



IPSec tunnel for ER75i routers application guide



Contents

1. Generally.....	3
2. IPSec limitation.....	3
3. Example of use IPSec tunnel – Client side at ER75i.....	4
3.1. IPSec tunnel – client side at ER75i.....	4
3.1.1. Web configuration in ER75i.....	4
3.1.1.1. Web interface in ER75i.....	4
3.1.1.2. IPSec tunnel web configuration in ER75i.....	5
3.1.1.3. IPSec status in ER75i.....	6
3.1.1.4. IPSec status in ER75i.....	6
3.2. IPSec tunnel – server side at ER75i.....	7
3.2.1. Web configuration in ER75i.....	7
3.2.1.1. Web interface in ER75i.....	7
3.2.1.2. IPSec tunnel web configuration in ER75i.....	8
3.2.1.3. IPSec status in ER75i.....	9
3.2.1.4. IPSec status in ER75i.....	9
3.3. Linux server configuration.....	10
3.4. CISCO configuration statement.....	11
3.4.1. CISCO configuration – client at ER75i side.....	11
3.4.2. CISCO configuration – server at ER75i side.....	16
3.5. IPSec configuration in Windows.....	21
3.5.1. IPSec configuration in the NCP Secure Entry Client program.....	21
3.5.1.1. NCP Secure Entry Client program interface.....	21
3.5.1.2. Profile settings for IPSec tunnel establishment.....	22
3.5.1.3. IPSec tunnel configuration – main settings.....	22
3.5.1.4. IKE policy configuration.....	23
3.5.1.5. IPSec policy configuration.....	24
3.5.1.6. Identification configuration.....	25
3.5.1.7. IPSec address assignment configuration.....	25
3.5.1.8. Remote network configuration.....	26
3.5.1.9. ER75i configuration.....	26

Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Issue in CZ, 08/04/08



1. Generally

IPsec (Internet Protocol Security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.

- Authenticating – receiving packet process can authenticate sent packet to match existing sender. (1st phase, IKE phase, Main mode) In PSK it finished by changing the keys.
- Encrypting – the both sides prearrange the packet encrypting. Follow step to encrypting the packet except the IP header, eventually encrypting complete packet and new IP header adding. (2nd Phase, IPsec phase, Quick mode) End by tunnel establishment.

IPsec also includes protocols for cryptographic key establishment. IPsec protocols operate at the network OSI model layer 3.

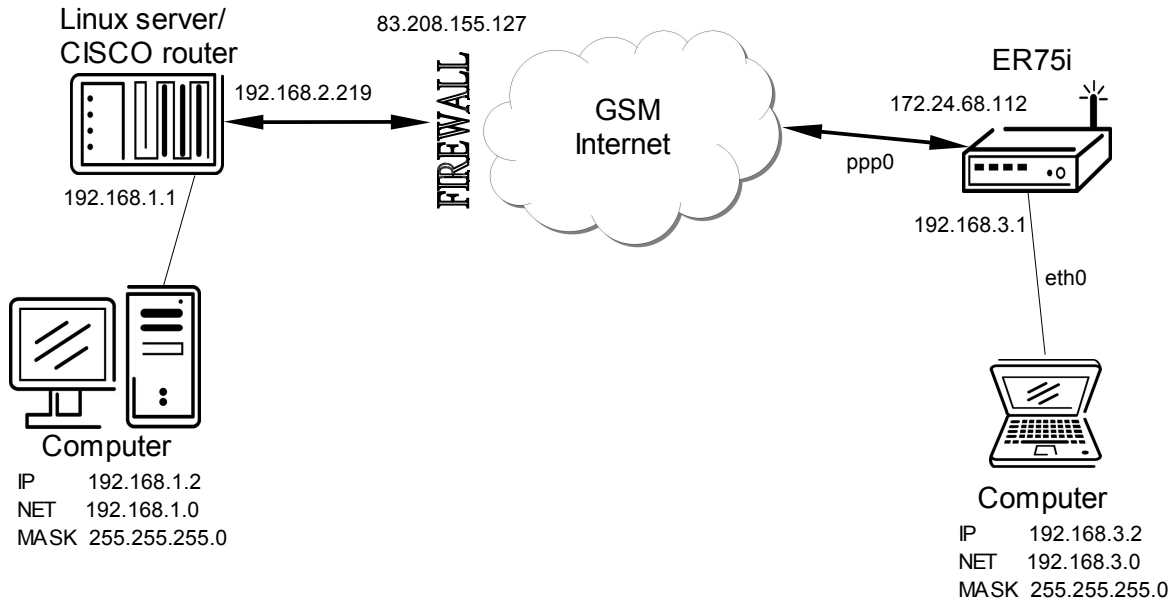
NAT-T (eventually NAT-Traversal) is shortcut for Network Address Translation Traversal. NAT is technology which serves to sharing of the one public IP address from non public network segment. It enables connection from the non public networks using IPsec tunnel.

2. IPsec limitation

- Only CISCO routers with IPsec support, from IOS 7.1
- Only ER75i routers with IPsec support, from firmware V1.1.1

3. Example of use IPsec tunnel – Client side at ER75i

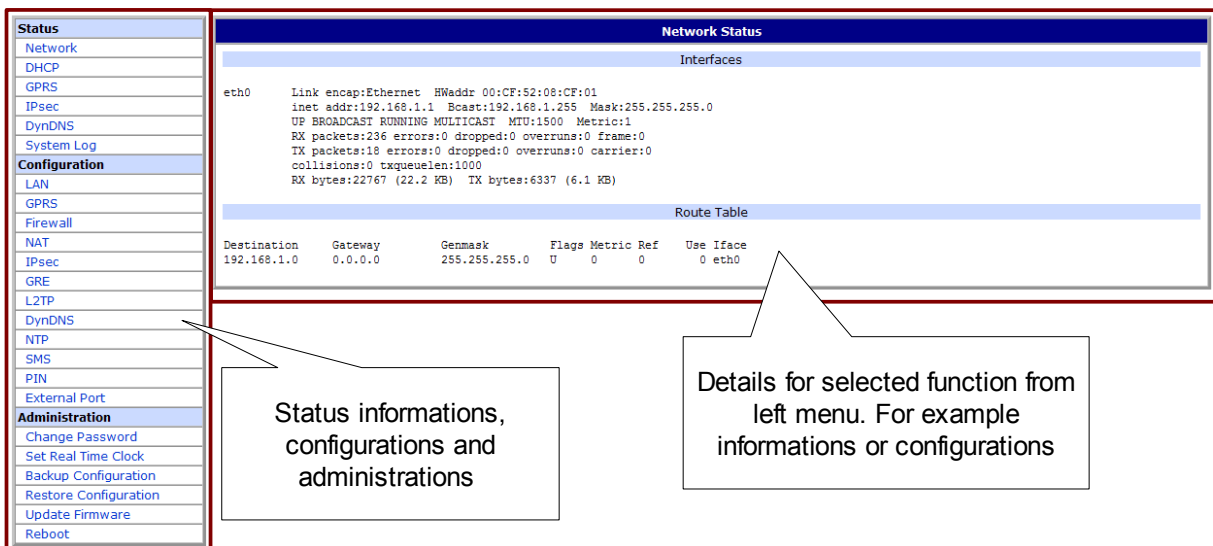
3.1. IPsec tunnel – client side at ER75i



3.1.1. Web configuration in ER75i

3.1.1.1. Web interface in ER75i

EDGE router ER75i



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)
```

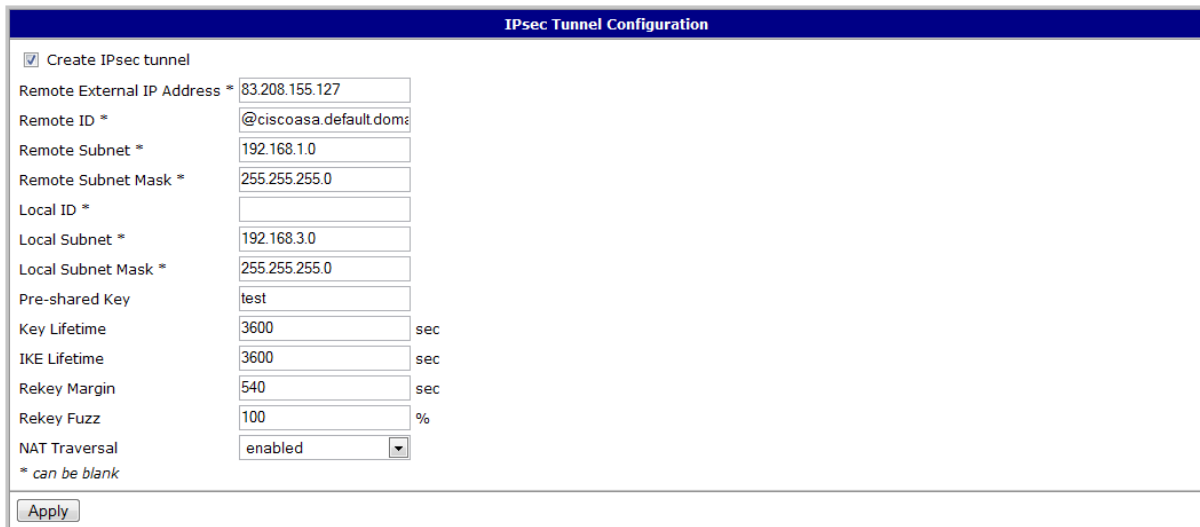
Route Table

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 informations, configurations and administrations

Details for selected function from left menu. For example informations or configurations

3.1.1.2. IPSec tunnel web configuration in ER75i



Remote ID **@ciscoasa.default.domain** is from two parts:

hostname: ciscoasa
domain-name: default.domain

When your network used address translation, then must be enabled NAT Traversal.

The IPsec setting is possible see on the next table.

Configuration	ER75i
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

The other settings is possible leave in default state. If „Remote External IP Address“ is blank in one side configuration then this side will wait connection and don't try establish connection itself.

Items, which can be blank, are used to exact tunnel identification.

3.1.1.3. IPsec status in ER75i

Example of successful IPsec tunnel establishment.

```

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

```

You can see choose encryption by tunnel establishment phases:

ER75i IKE: 3DES_CBC_192-MD5-MODP1024 IPsec: 3DES_0-HMAC_MD5, pfsgroup = none

In red cover is information about successful tunnel establishment.

3.1.1.4. IPsec status in ER75i

```

Network Status
Interfaces

eth0      Link encap:Ethernet  HWaddr 00:CF:52:08:CF:01
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:802 errors:0 dropped:0 overruns:0 frame:0
          TX packets:504 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:74844 (73.0 KB)  TX bytes:126074 (123.1 KB)

ipsec0    Link encap:Point-Point Protocol
          inet addr:10.0.2.36  Mask:255.255.255.255
          UP RUNNING NOARP  MTU:16260  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:218 (218.0 B)  TX bytes:5200 (5.0 KB)

ppp0      Link encap:Point-Point Protocol
          inet addr:10.0.2.36  P-t-P:10.0.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:205 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:12930 (12.6 KB)  TX bytes:22540 (22.0 KB)

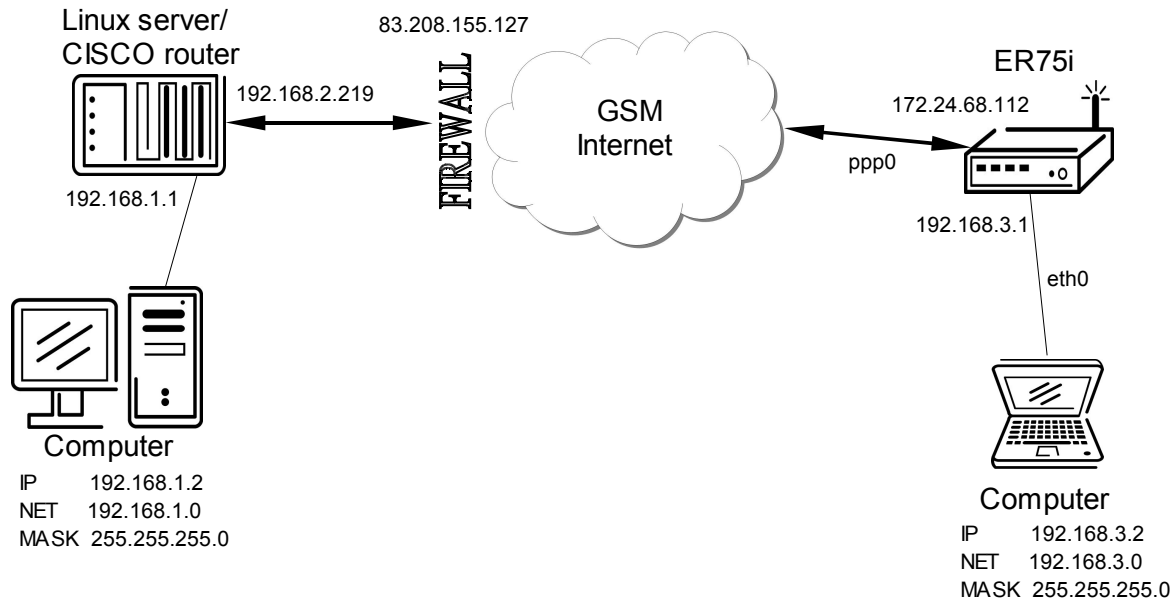
Route Table

Destination  Gateway      Genmask      Flags Metric Ref  Use Iface
83.208.155.127  0.0.0.0      255.255.255.255  UH  0    0    0  ppp0
192.168.3.0    0.0.0.0      255.255.255.0   U   0    0    0  eth0
192.168.2.0    0.0.0.0      255.255.255.0   U   0    0    0  ipsec0
0.0.0.0        83.208.155.127  0.0.0.0         UG  0    0    0  ppp0

```

In Network Status you can see IPsec interface status and ER75i route table after IPsec tunnel establishment.

3.2. IPsec tunnel – server side at ER75i

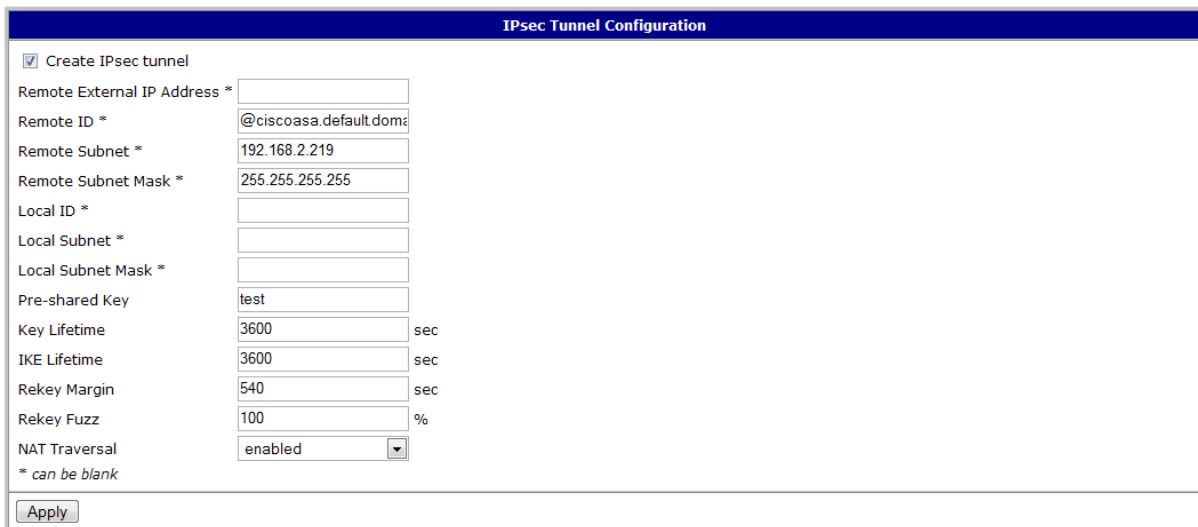


3.2.1. Web configuration in ER75i

3.2.1.1. Web interface in ER75i

See chapter 3.1.1.1.

3.2.1.2. IPsec tunnel web configuration in ER75i



The screenshot shows the 'IPsec Tunnel Configuration' web interface. It includes a checkbox for 'Create IPsec tunnel' which is checked. Below this are several input fields: 'Remote External IP Address *', 'Remote ID *' (containing '@ciscoasa.default.domain'), 'Remote Subnet *' (192.168.2.219), 'Remote Subnet Mask *' (255.255.255.255), 'Local ID *', 'Local Subnet *', 'Local Subnet Mask *', 'Pre-shared Key' (test), 'Key Lifetime' (3600 sec), 'IKE Lifetime' (3600 sec), 'Rekey Margin' (540 sec), 'Rekey Fuzz' (100 %), and 'NAT Traversal' (enabled). A note at the bottom states '* can be blank'. An 'Apply' button is located at the bottom left.

Remote ID **@ciscoasa.default.domain** is from two parts:

hostname: ciscoasa
domain-name: default.domain

When your network used address translation, then must be enabled NAT Traversal.

The IPsec setting is possible see on the next table.

Configuration	ER75i
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

The other settings is possible leave in default state. If „Remote External IP Address“ is blank in one side configuration then this side will wait connection and don't try establish connection itself.

Items, which can be blank, are used to exact tunnel identification.

3.2.1.3. IPsec status in ER75i

Example of successful IPsec tunnel establishment.

```

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

```

You can see choose encryption by tunnel establishment phases:

ER75i IKE: 3DES_CBC_192-MD5-MODP1024 IPsec: 3DES_0-HMAC_MD5, pfsgroup = none

In red cover is information about successful tunnel establishment.

3.2.1.4. IPsec status in ER75i

```

Network Status
Interfaces

eth0    Link encap:Ethernet HWaddr 00:CF:52:08:CF:01
        inet addr:192.168.3.1 Bcast:192.168.3.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:802 errors:0 dropped:0 overruns:0 frame:0
        TX packets:504 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:74844 (73.0 KB) TX bytes:126074 (123.1 KB)

ipsec0  Link encap:Point-Point Protocol
        inet addr:10.0.2.36 Mask:255.255.255.255
        UP RUNNING NOARP MTU:16260 Metric:1
        RX packets:2 errors:0 dropped:0 overruns:0 frame:0
        TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:10
        RX bytes:218 (218.0 B) TX bytes:5200 (5.0 KB)

ppp0    Link encap:Point-Point Protocol
        inet addr:10.0.2.36 P-t-P:10.0.0.1 Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
        RX packets:205 errors:0 dropped:0 overruns:0 frame:0
        TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:3
        RX bytes:12930 (12.6 KB) TX bytes:22540 (22.0 KB)

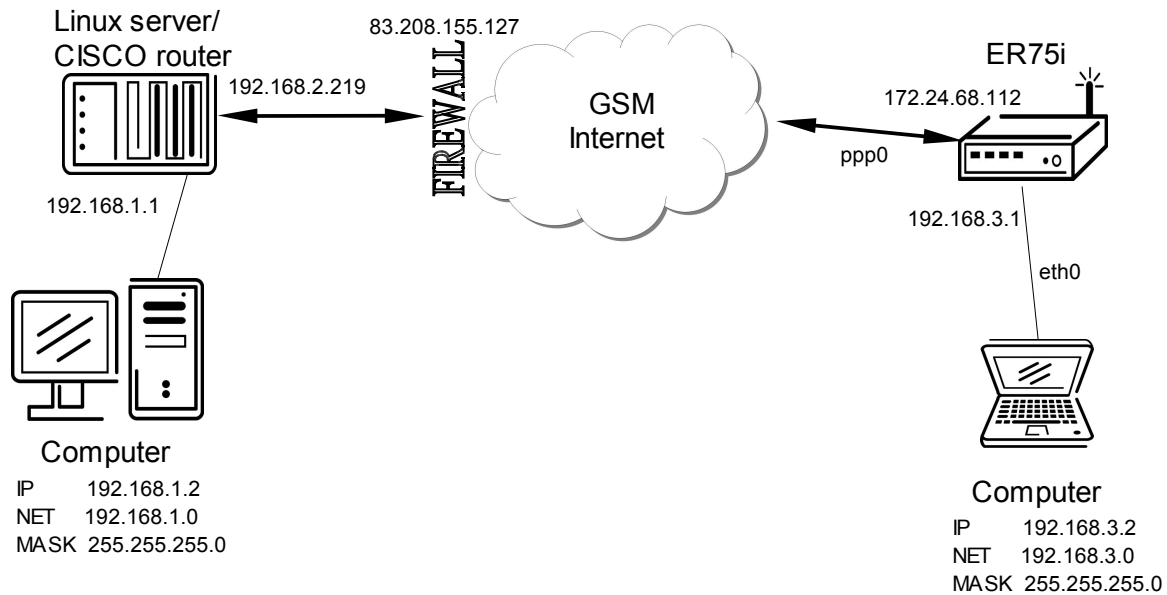
Route Table

Destination Gateway Genmask Flags Metric Ref Use Iface
83.208.155.127 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 ipsec0
0.0.0.0 83.208.155.127 0.0.0.0 UG 0 0 0 ppp0

```

In Network Status you can see IPsec interface status and ER75i route table after IPsec tunnel establishment.

3.3. Linux server configuration



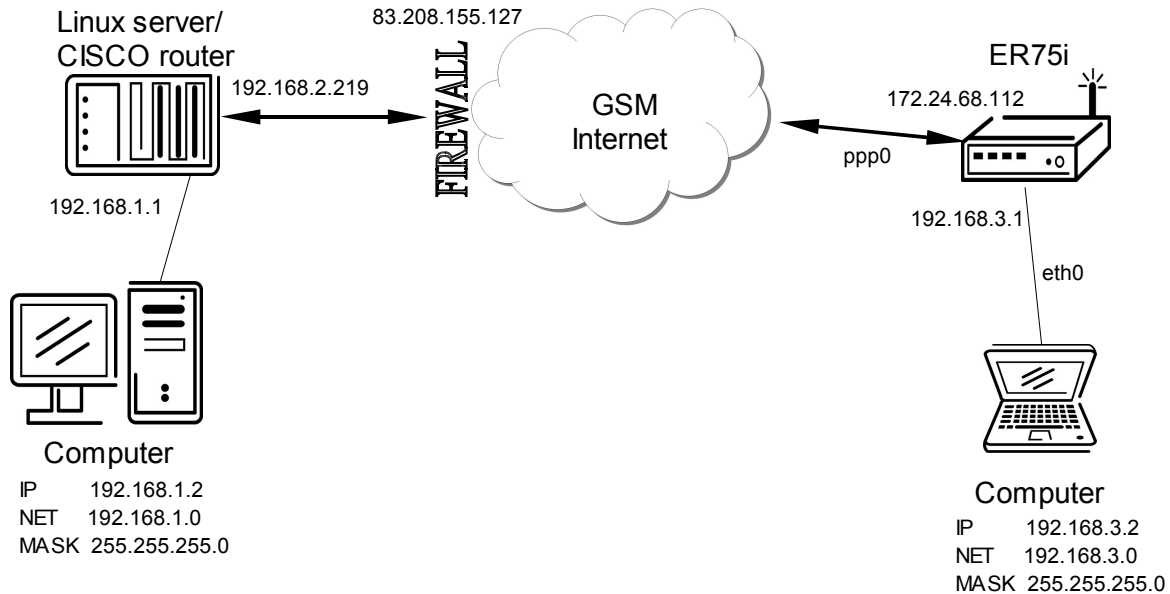
It is need configurate file *ipsec.conf*.

```
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
```

It is need set of the configuration file *ipsec.secrets*.

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

3.4. CISCO configuration statement



3.4.1. CISCO configuration – client at ER75i side

```

ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain
enable password 8Ry2Yjlyt7RRXU24 encrypted
names
!
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
11

```



```
!  
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  
12
```



```
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
```

13



```
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
```

14



```
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. CISCO configuration – server at ER75i side

```
ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain
enable password 8Ry2Yjlyt7RRXU24 encrypted
names
!
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
```

17



```
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
```

18



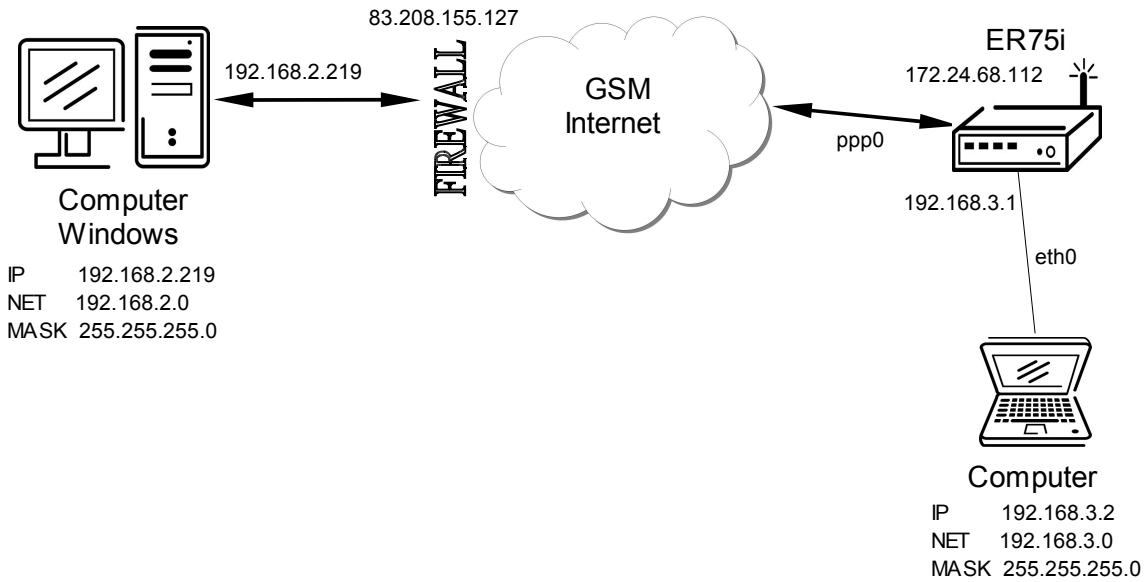
```
inspect ipsec-pass-thru
!  
service-policy global_policy global  
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5  
group-policy DfltGrpPolicy attributes  
banner none  
wins-server none  
dns-server none  
dhcp-network-scope none  
vpn-access-hours none  
vpn-simultaneous-logins 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
```

19



```
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 us
e 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 configuration in Windows

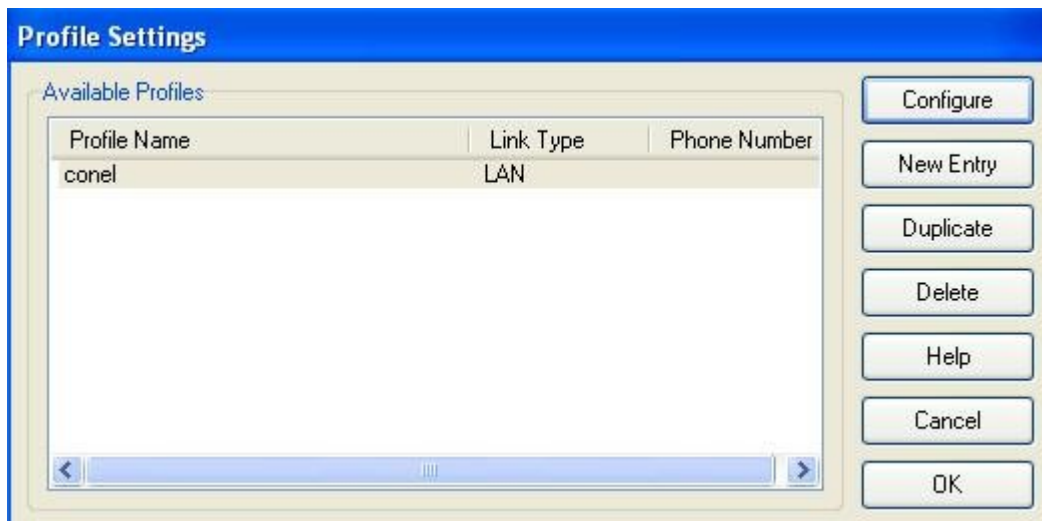


3.5.1. IPSec configuration in the NCP Secure Entry Client program

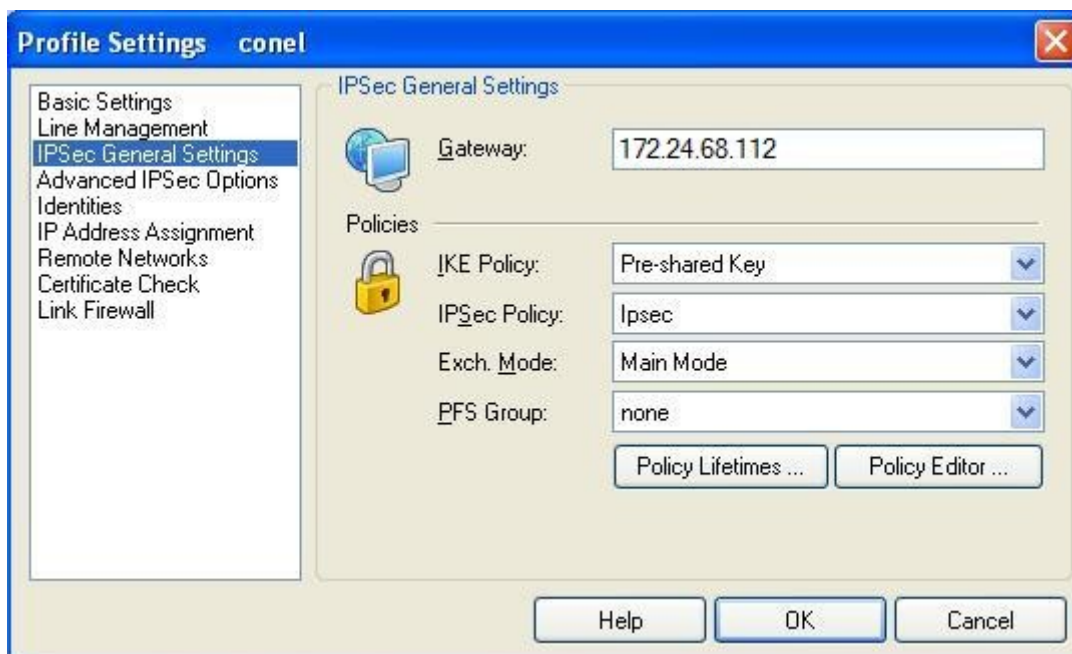
3.5.1.1. NCP Secure Entry Client program interface



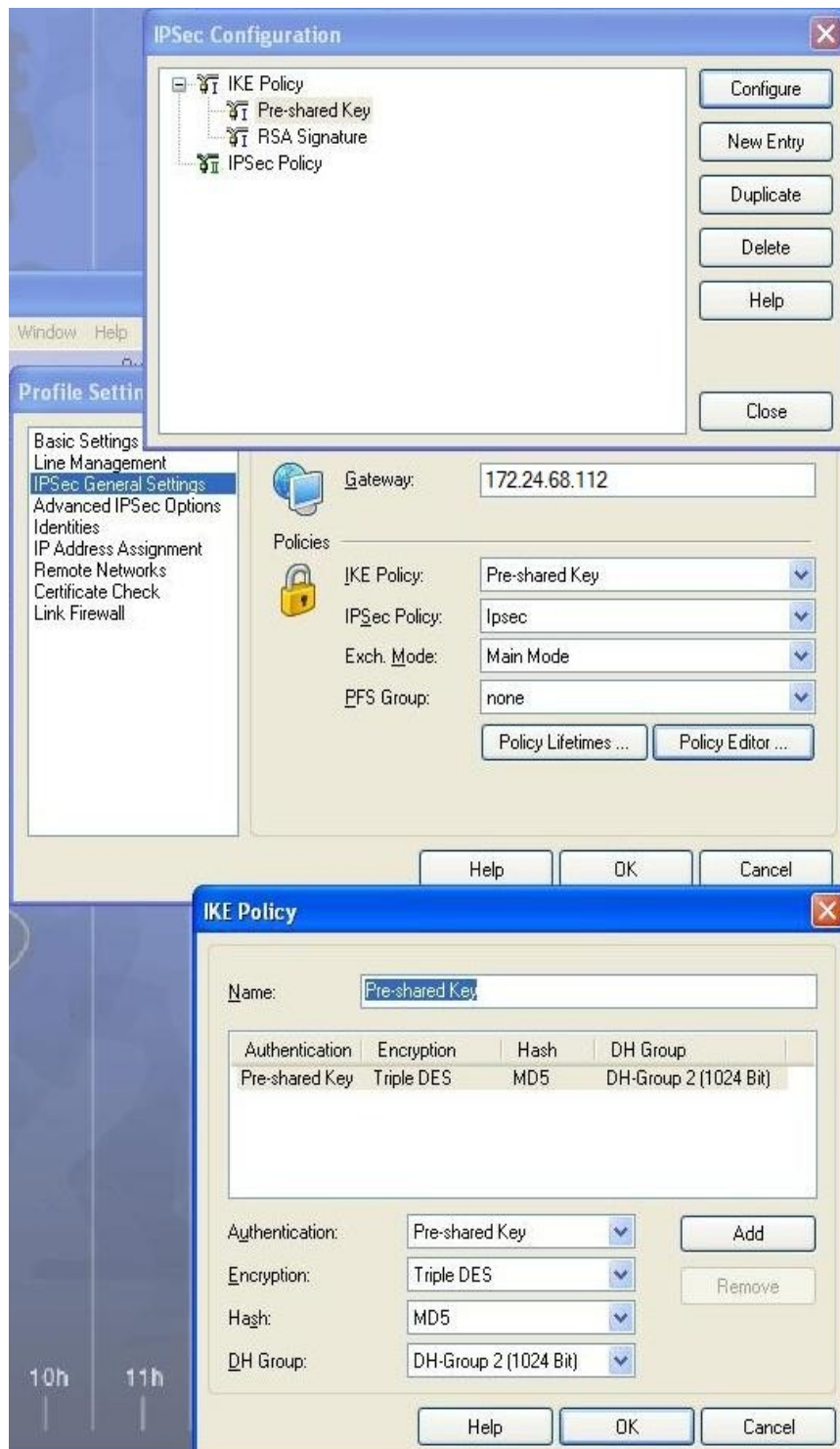
3.5.1.2. Profile settings for IPSec tunnel establishment



3.5.1.3. IPSec tunnel configuration – main settings



3.5.1.4. IKE policy configuration



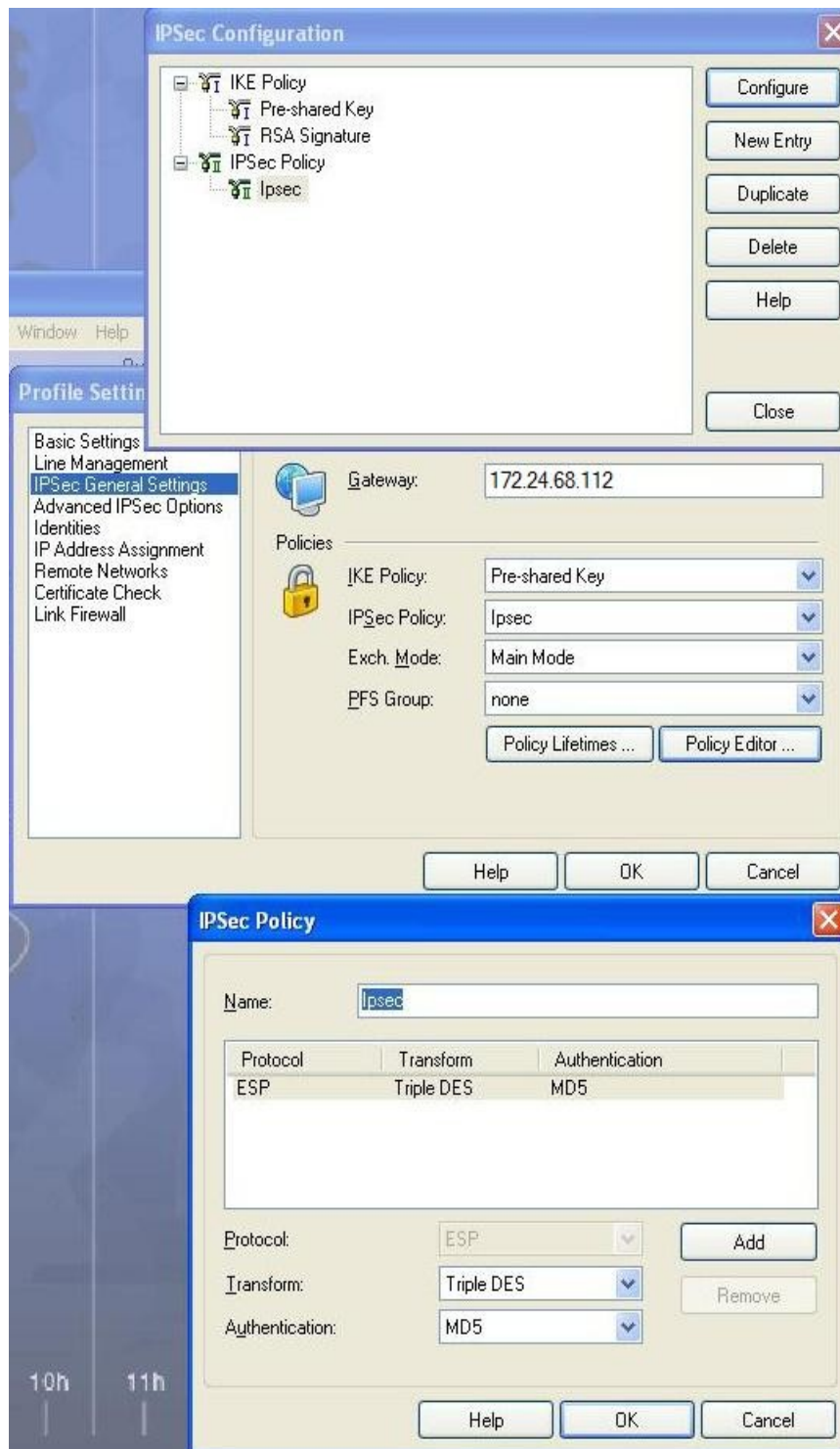
The screenshot shows two windows from a network configuration application. The top window is titled "IPSec Configuration" and displays a tree view on the left with "IKE Policy" selected. On the right, there are buttons for "Configure", "New Entry", "Duplicate", "Delete", "Help", and "Close". Below the tree view, the "Gateway" is set to "172.24.68.112". Under the "Policies" section, "IKE Policy" is set to "Pre-shared Key", "IPsec Policy" is set to "Ipsec", "Exch. Mode" is set to "Main Mode", and "PFS Group" is set to "none". There are also buttons for "Policy Lifetimes ..." and "Policy Editor ...".

The bottom window is titled "IKE Policy" and shows the configuration for the selected "Pre-shared Key" policy. The "Name" field contains "Pre-shared Key". Below this is a table with columns for Authentication, Encryption, Hash, and DH Group.

Authentication	Encryption	Hash	DH Group
Pre-shared Key	Triple DES	MD5	DH-Group 2 (1024 Bit)

Below the table, there are dropdown menus for "Authentication" (Pre-shared Key), "Encryption" (Triple DES), "Hash" (MD5), and "DH Group" (DH-Group 2 (1024 Bit)). There are "Add" and "Remove" buttons to the right of these dropdowns. At the bottom of the window are "Help", "OK", and "Cancel" buttons.

3.5.1.5. IPSec policy configuration



The screenshot shows two windows from a network configuration application. The top window is titled "IPSec Configuration" and displays a tree view with "IKE Policy" (containing "Pre-shared Key" and "RSA Signature") and "IPSec Policy" (containing "Ipsec"). On the right side of this window are buttons for "Configure", "New Entry", "Duplicate", "Delete", "Help", and "Close".

The bottom window is titled "IPSec Policy" and shows the configuration for the "Ipsec" policy. It includes a "Name" field with "Ipsec" entered. Below this is a table of selected policies:

Protocol	Transform	Authentication
ESP	Triple DES	MD5

Below the table are dropdown menus for "Protocol" (ESP), "Transform" (Triple DES), and "Authentication" (MD5), along with "Add" and "Remove" buttons. At the bottom of the window are "Help", "OK", and "Cancel" buttons.

3.5.1.6. Identification configuration



Profile Settings conel

Identities

Local Identity

Type: Fully Qualified Domain Name

ID: @ciscoasa.default.domain

Pre-shared Key

Shared Secret: [masked]

Confirm Secret: [masked]

Extended Authentication (XAUTH)

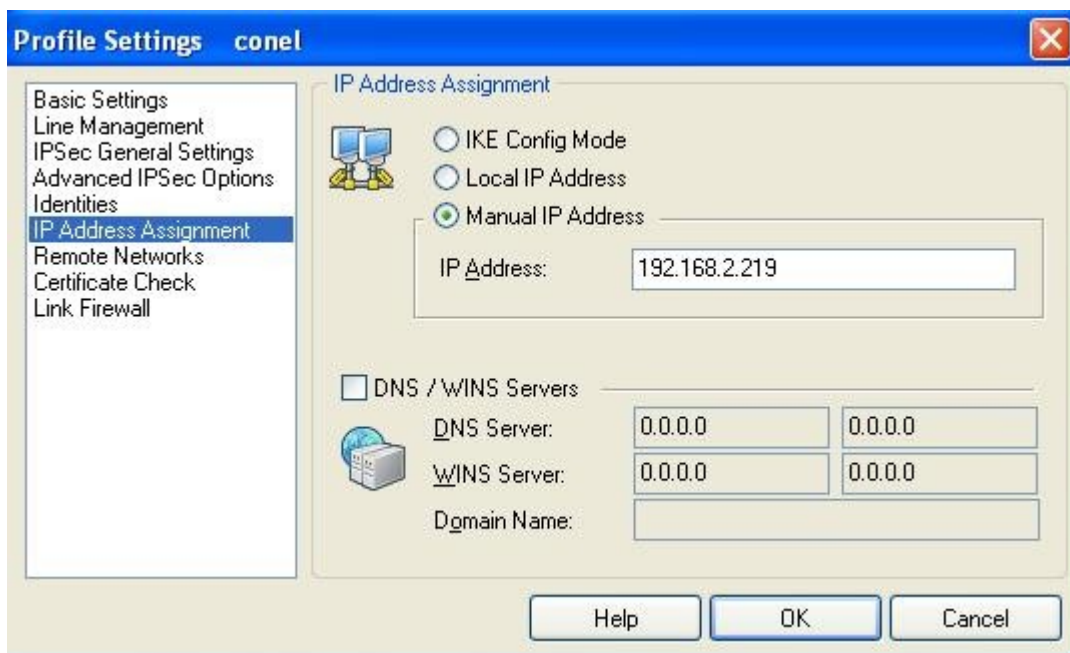
User ID: ncpipsecnative

Password: [masked]

from the configuration above

Help OK Cancel

3.5.1.7. IPsec address assignment configuration



Profile Settings conel

IP Address Assignment

IKE Config Mode

Local IP Address

Manual IP Address

IP Address: 192.168.2.219

DNS / WINS Servers

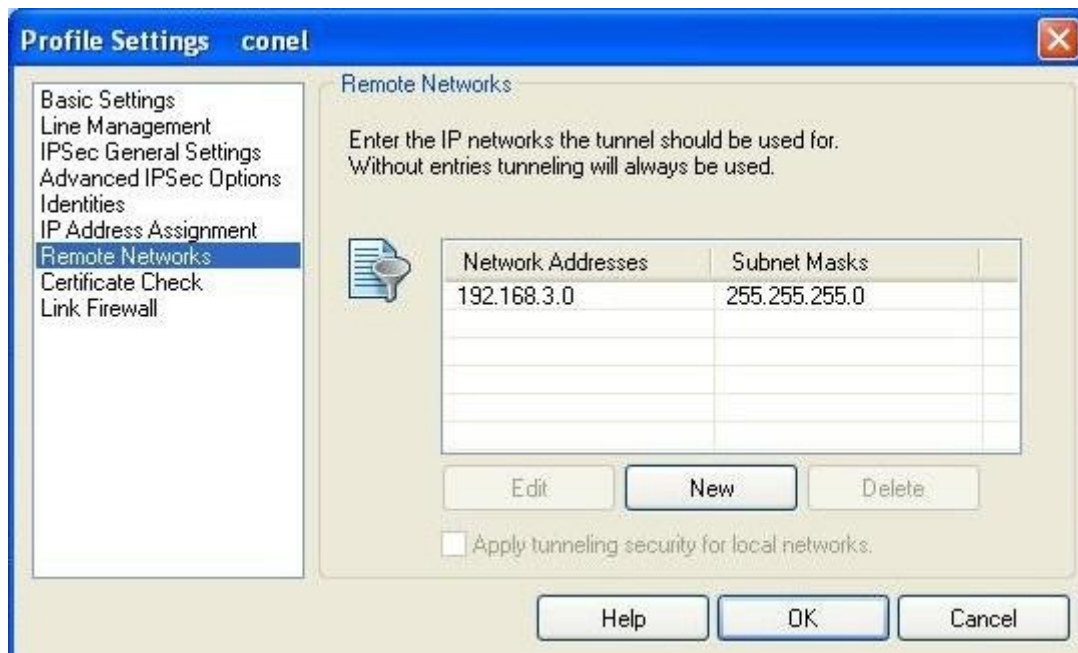
DNS Server: 0.0.0.0 0.0.0.0

WINS Server: 0.0.0.0 0.0.0.0

Domain Name:

Help OK Cancel

3.5.1.8. Remote network configuration



3.5.1.9. ER75i configuration

The ER75i router is set according to chapter 3.1.