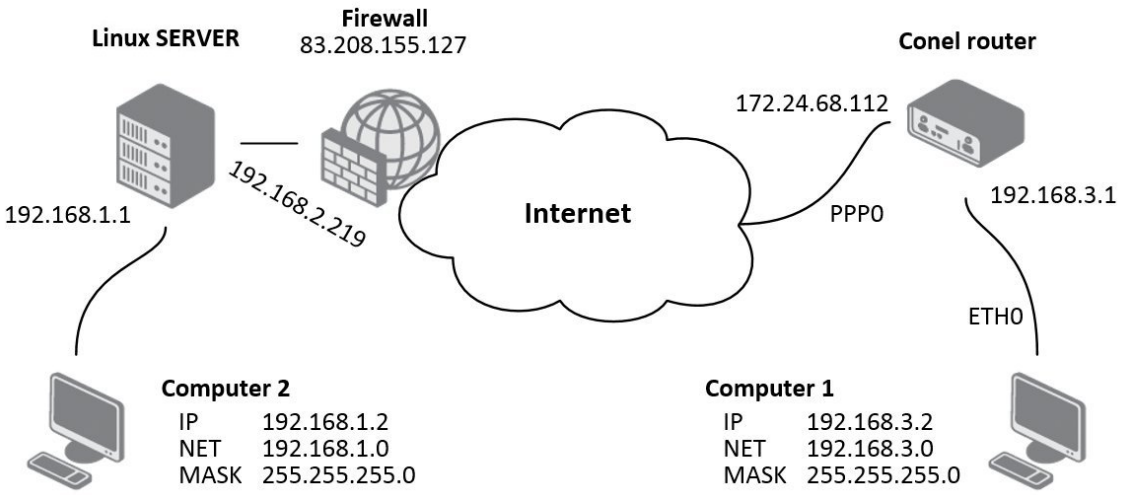


Figure 11: IPsec tunnel – Linux server

On the Linux server is needed to configure *ipsec.conf* and *ipsec.secrets* files. Configuration of *ipsec.conf* file can be performed for example like this:

```
conn conelrouter
   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
```

ipsec.secrets file shall be configured as follows:

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

3.4 IPsec tunnel – CISCO router

Please note that CISCO routers support IPsec protocol since IOS version no. 7.1.

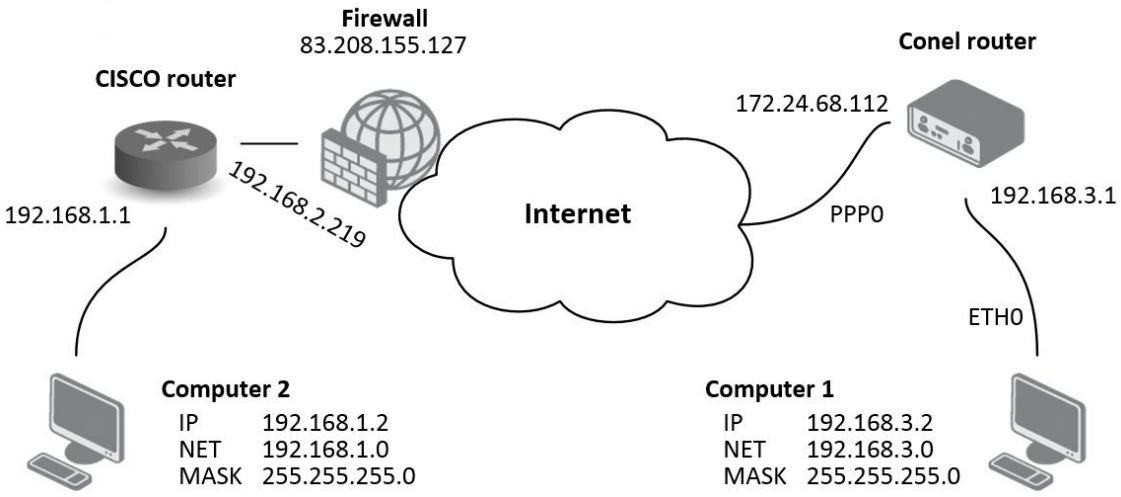


Figure 12: IPsec tunnel – CISCO router

3.4.1 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 2KFQnbNIdI.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
```

3.4.2 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 2KFQnbNIdI.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
```

3.5 IPsec tunnel – Computer with Windows

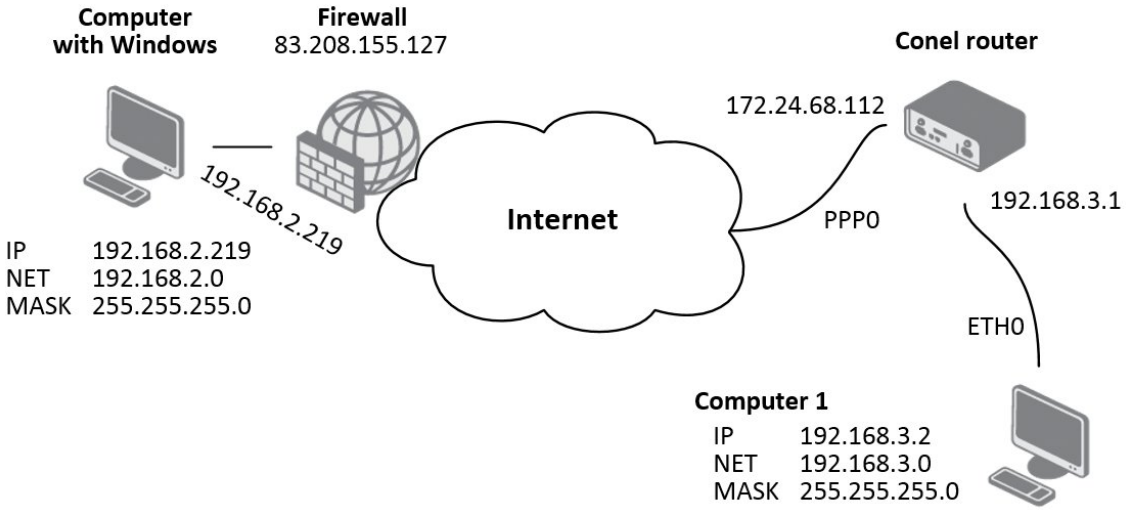


Figure 13: IPsec tunnel – Windows

Recommended program for Windows operating system is *NCP Secure Entry Client* on which the following description is based on.

3.5.1 IPsec configuration (NCP Secure Entry Client)

The figure below shows the environment of the NCP Secure Entry Client (version 9.32, build 218).

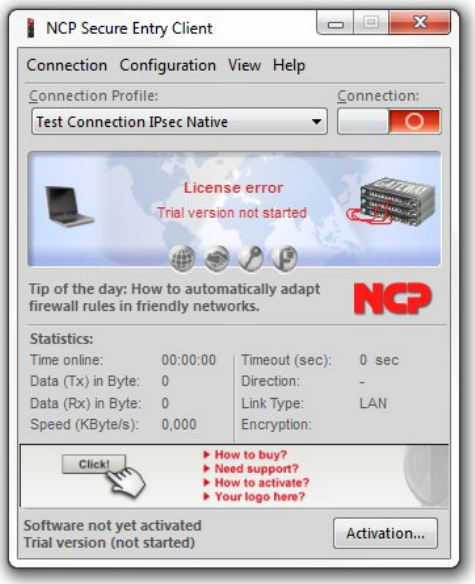


Figure 14: NCP Secure Entry Client

First it is necessary to create a profile for establishing IPsec tunnel. Select *Configuration* tab in the menu (of NCP Secure Entry Client program) and then select *Profiles* item. The following window will be open:

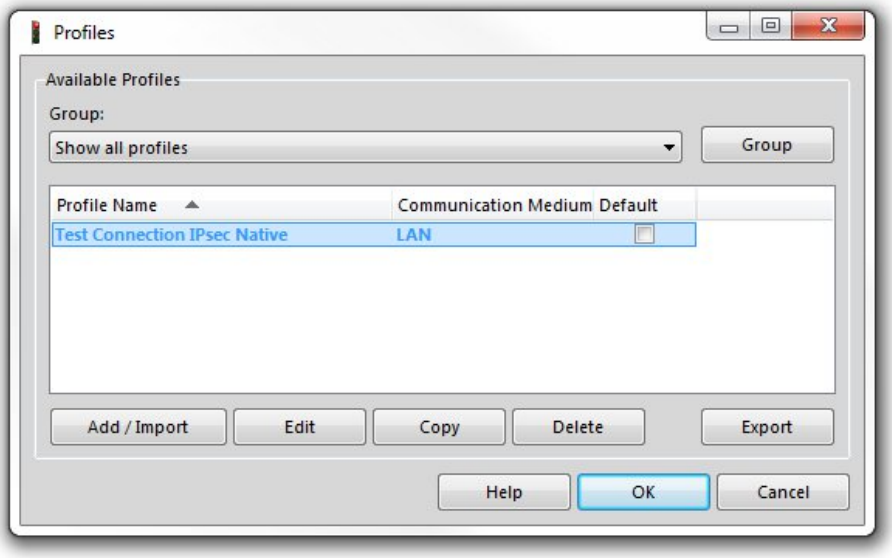


Figure 15: NCP Secure Entry Client – Profiles

Add a new profile using the *Add/Import* button. On the second screen, you must enter the profile name. In other cases (on the other screens) it is possible only to confirm using the *Next* button (on the last screen using the *Finish* button) and make the necessary settings later.

Configuration of the IPsec tunnel is done by marking the profile and pressing *Edit* button.

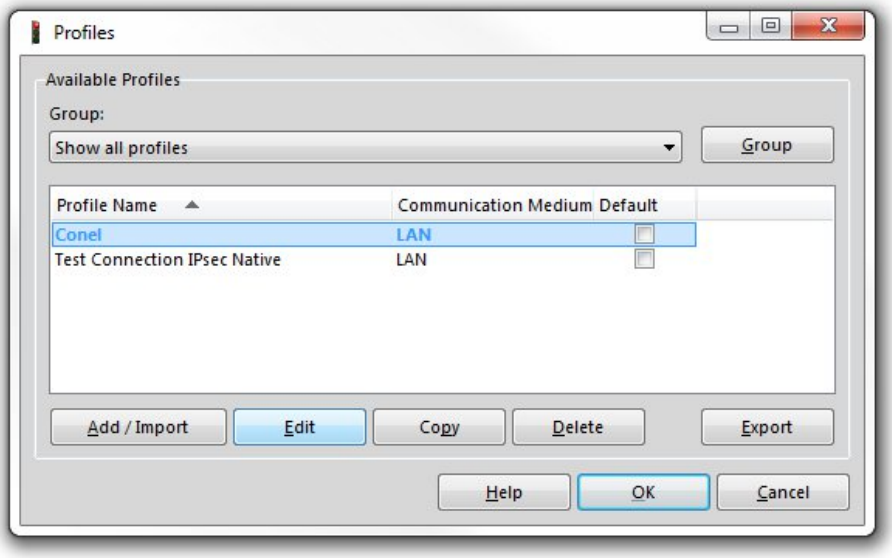


Figure 16: NCP Secure Entry Client – Edit

Select *IPsec General Settings* item in the menu on the left side. Then press *Police Editor. . .* button on the right side.

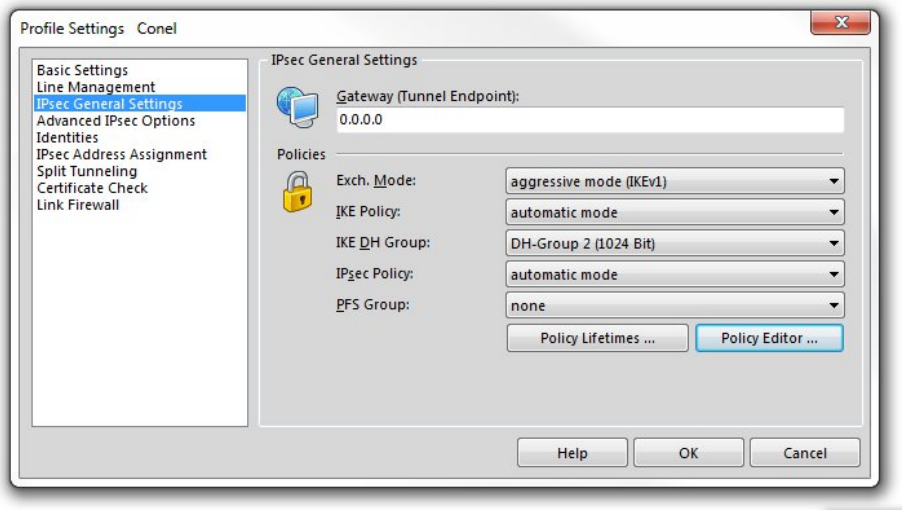


Figure 17: NCP Secure Entry Client – IPsec General Settings

In the new window highlight the *Pre-shared Key* item (in *IKE Policy* section) and then press *Edit* button.

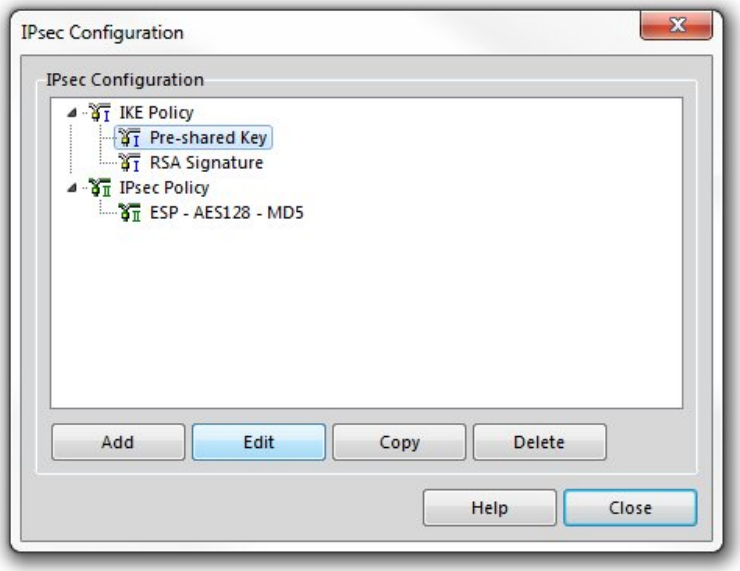


Figure 18: NCP Secure Entry Client – Policy Editor

This opens a window in which select encryption and hash algorithm (for example *Triple DES* and *MD5*) and then confirm by pressing the *OK* button.

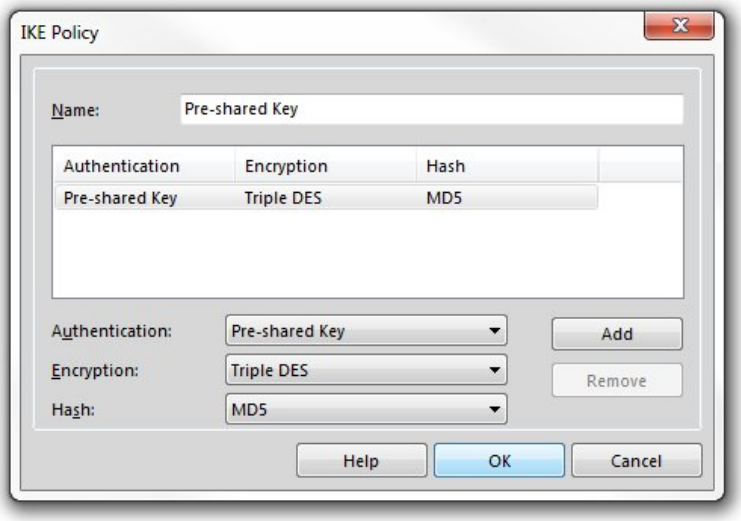


Figure 19: NCP Secure Entry Client – Pre-shared Key

Now, select the only available item in *IPsec Policy* section of configuration window. The item has a name *ESP - AES128 - MD5*. Then press *Edit* button.

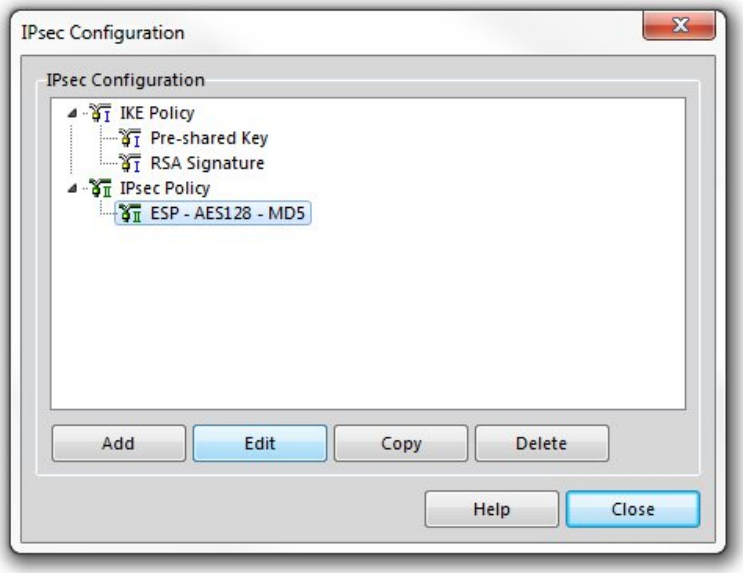


Figure 20: NCP Secure Entry Client – Policy Editor

Enter the desired name (for example *IPsec*) in the new window and select encryption and hash algorithm (for example *Triple DES* and *MD5*). Then confirm it by pressing the *OK* button.

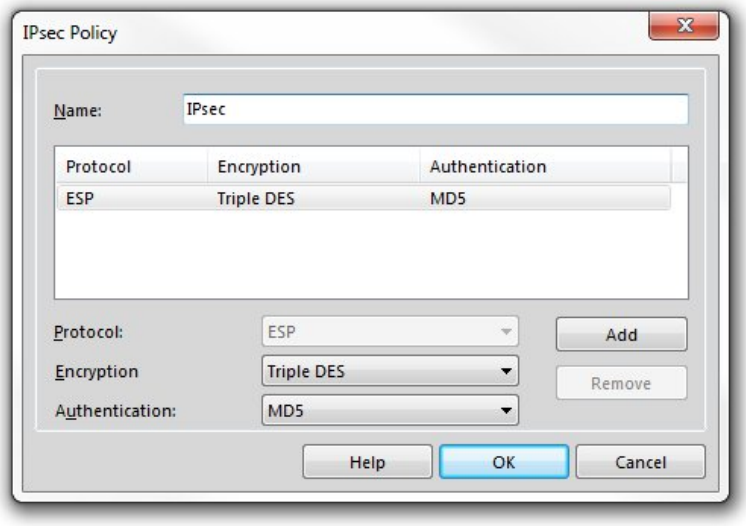


Figure 21: NCP Secure Entry Client – IPsec Policy

Go back to the main window of *IPsec General Settings* item and set *IKE Policy* and *IPsec Policy* items based on the previous configuration (see figure below). *IKE DH Group* item will have a value of *DH-Group 2 (2014 bit)*.

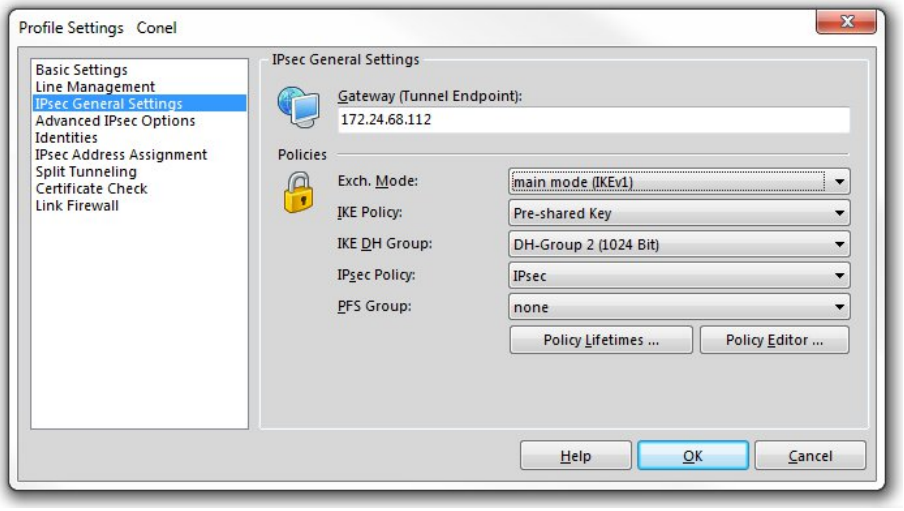


Figure 22: NCP Secure Entry Client – IPsec General Settings

Now, select *Identities* item in the menu on the left side and fill in the configuration form as shown below. Note that the IP address corresponds to the exemplary situation from the beginning of this section.

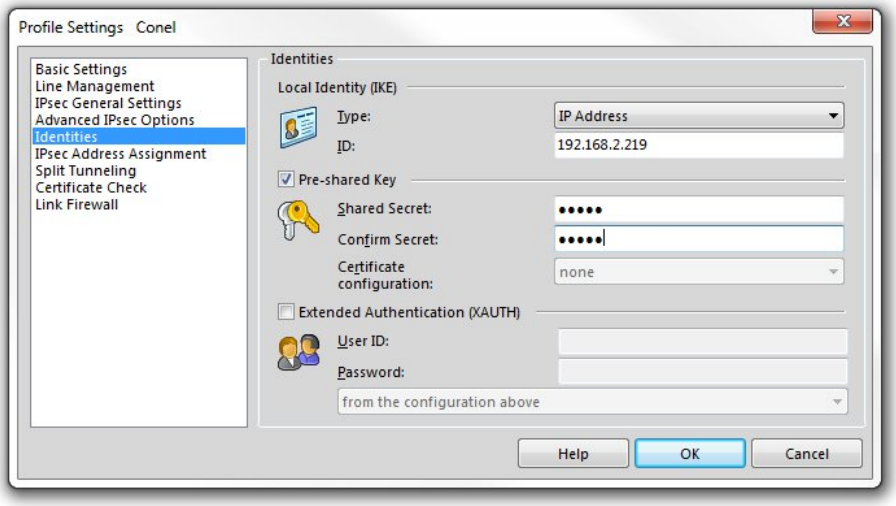


Figure 23: NCP Secure Entry Client – Identities

The same IP address (192.168.2.219 acccording to the exemplary situation) is also required on the *IPsec Address Assignment* page.

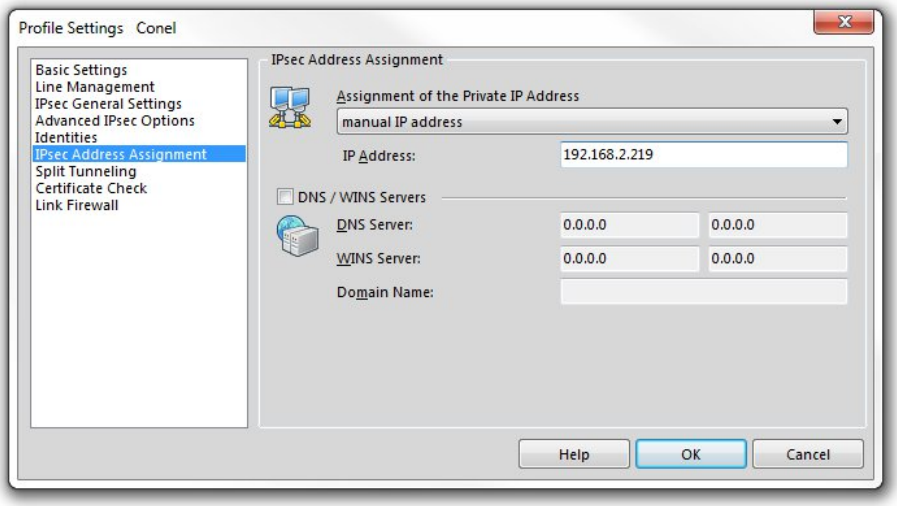


Figure 24: NCP Secure Entry Client – IPsec Address Assignment

Press *Add* button on the *Split Tunneling* page and enter the IP address of the subnet behind the router Conel (192.168.3.0 in the exemplary situation) and relevant subnet mask (255.255.255.0) to the newly opened window. Confirm it by pressing the *OK* button.

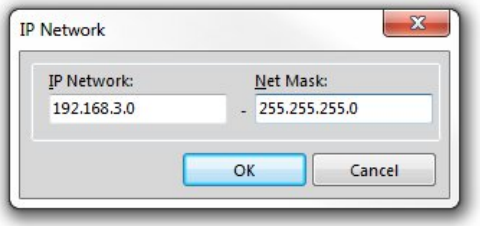


Figure 25: NCP Secure Entry Client – Add IP network

Specified data are displayed in the original window of the *Split Tunneling* page.

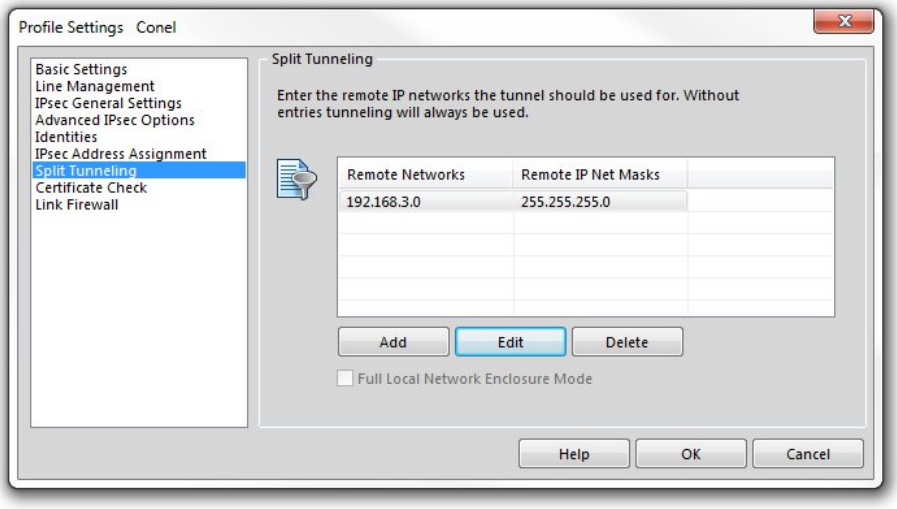


Figure 26: NCP Secure Entry Client – Split Tunneling

3.5.2 Configuration of Conel router

On the following page is displayed configuration form with IPsec tunnel settings. Entered values correspond to the exemplary situation from the beginning of this section.

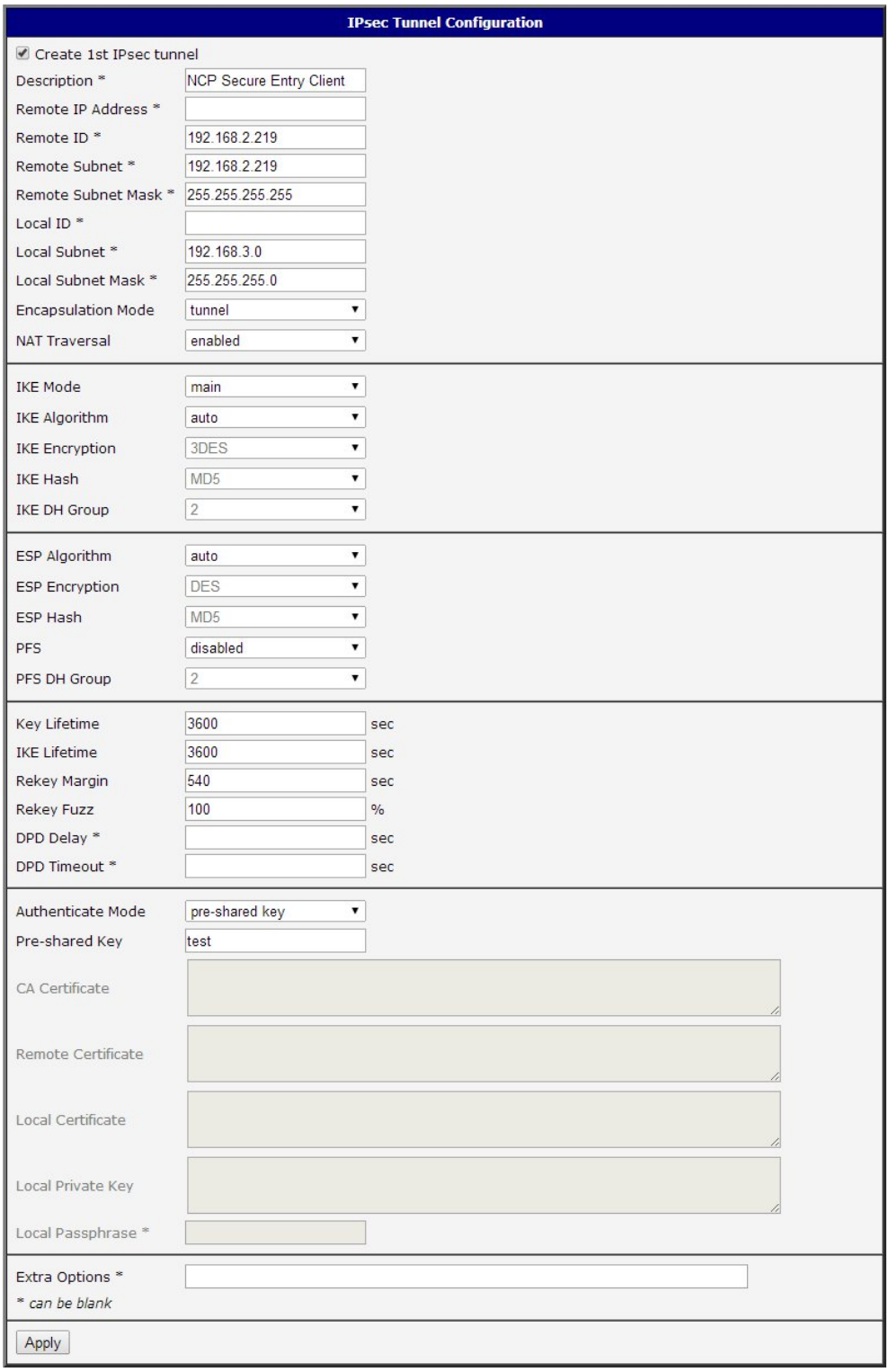


Figure 27: Configuration of Conel router

4. Recommended literature

[1] Conel: **Configuration manual for v2 routers**