Godinich Consulting

VPN's Between Mikrotik and 3rd Party Devices

Vince Godinich

experience

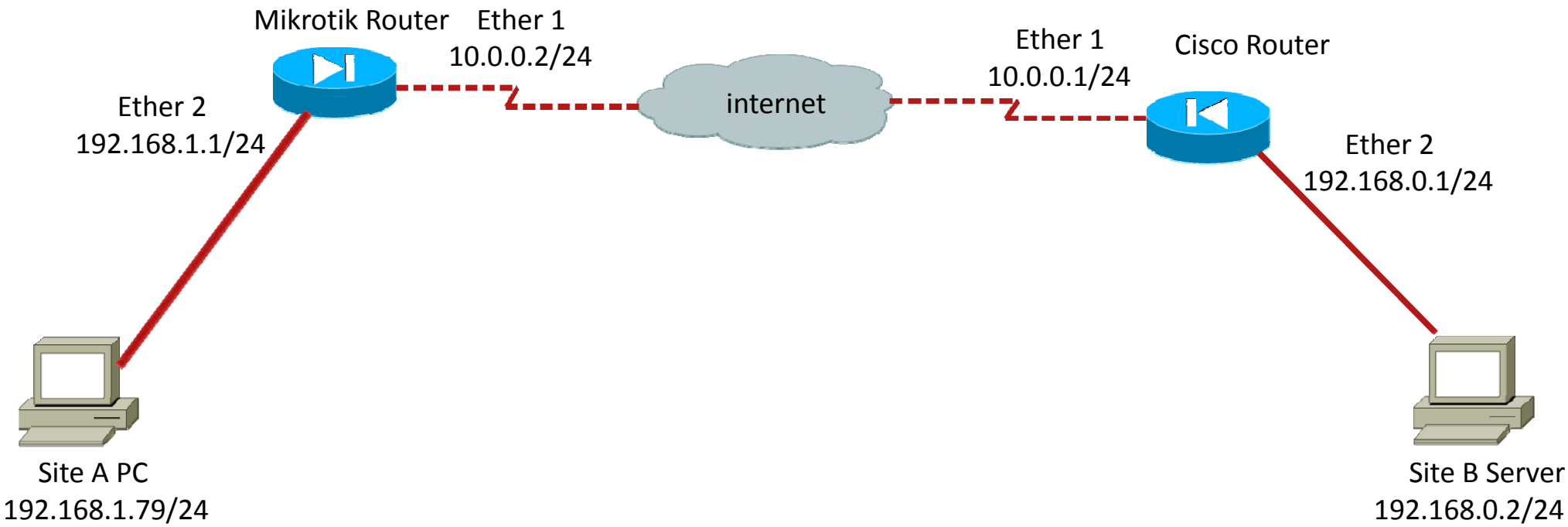
TOPICS

- PPTP Mikrotik Client to Cisco Server
- IPSEC Shrew Client To Mikrotik router
- IPSEC Mikrotik router to Cisco IOS router

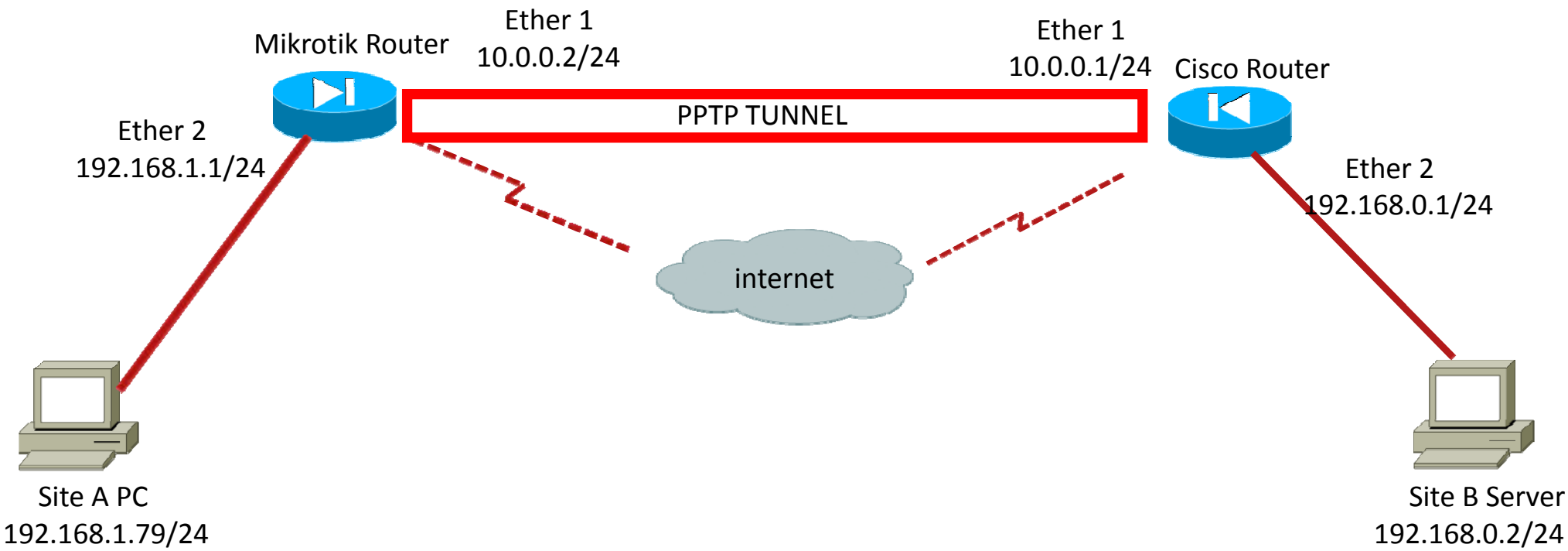
PPTP Mikrotik Client to Cisco Server

- Configure a Mikrotik router to act as a PPTP client connecting to a Cisco PPTP server to connect remote lans
- Allows replacement of a Cisco branch router with a MikroTik router without changing or replacing existing Cisco main router

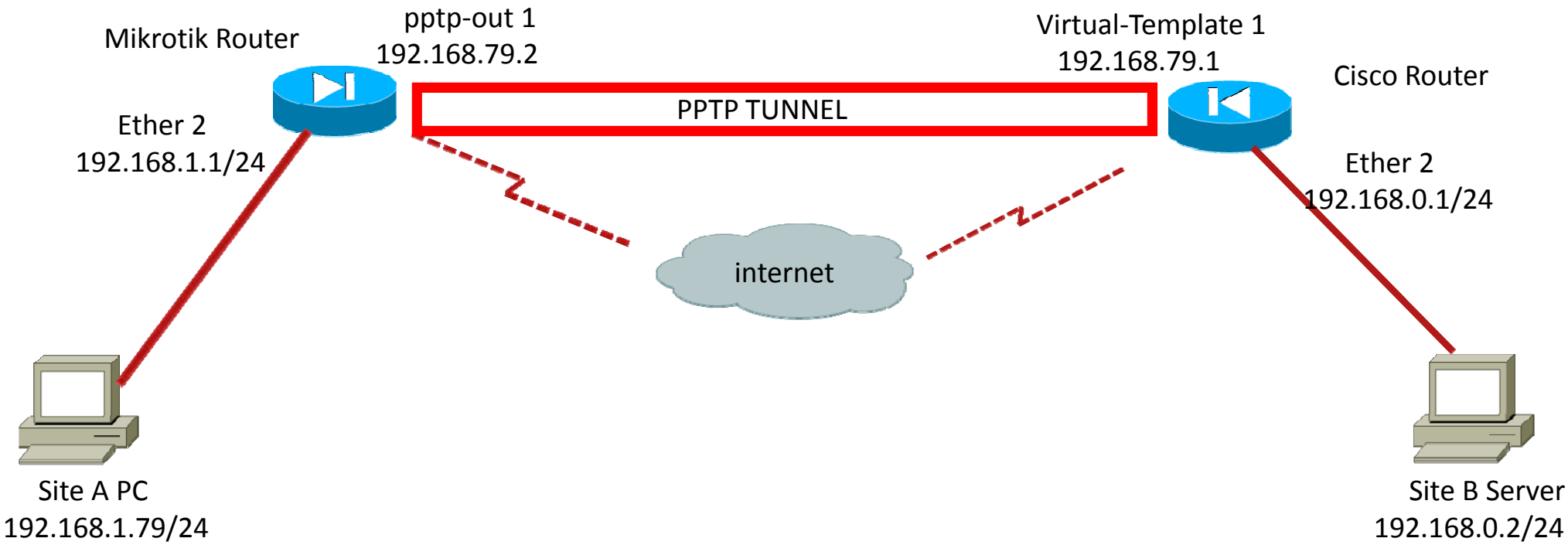
PPTP Mikrotik Client to Cisco Server



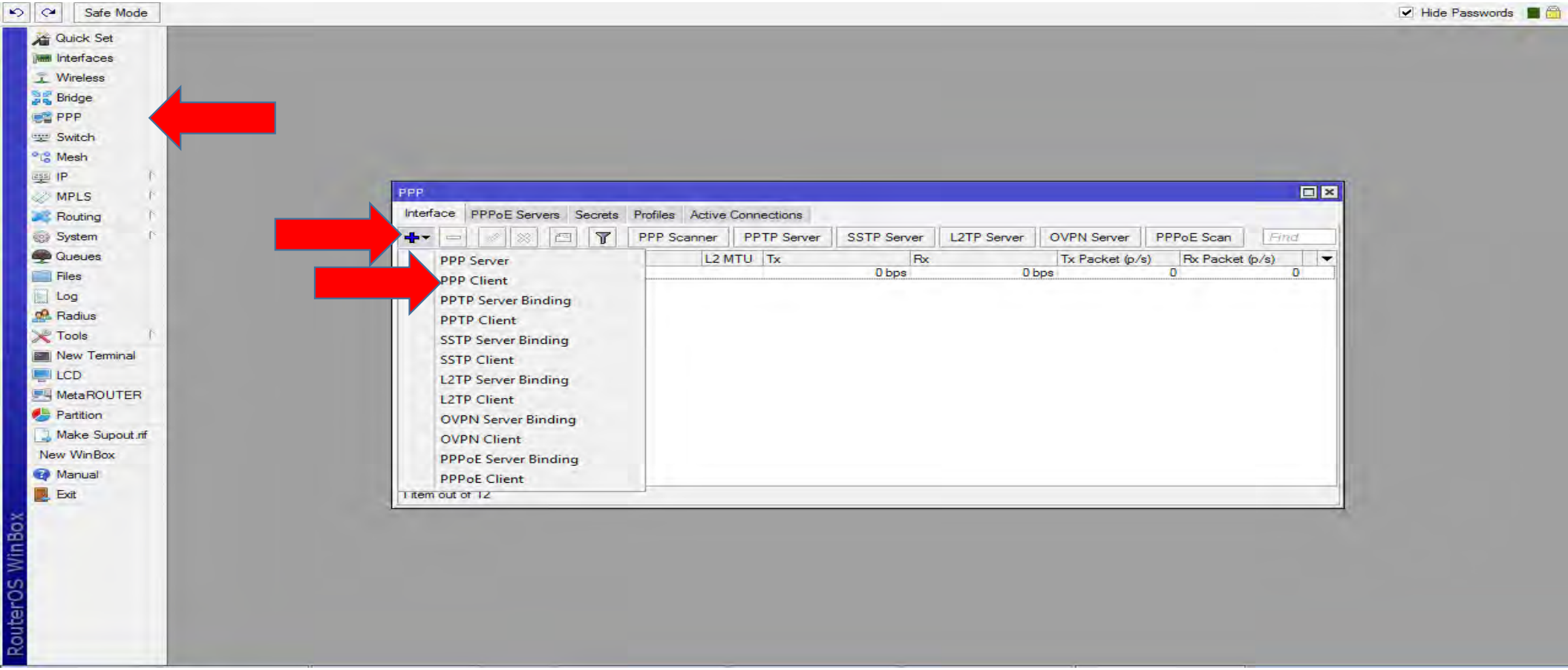
PPTP Mikrotik Client to Cisco Server



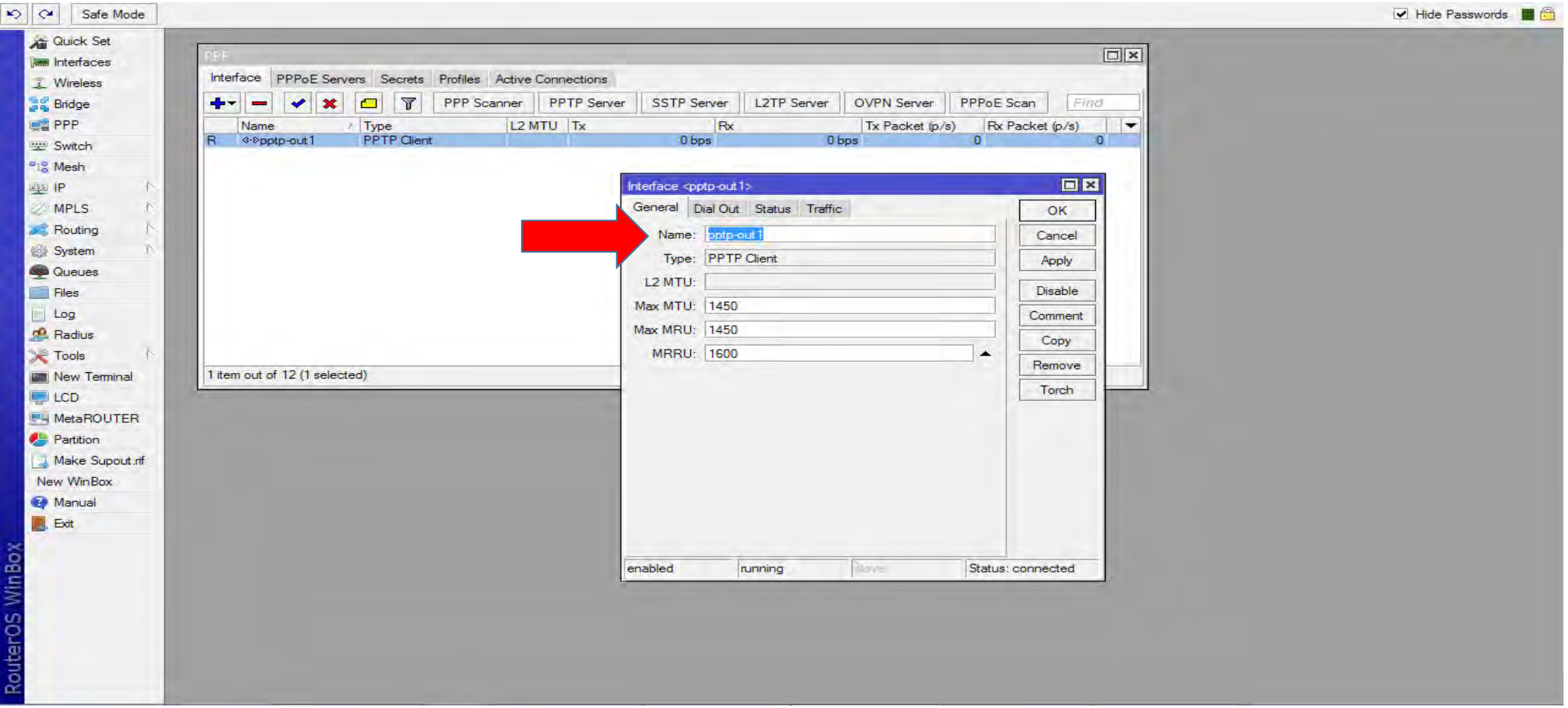
PPTP Mikrotik Client to Cisco Server



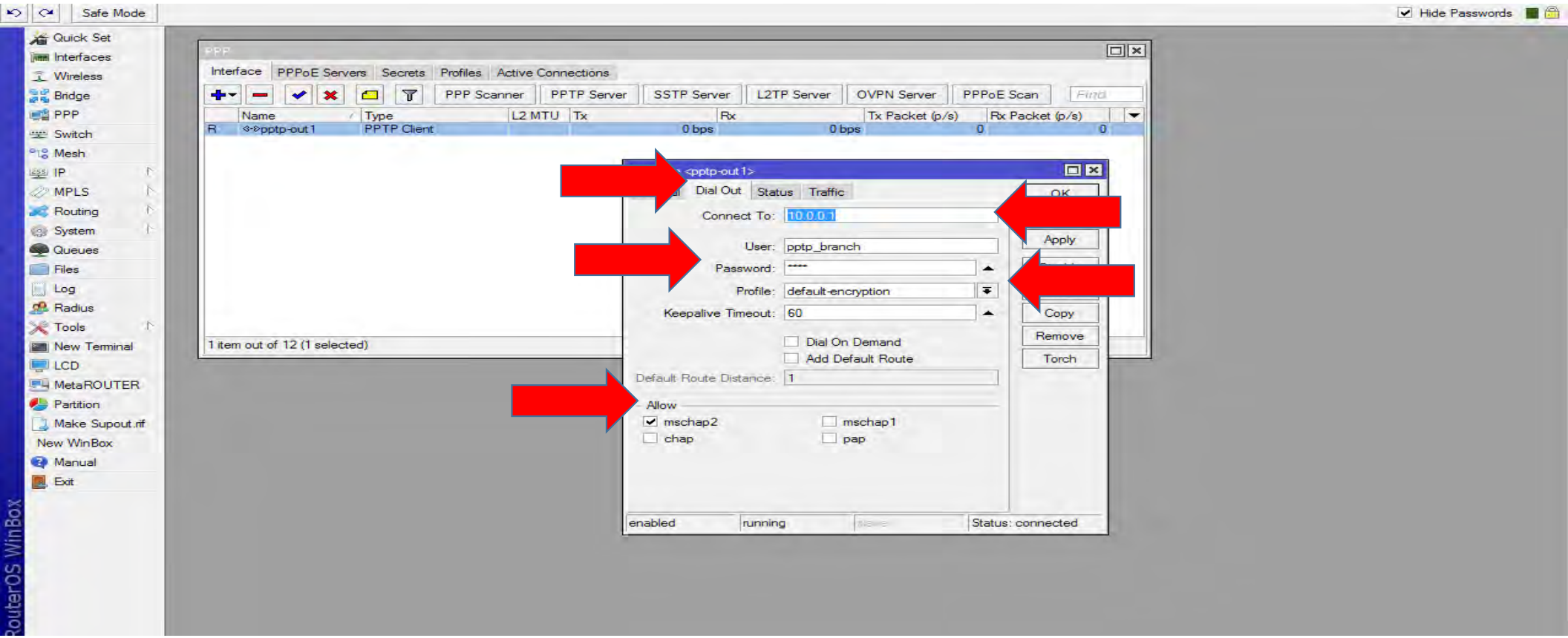
PPTP Mikrotik Client to Cisco Server



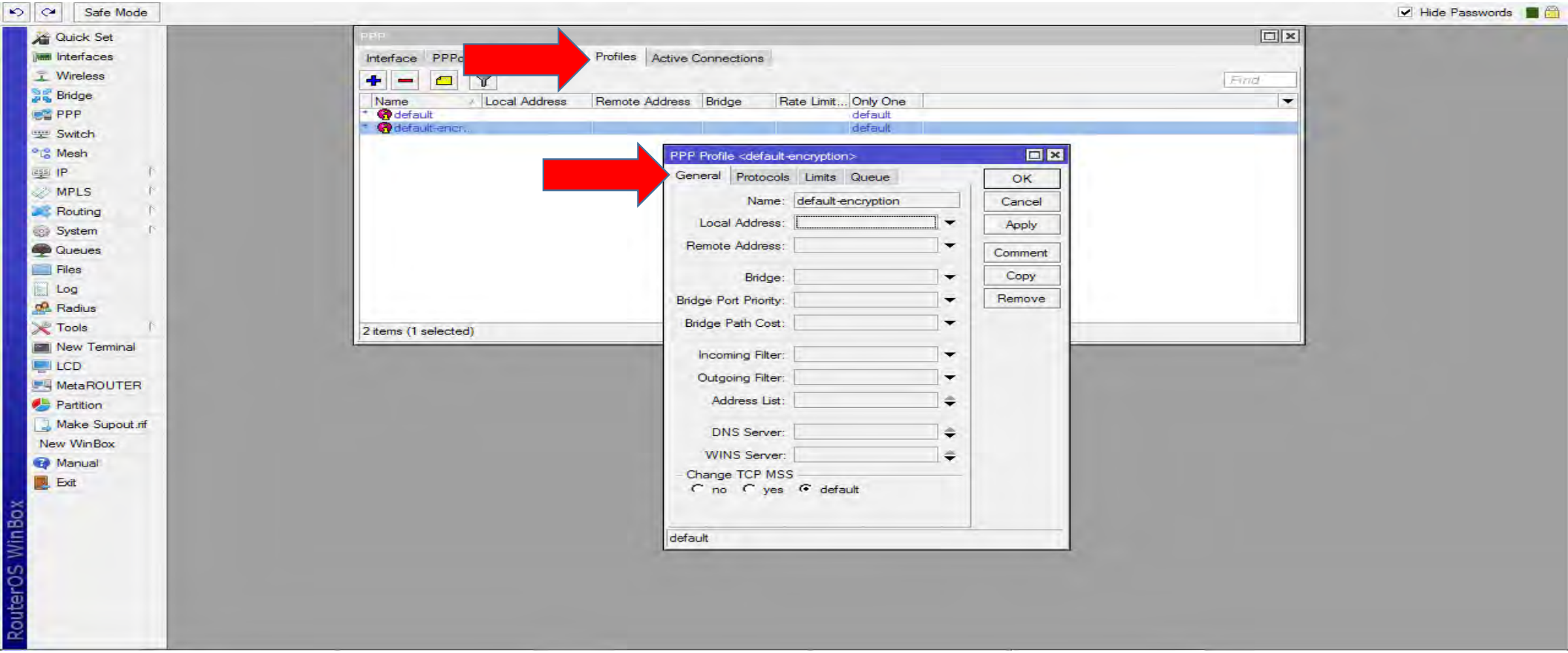
PPTP Mikrotik Client to Cisco Server



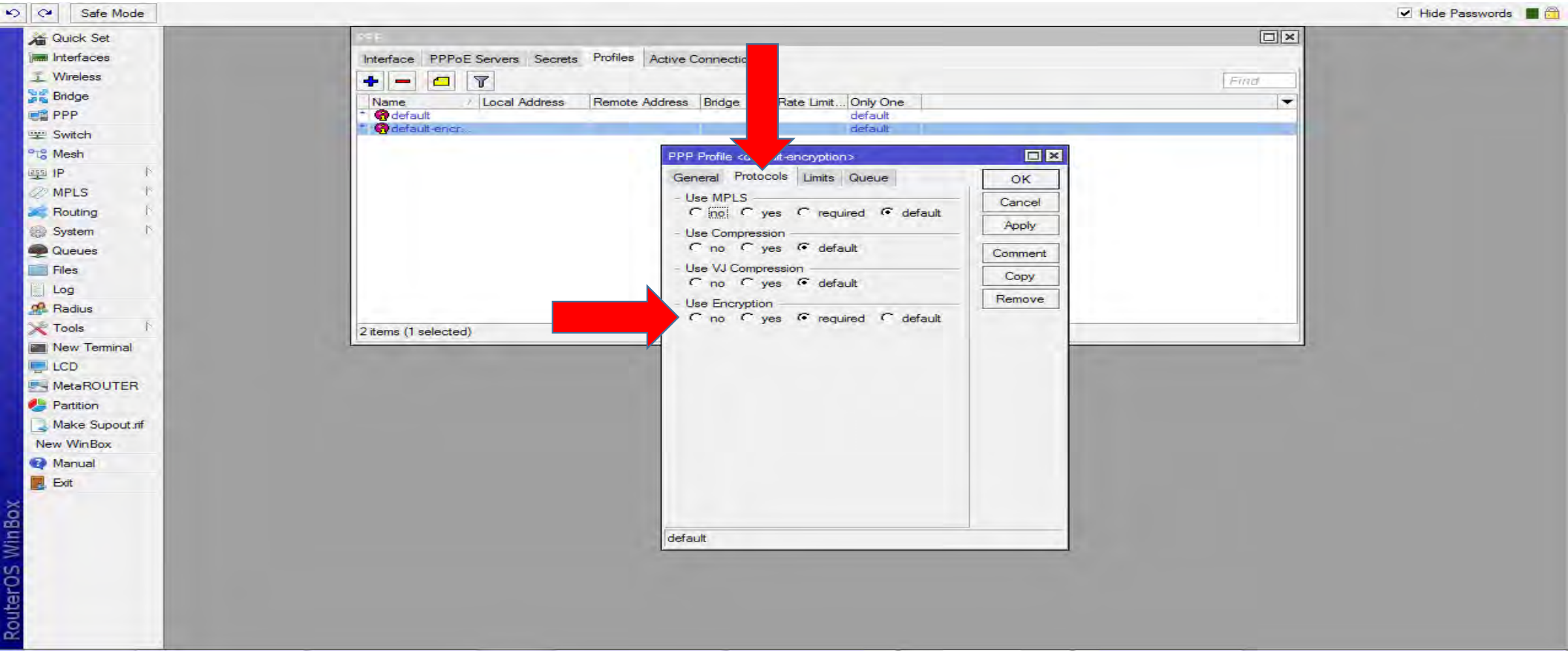
PPTP Mikrotik Client to Cisco Server



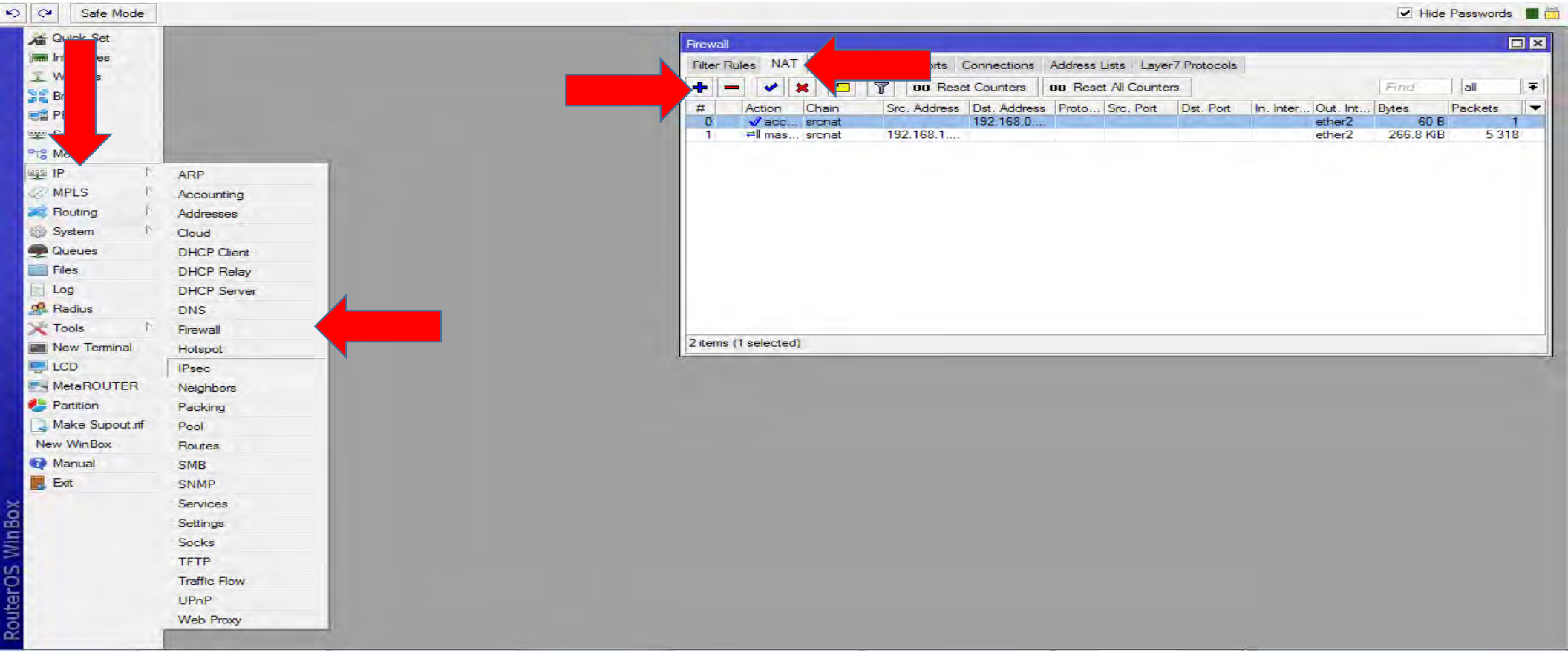
PPTP Mikrotik Client to Cisco Server



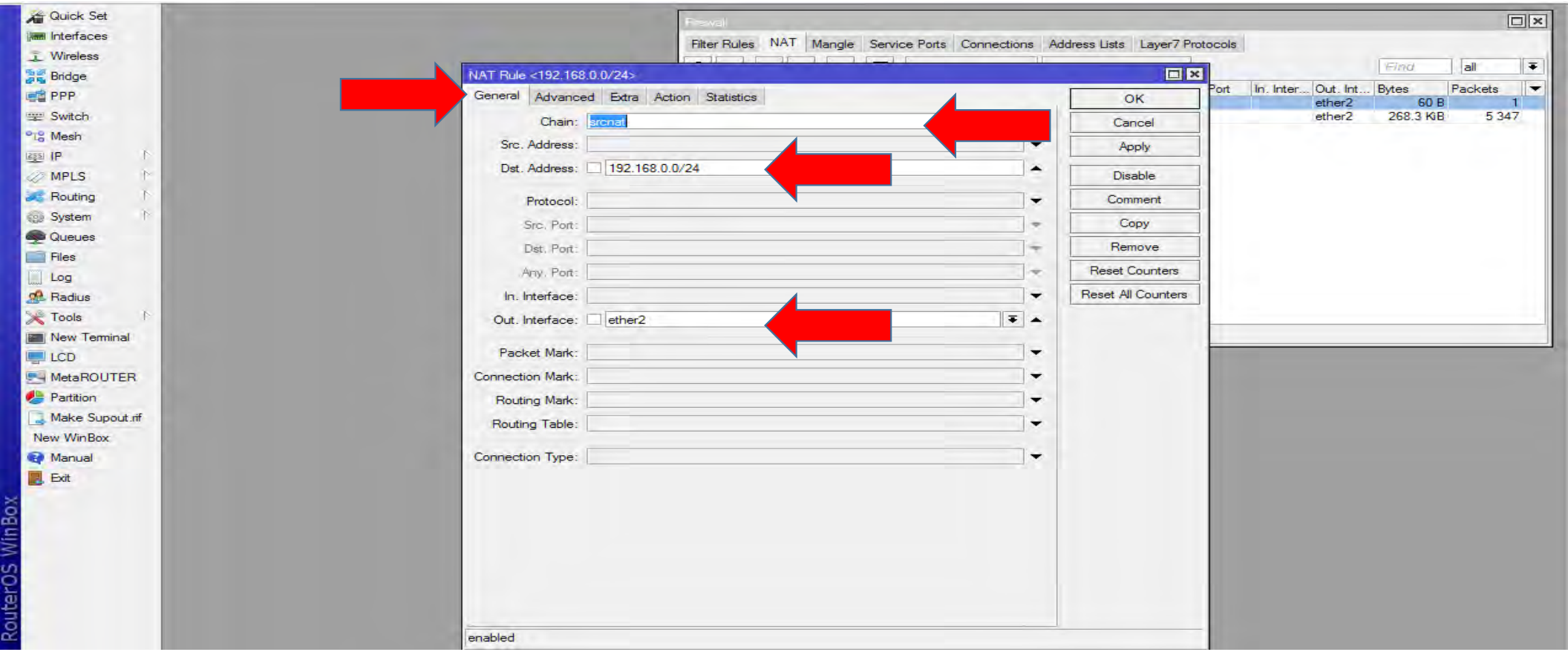
PPTP Mikrotik Client to Cisco Server



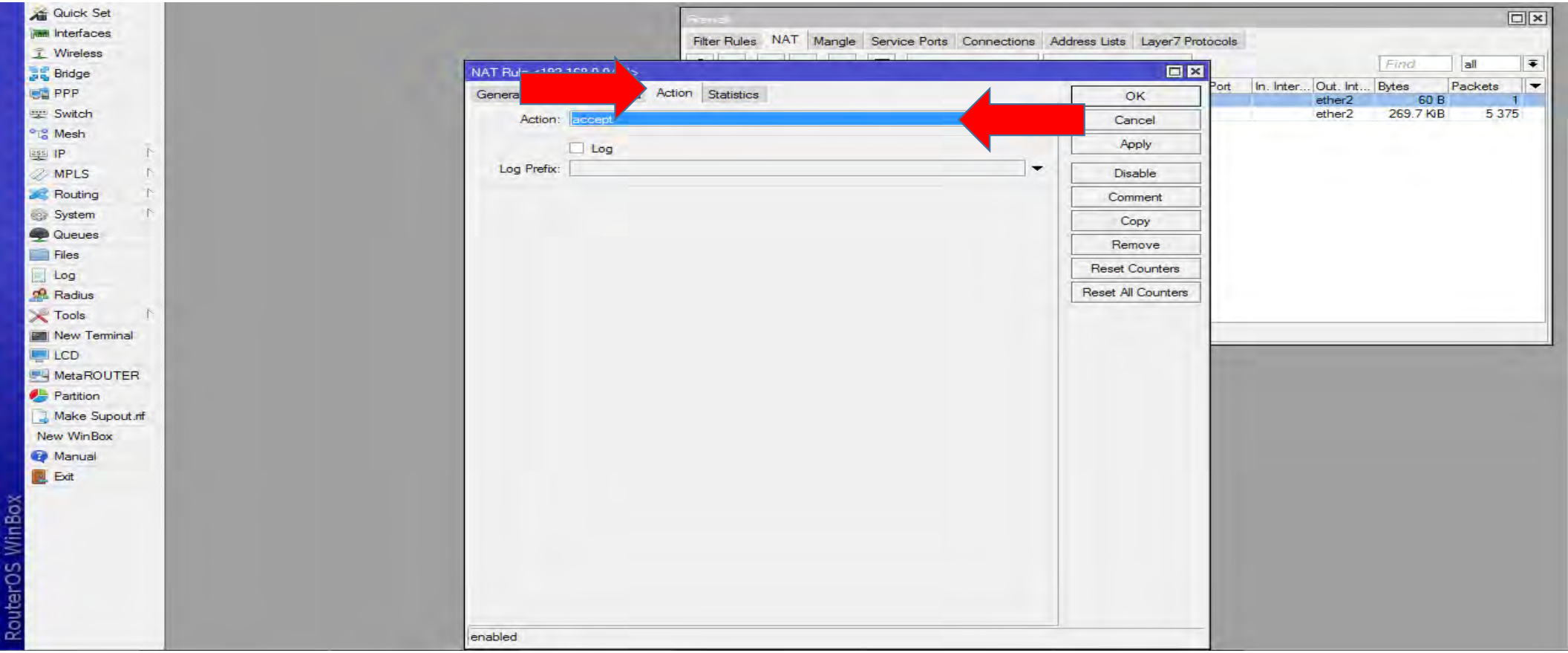
PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server

- aaa new-model
- aaa authentication ppp default local
- vpdn enable
- vpdn-group 1
- accept-dialin
- protocol pptp
- virtual-template 1
- l2tp tunnel timeout no-session 15

- username pptp_branch password 0 1234

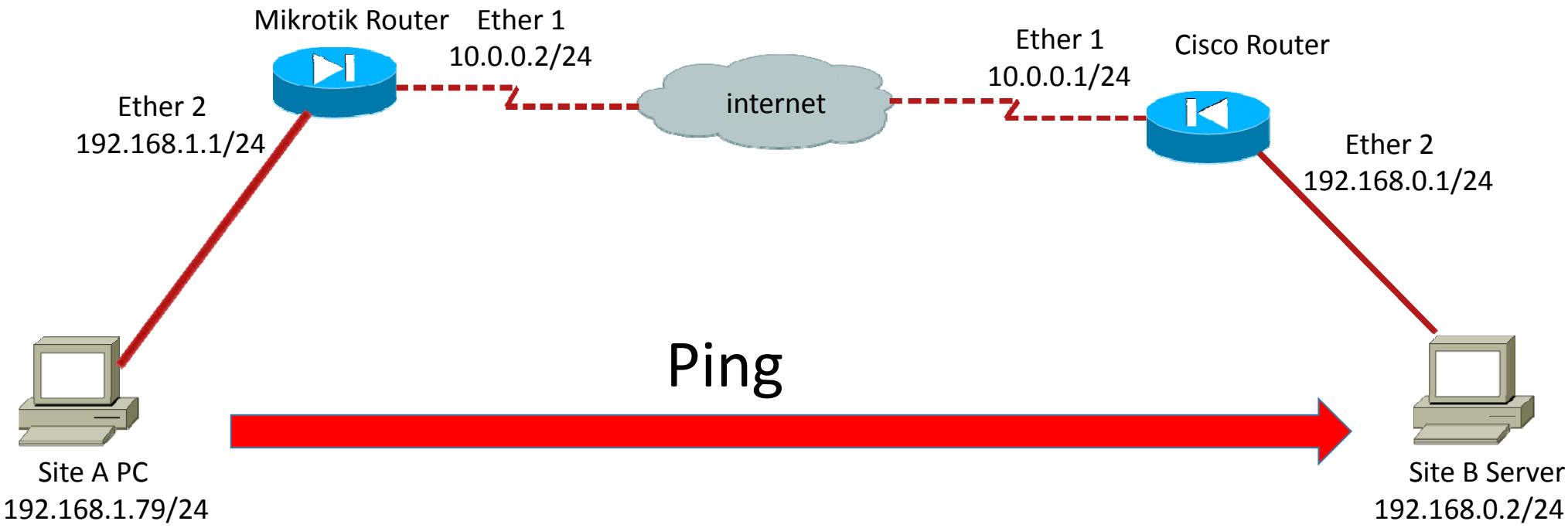
PPTP Mikrotik Client to Cisco Server

- interface Virtual-Template1
- ip address 192.168.79.1 255.255.255.0
- peer default ip address pool PPTP_POOL
- no keepalive
- ppp encrypt mppe 128 required
- ppp authentication ms-chap-v2
- ip local pool PPTP_POOL 192.168.79.2
-

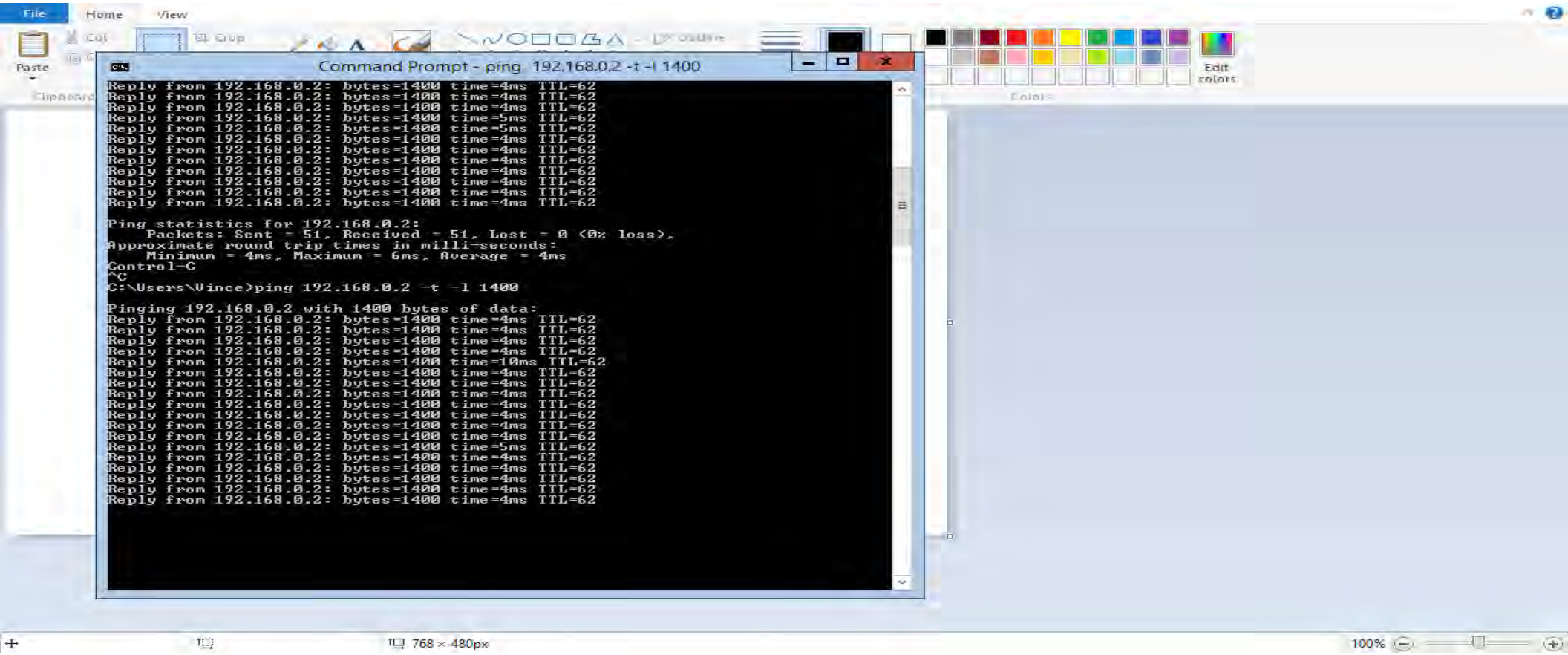
PPTP Mikrotik Client to Cisco Server

- ip nat inside source list nonat interface FastEthernet0/0 overload
- ip route 192.168.1.0 255.255.255.0 192.168.79.2
- ip access-list extended nonat
- deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255
- permit ip 192.168.1.0 0.0.0.255 any

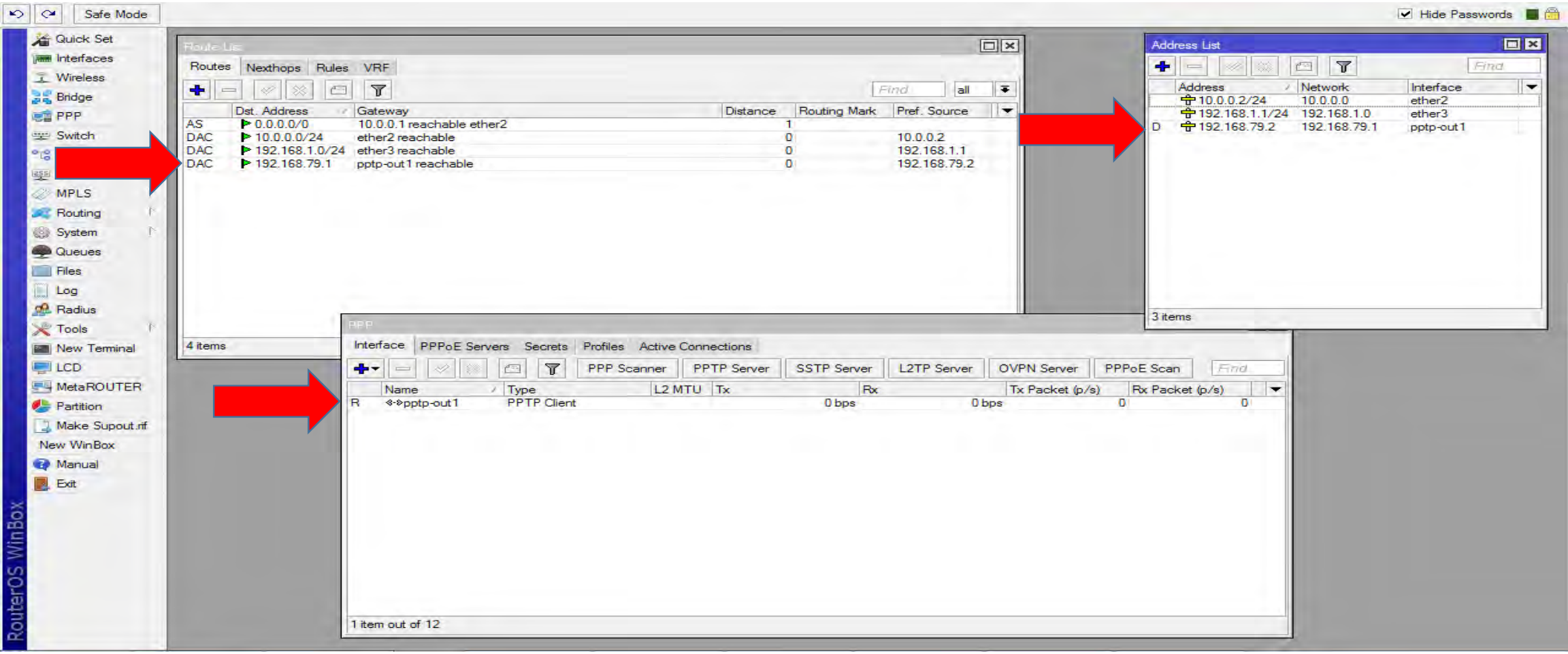
PPTP Mikrotik Client to Cisco Server



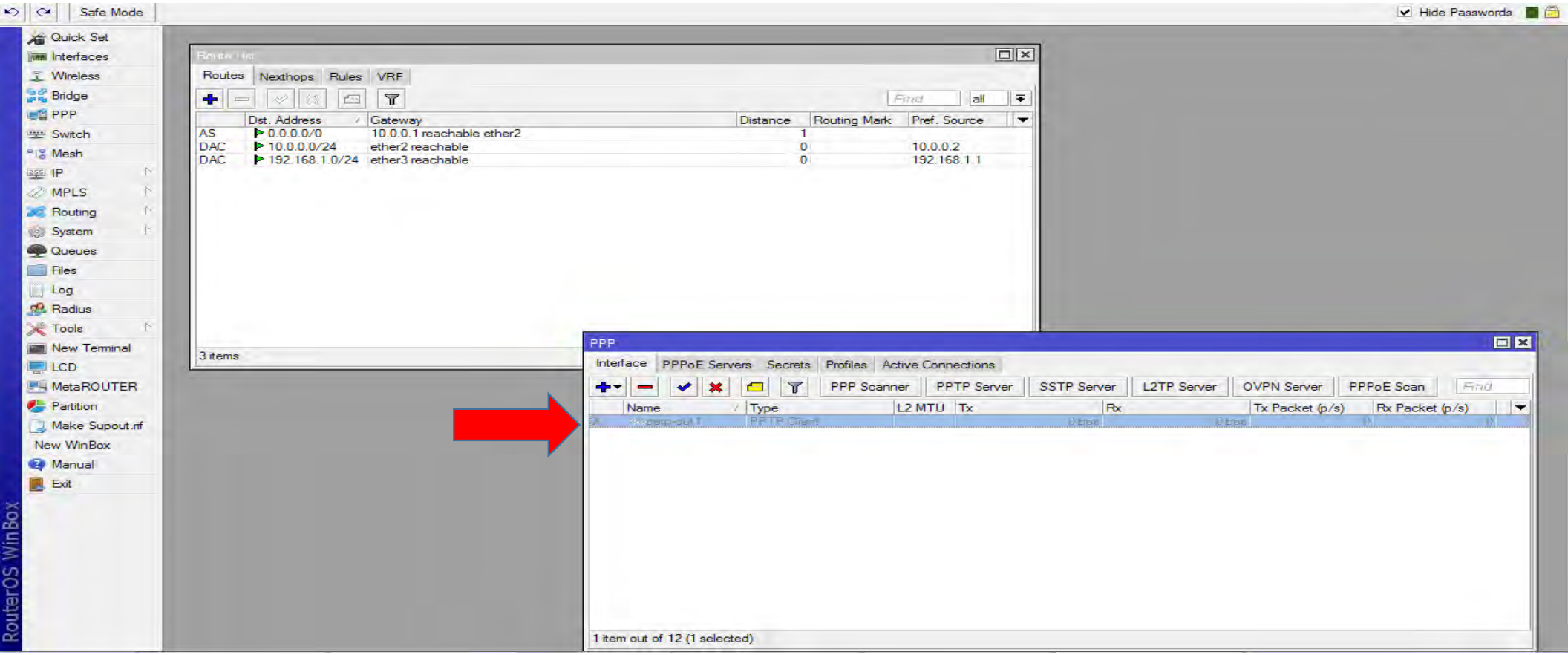
PPTP Mikrotik Client to Cisco Server



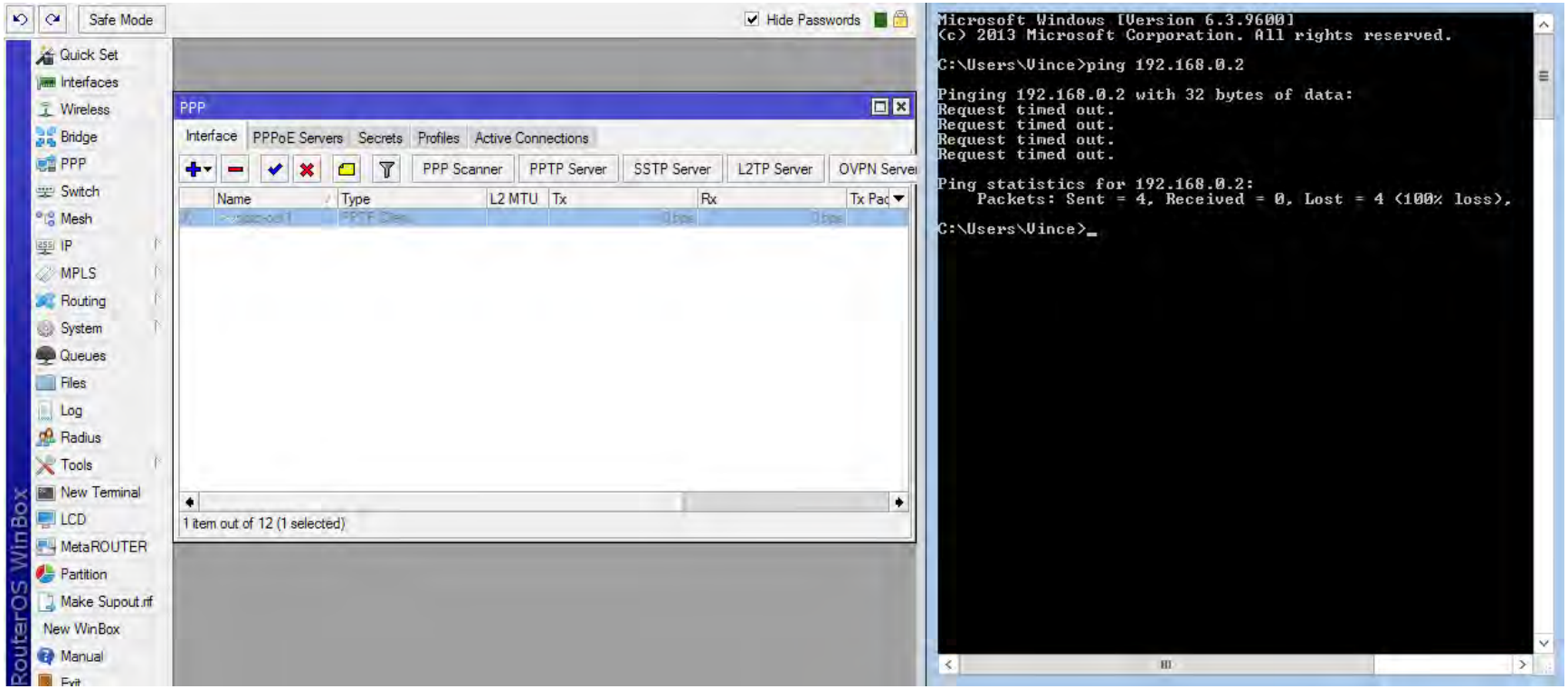
PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server

- /interface pptp-client
- add allow=mschap2 connect-to=10.0.0.1 disabled=no mrru=1600 name=pptp-out1 \
- password=1234 user=pptp_branch

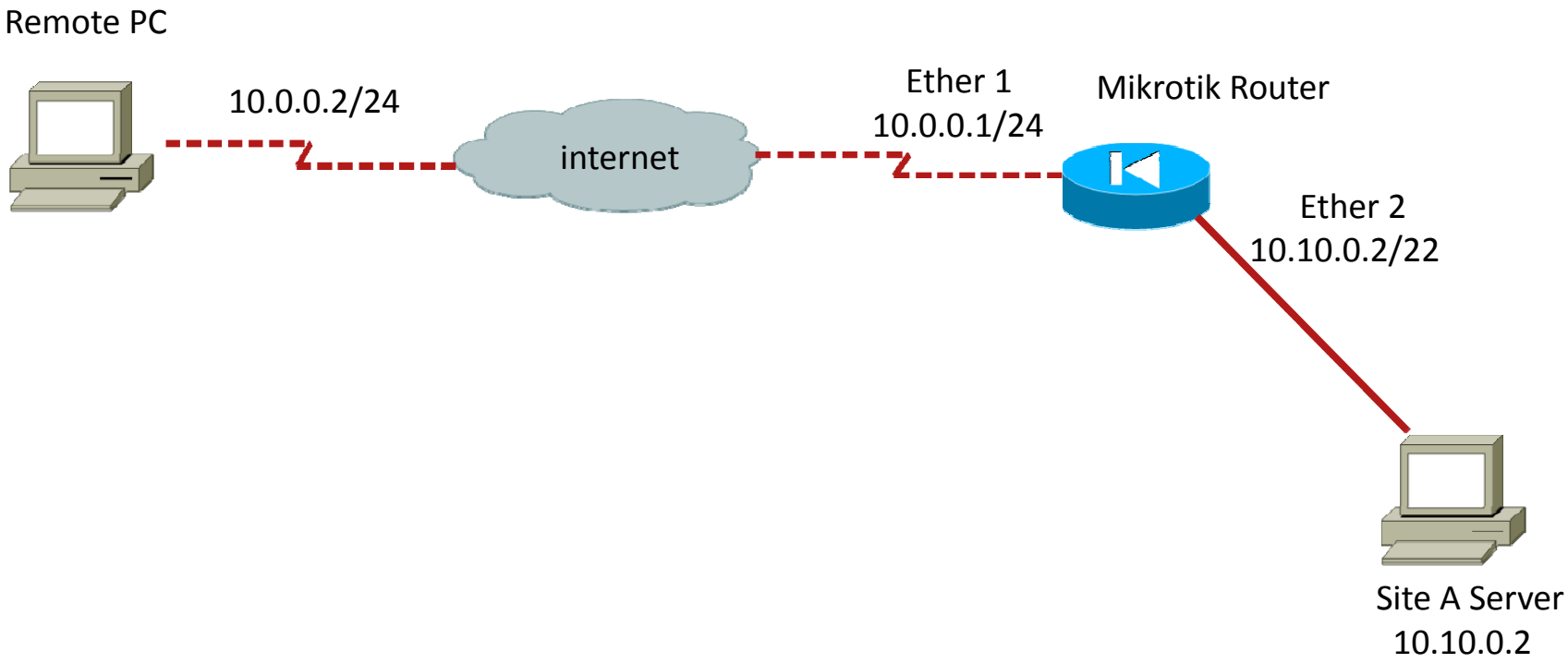
- /ppp profile
- set 1 use-encryption=required

- /ip firewall nat
- add chain=srcnat dst-address=192.168.0.0/24 out-interface=ether2

IPSEC Shrew Client To Mikrotik

- Configure a Shrew client on remote PC to connect to a Mikrotik router
- and access internal lan network
- Eliminates need for Microsoft VPN client
- Enables one client to be used for remote access to Mikrotik and Cisco devices eliminating need for a Cisco VPN Client
- Easy to import existing Cisco VPN profiles into Shrew client
- Allows for ease of migration from Cisco devices to Mikrotik routers

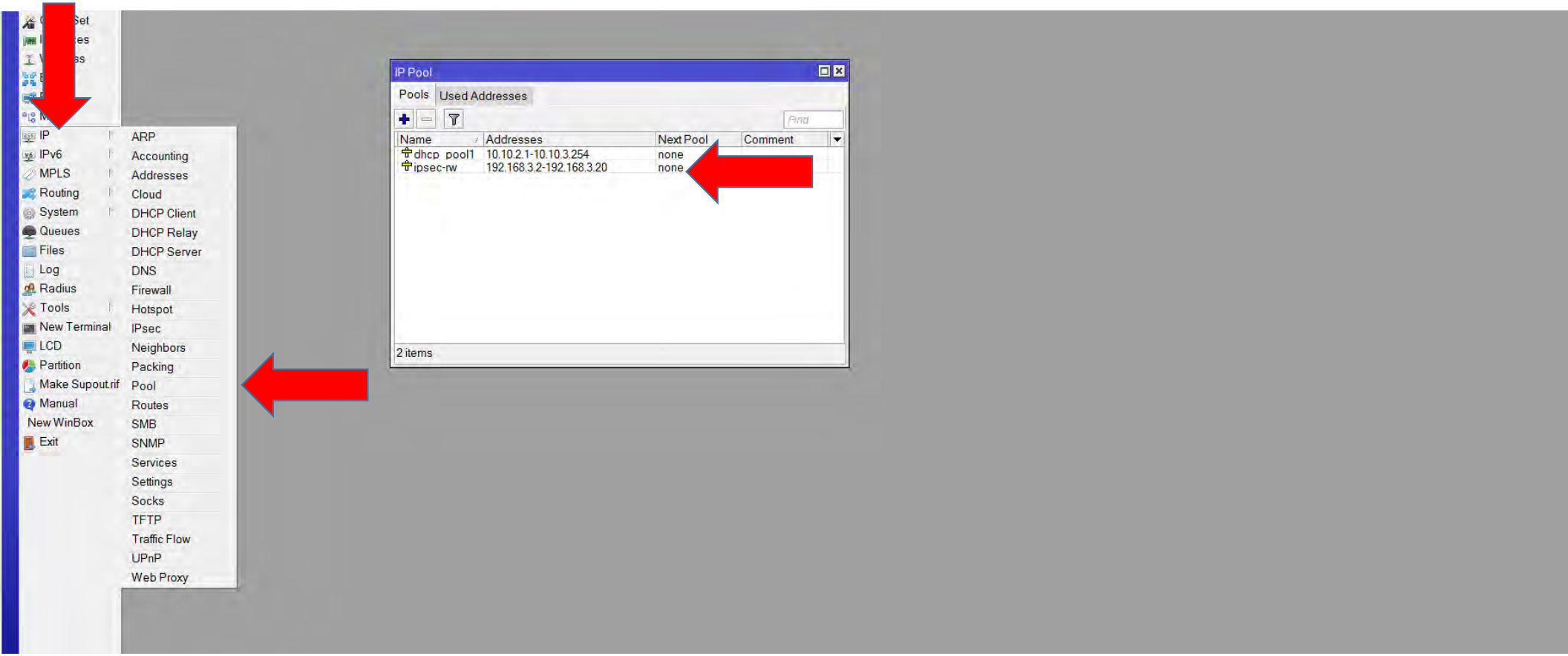
IPSEC Shrew Client To Mikrotik



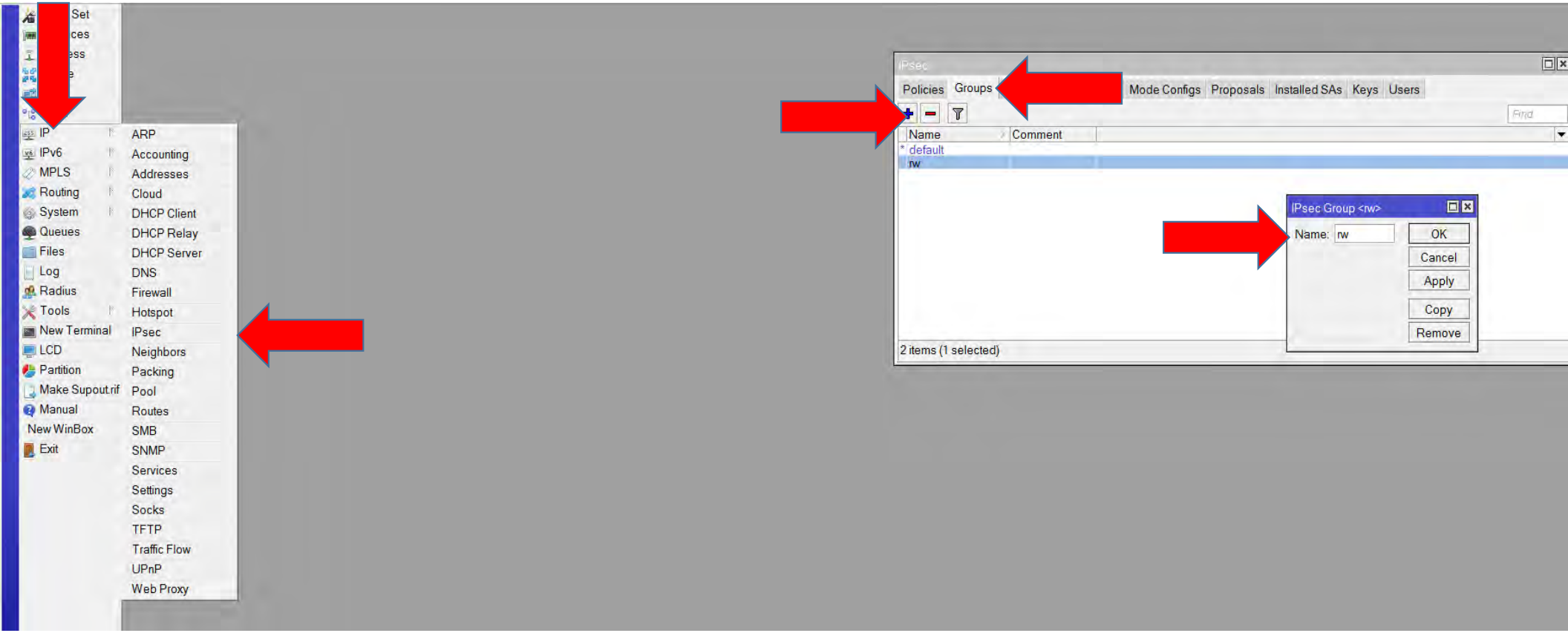
IPSEC Shrew Client To Mikrotik

- www.shrew.net/download/vpn

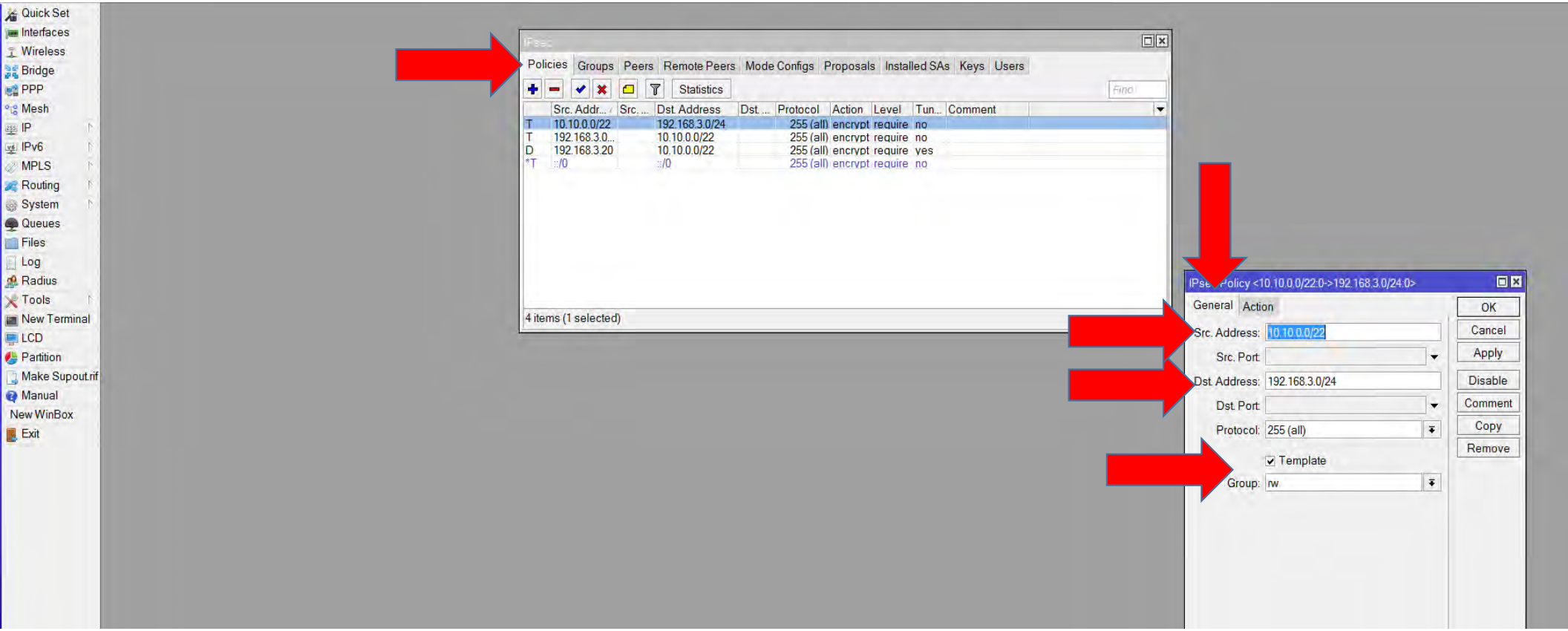
IPSEC Shrew Client To Mikrotik



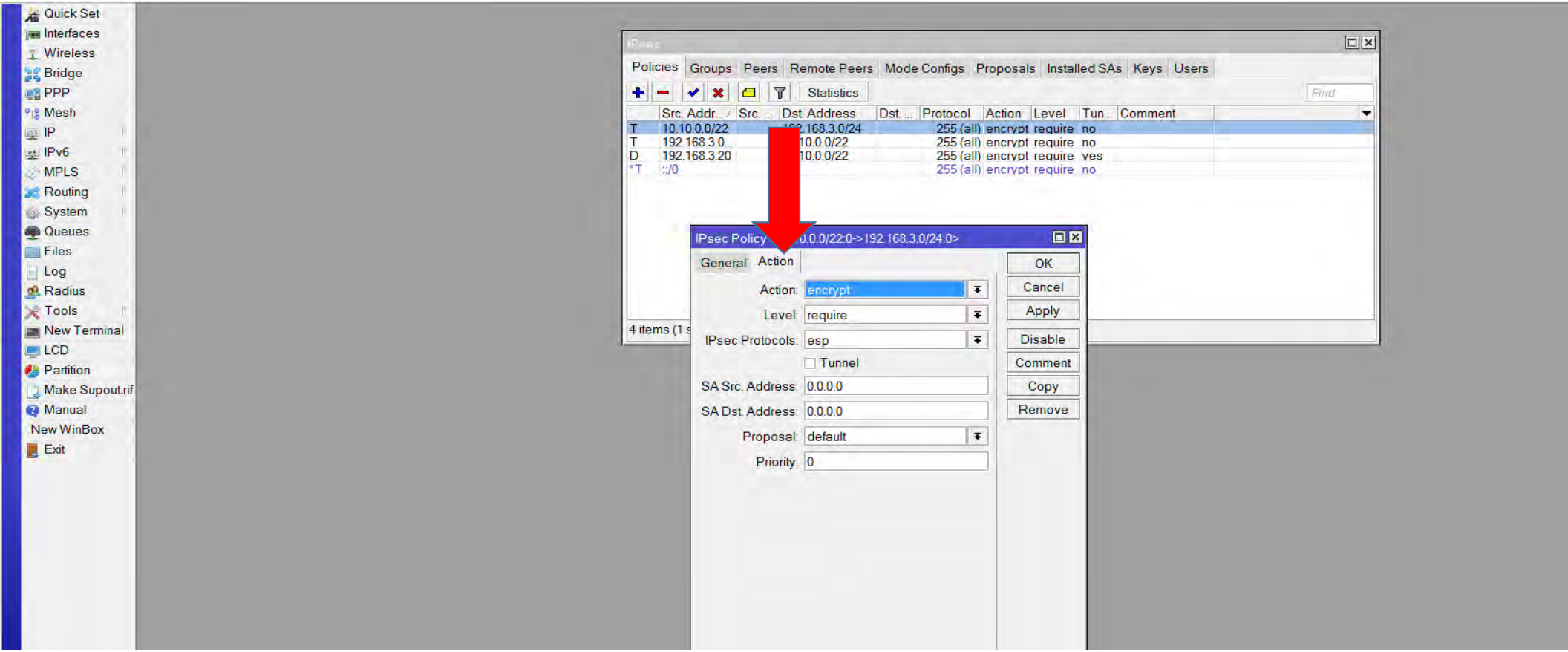
IPSEC Shrew Client To Mikrotik



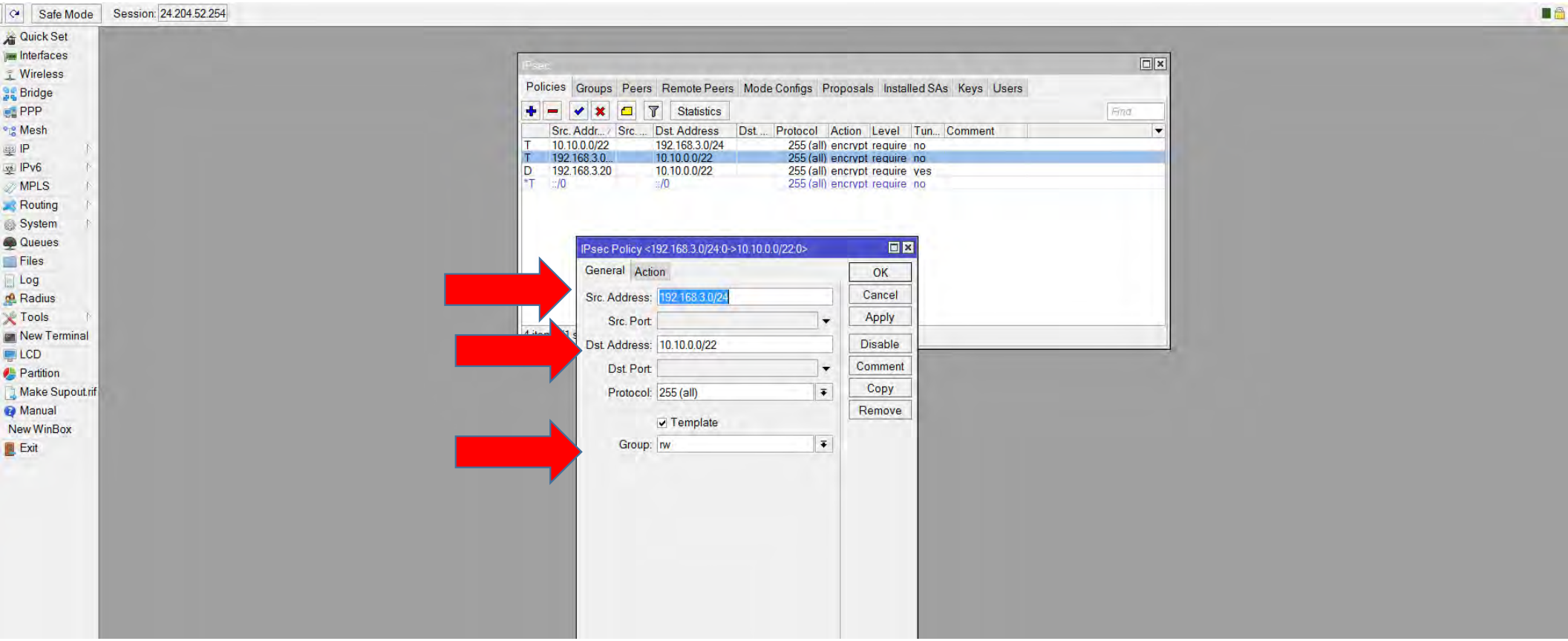
IPSEC Shrew Client To Mikrotik



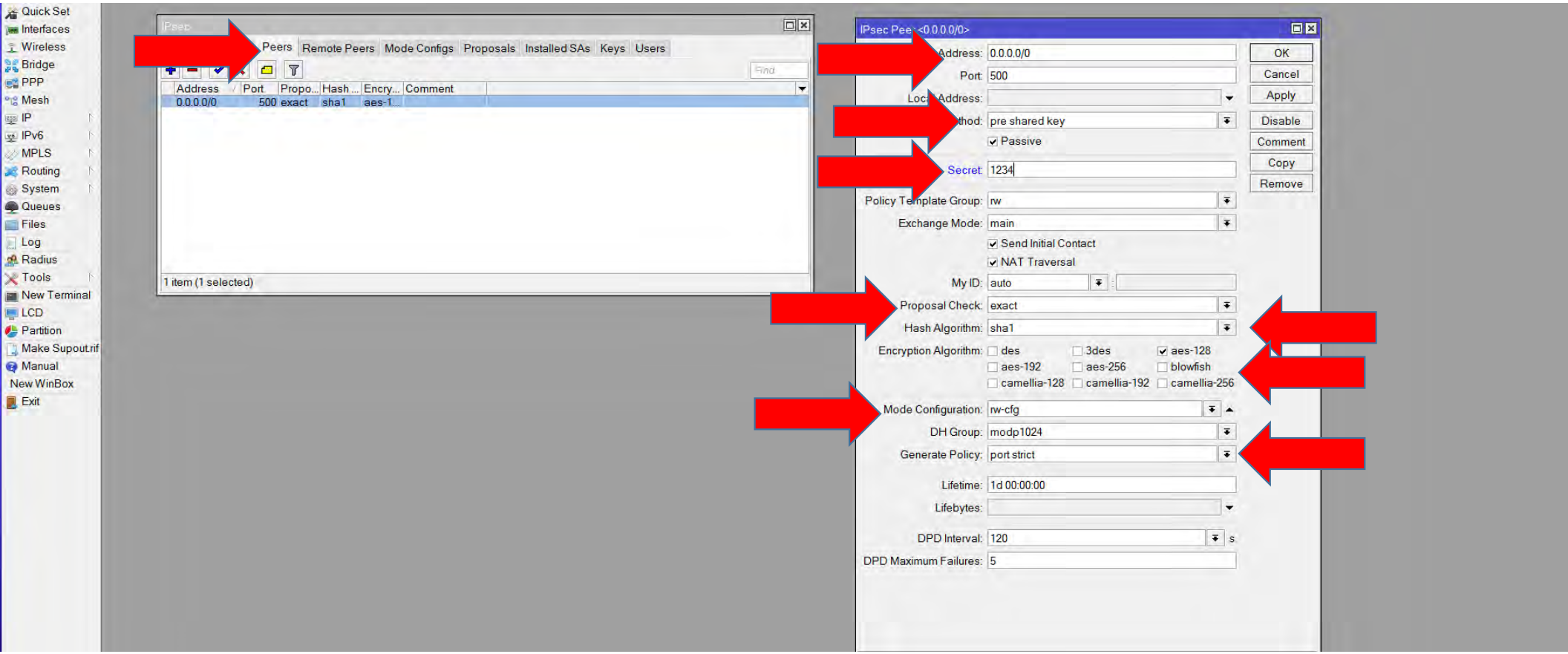
IPSEC Shrew Client To Mikrotik



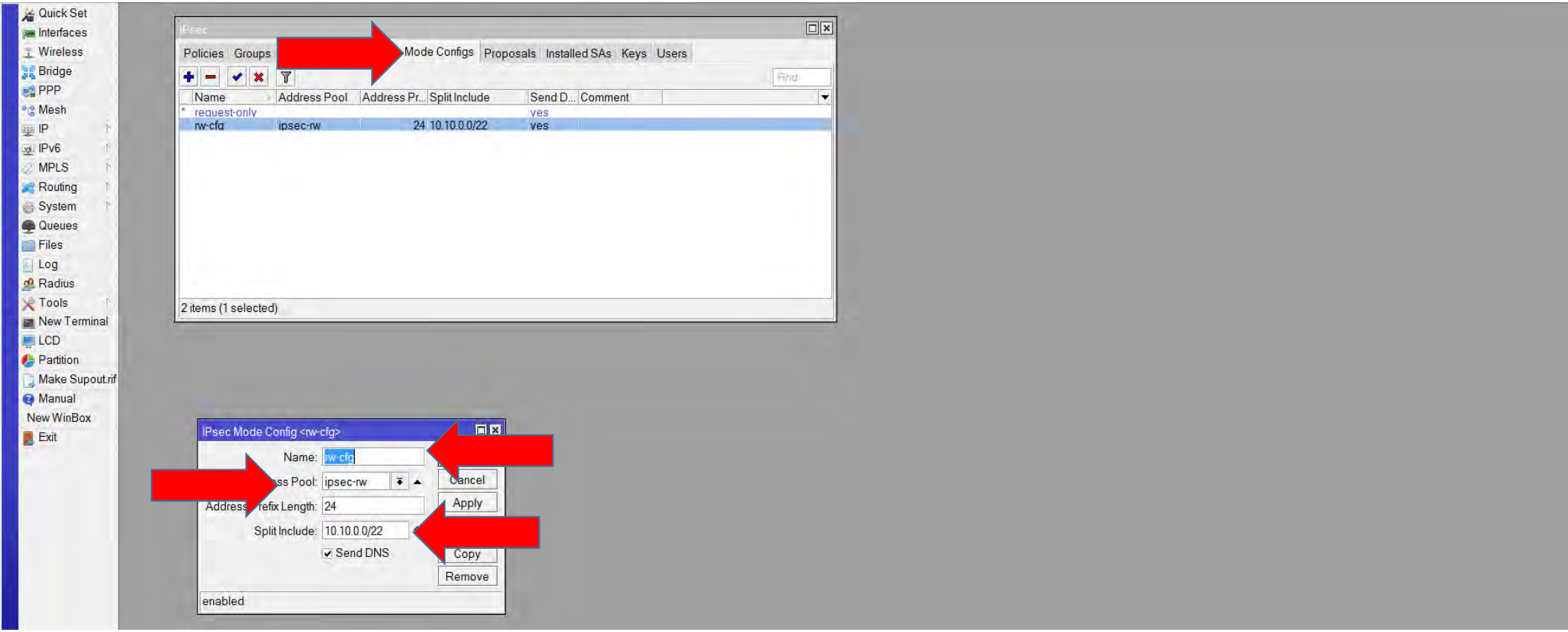
IPSEC Shrew Client To Mikrotik



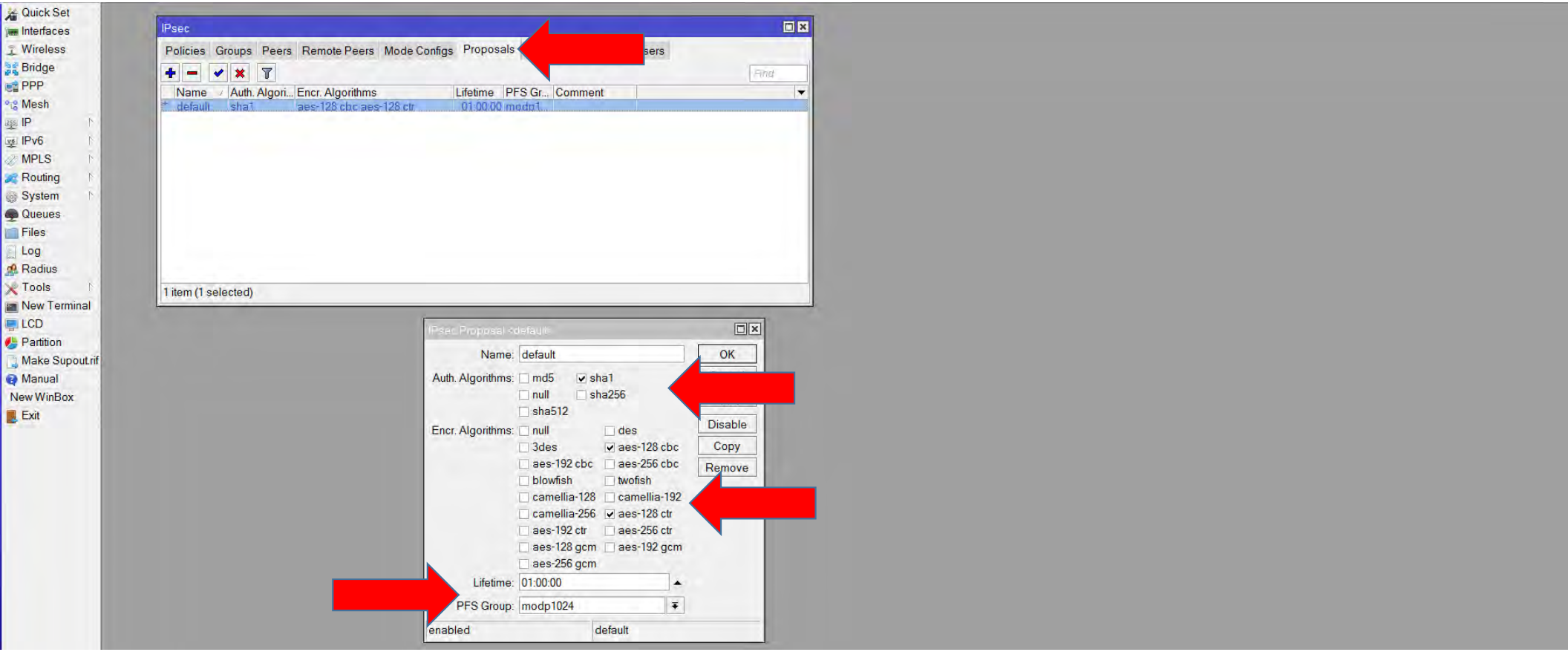
IPSEC Shrew Client To Mikrotik



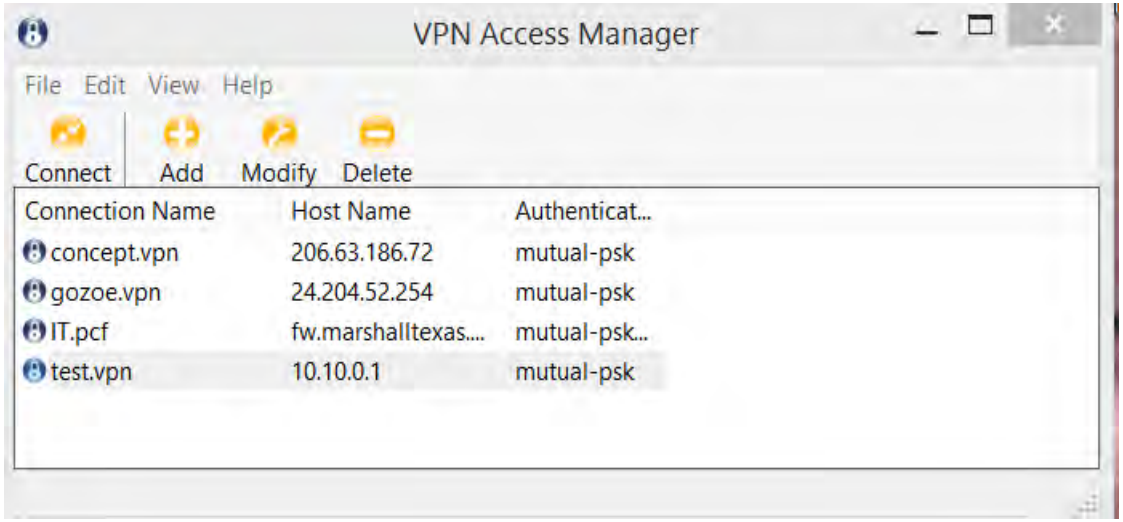
IPSEC Shrew Client To Mikrotik



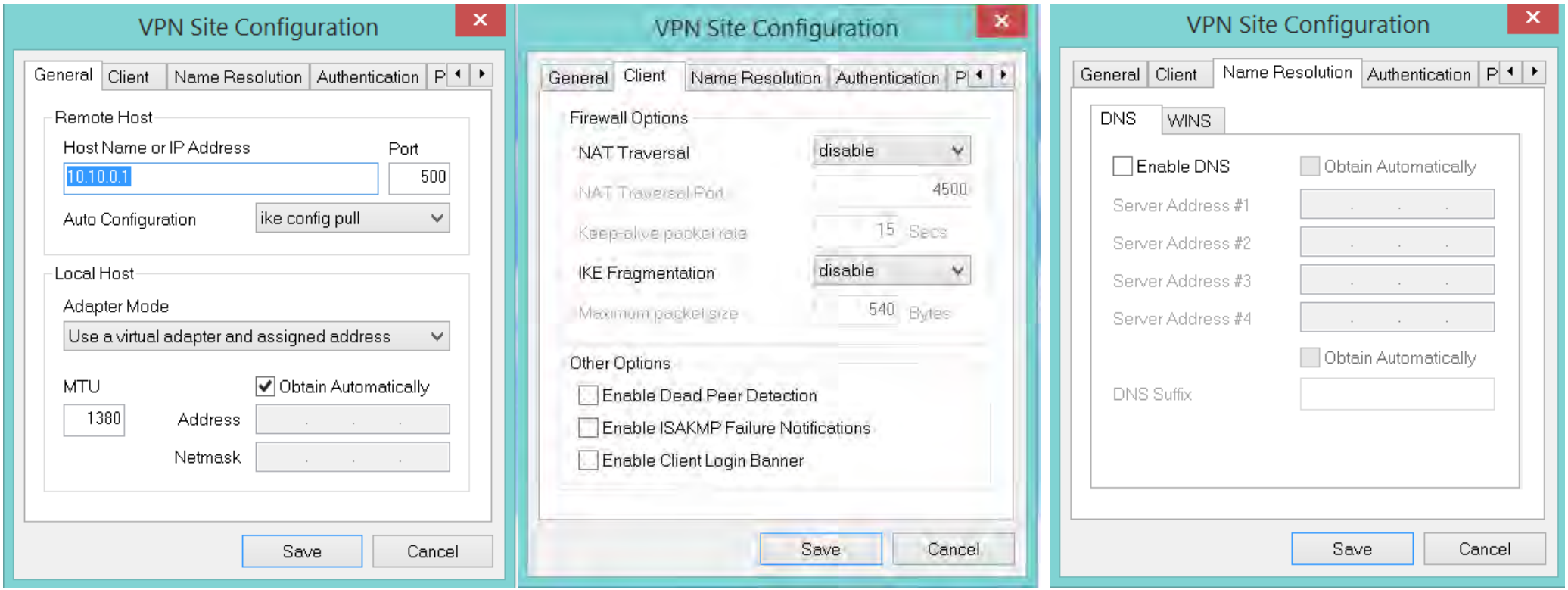
IPSEC Shrew Client To Mikrotik



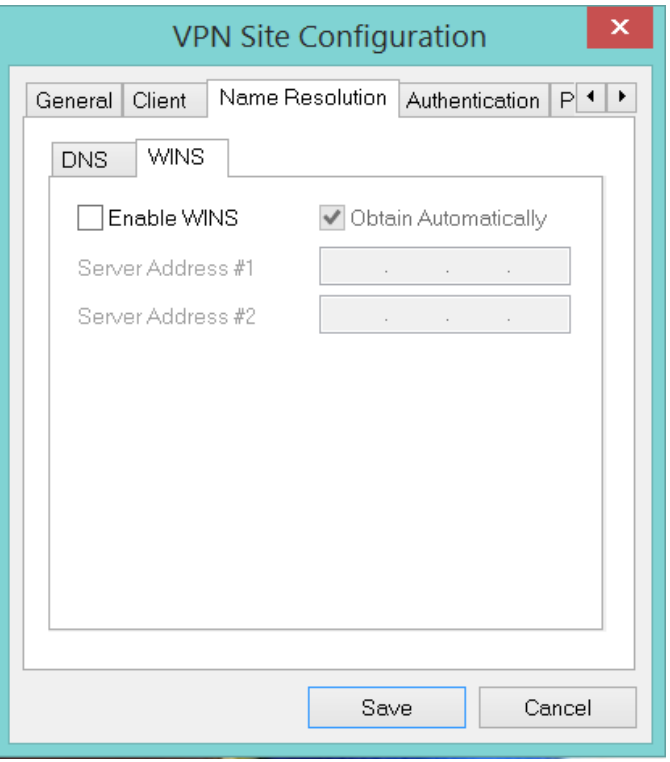
IPSEC Shrew Client To Mikrotik

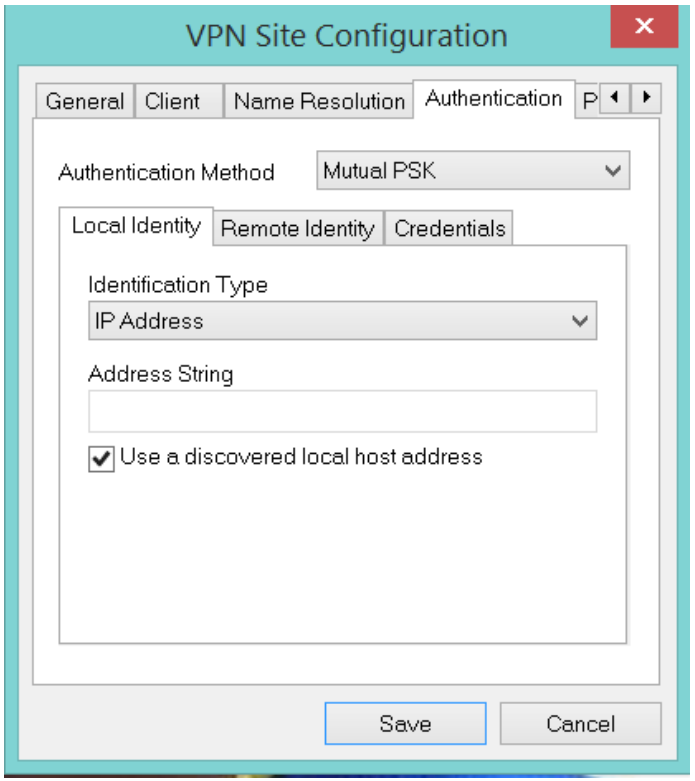


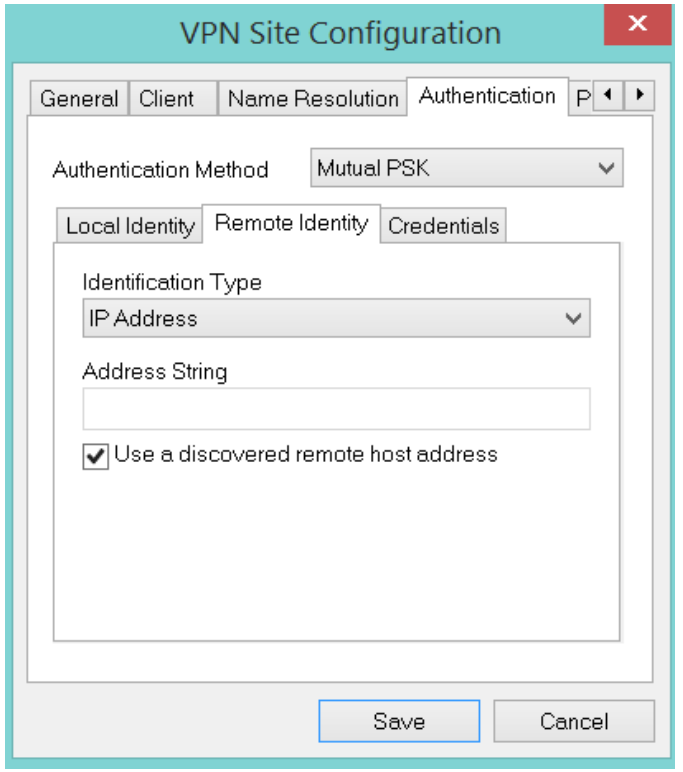
IPSEC Shrew Client To Mikrotik



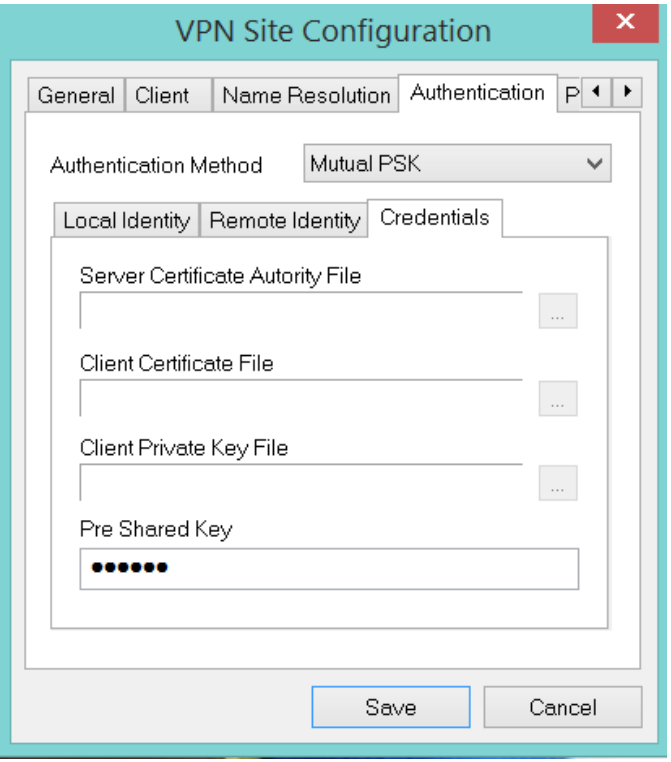
IPSEC Shrew Client To Mikrotik

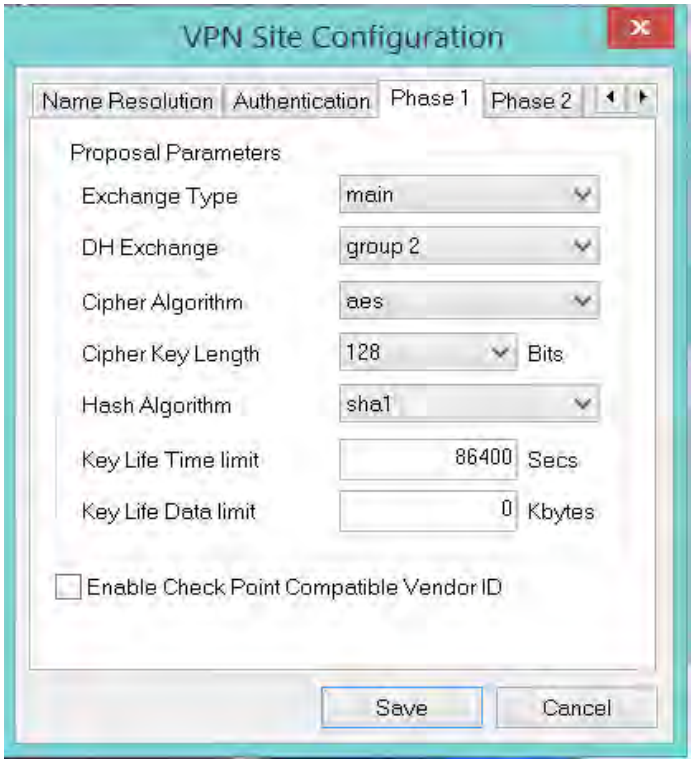


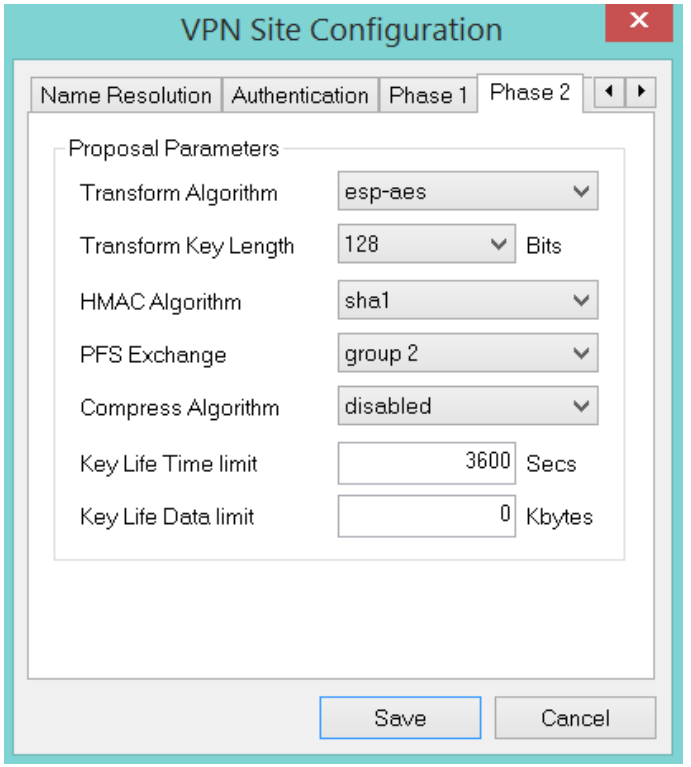




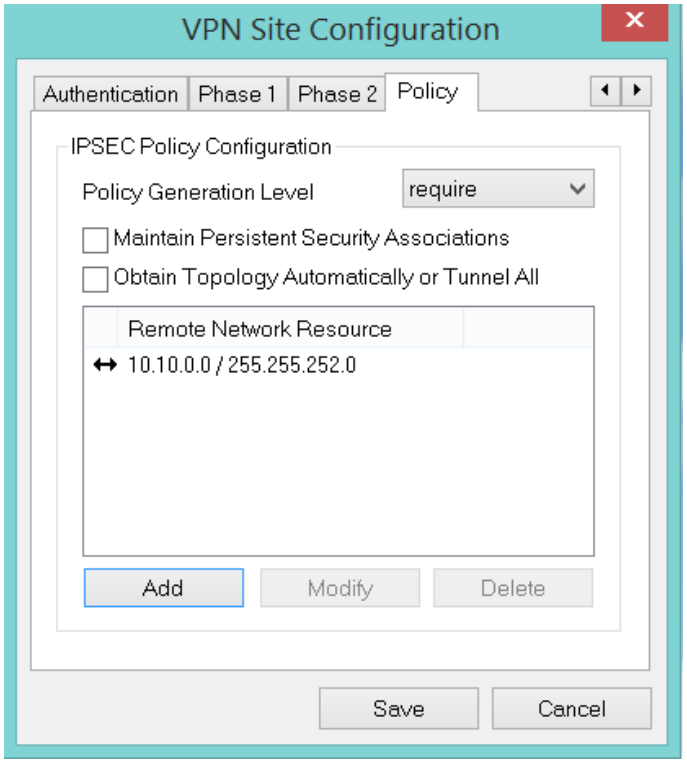
IPSEC Shrew Client To Mikrotik

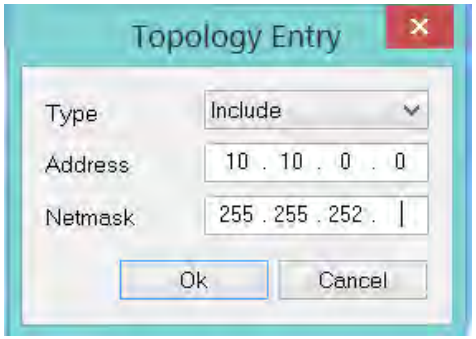




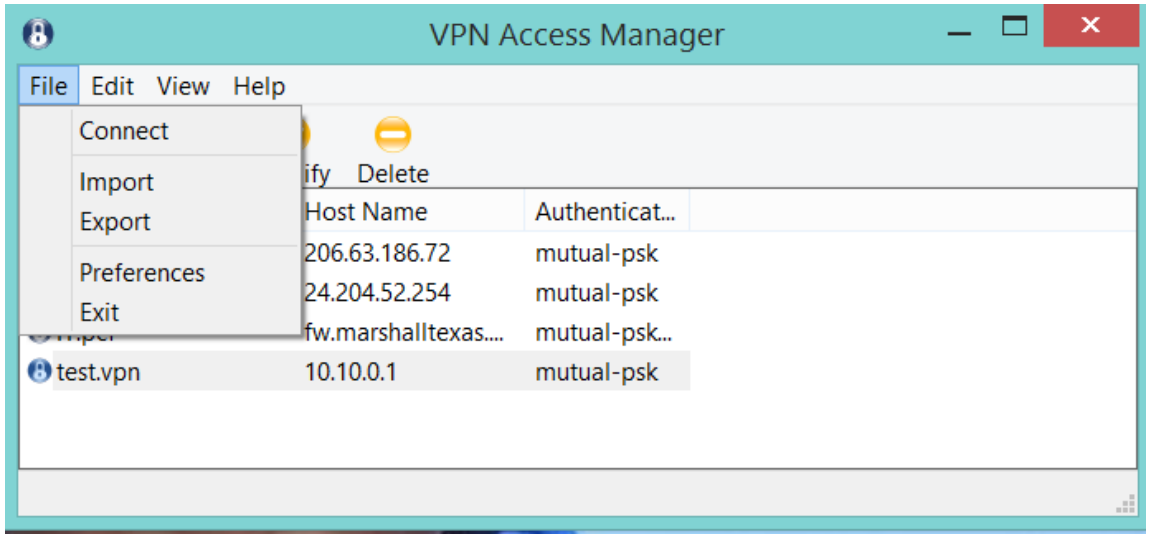


IPSEC Shrew Client To Mikrotik





IPSEC Shrew Client To Mikrotik



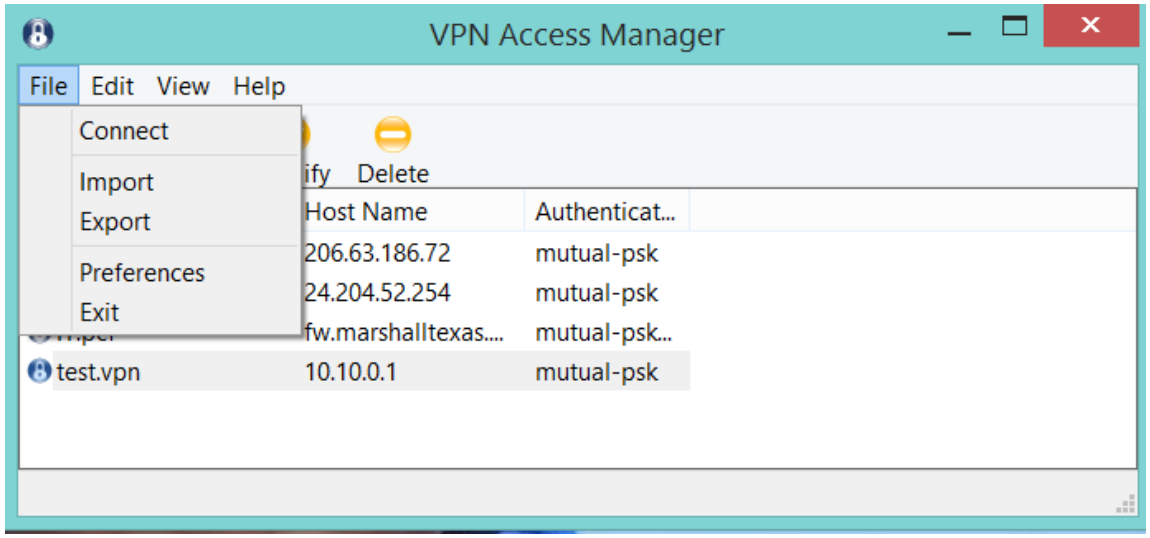
IPSEC Shrew Client To Mikrotik

n:version:4
n:network-ike-port:500
n:network-mtu-size:1380
n:client-addr-auto:1
n:network-natt-port:4500
n:network-natt-rate:15
n:network-frag-size:540
n:network-dpd-enable:0
n:client-banner-enable:0
n:network-notify-enable:0
n:client-dns-used:0
n:client-dns-auto:0
n:client-dns-suffix-auto:0
n:client-splitdns-used:0
n:client-splitdns-auto:0n:client-wins-used:0
n:client-wins-auto:1n:phase1-dhgroup:2
n:phase1-life-secs:86400

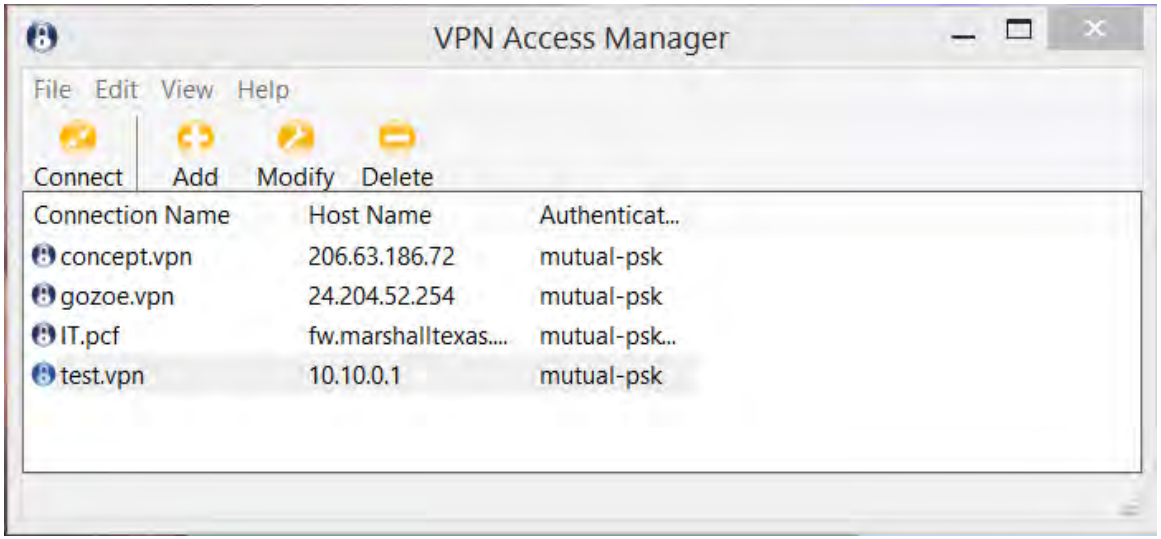
n:phase1-life-kbytes:0
n:vendor-chkpt-enable:0
n:phase2-life-secs:3600
n:phase2-life-kbytes:0
n:policy-nailed:0
n:policy-list-auto:0
n:phase1-keylen:128
n:phase2-keylen:128s:network-host:10.10.0.1
s:client-auto-mode:pull
s:client-iface:virtual
s:network-natt-mode:disable
s:network-frag-mode:disable

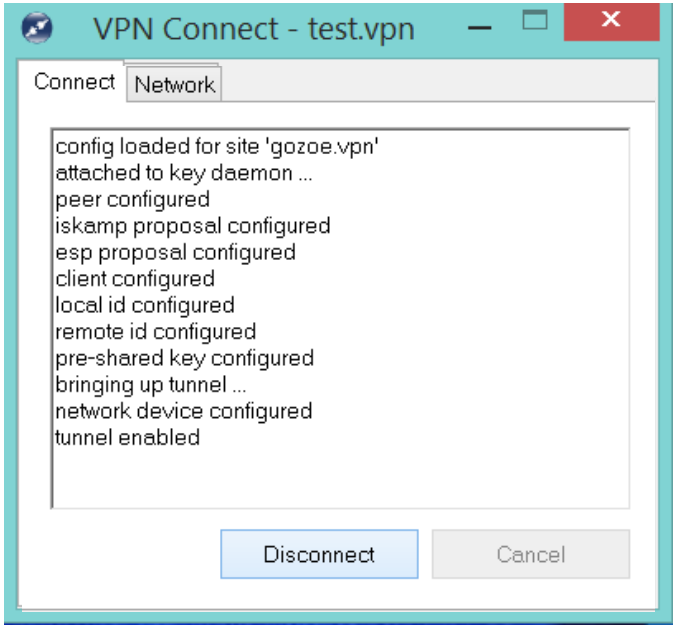
s:auth-method:mutual-psk
s:ident-client-type:address
s:ident-server-type:address
b:auth-mutual-psk:Y3RiNjUx
s:phase1-exchange:main
s:phase1-cipher:aes
s:phase1-hash:sha1
s:phase2-transform:esp-aes
s:phase2-hmac:sha1
s:ipcomp-transform:disabled
n:phase2-pfsgroup:2
s:policy-level:require
s:policy-list-include:10.10.0.0 / 255.255.252.0

IPSEC Shrew Client To Mikrotik

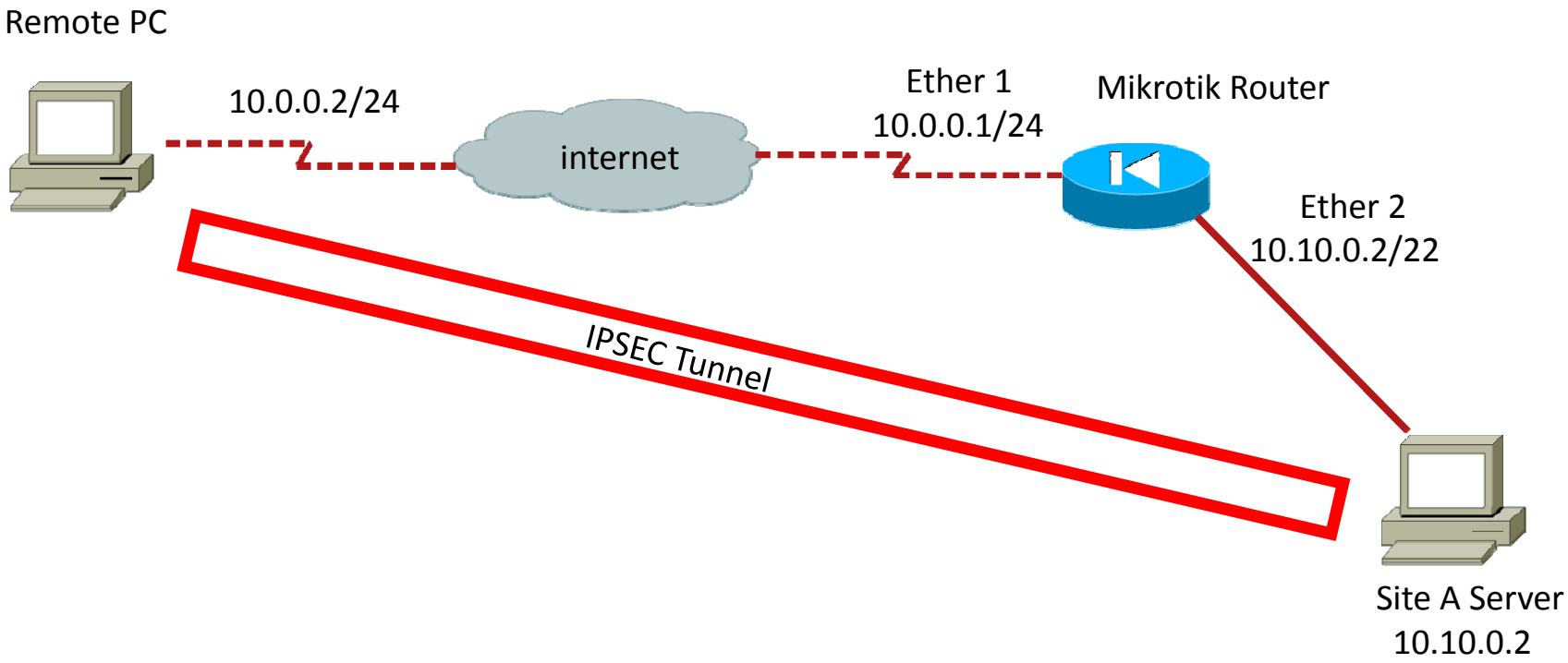


IPSEC Shrew Client To Mikrotik

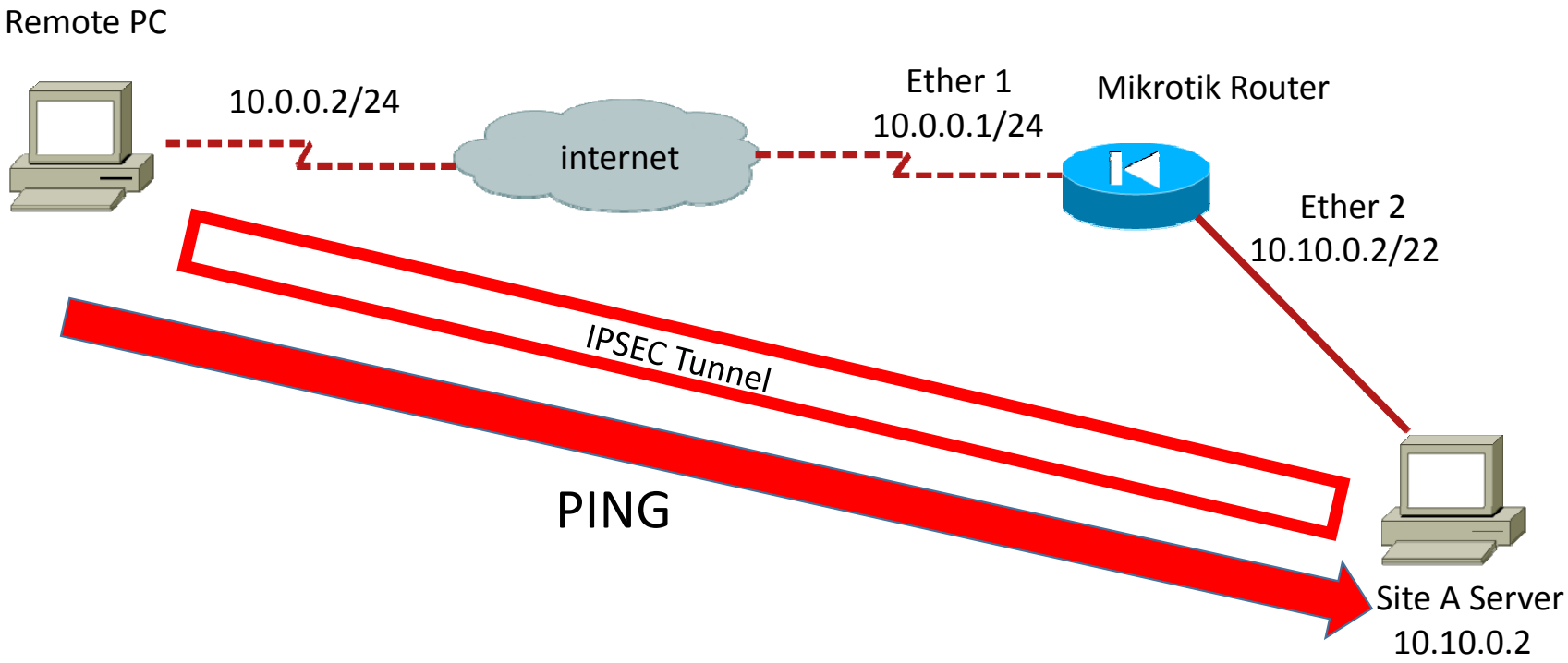




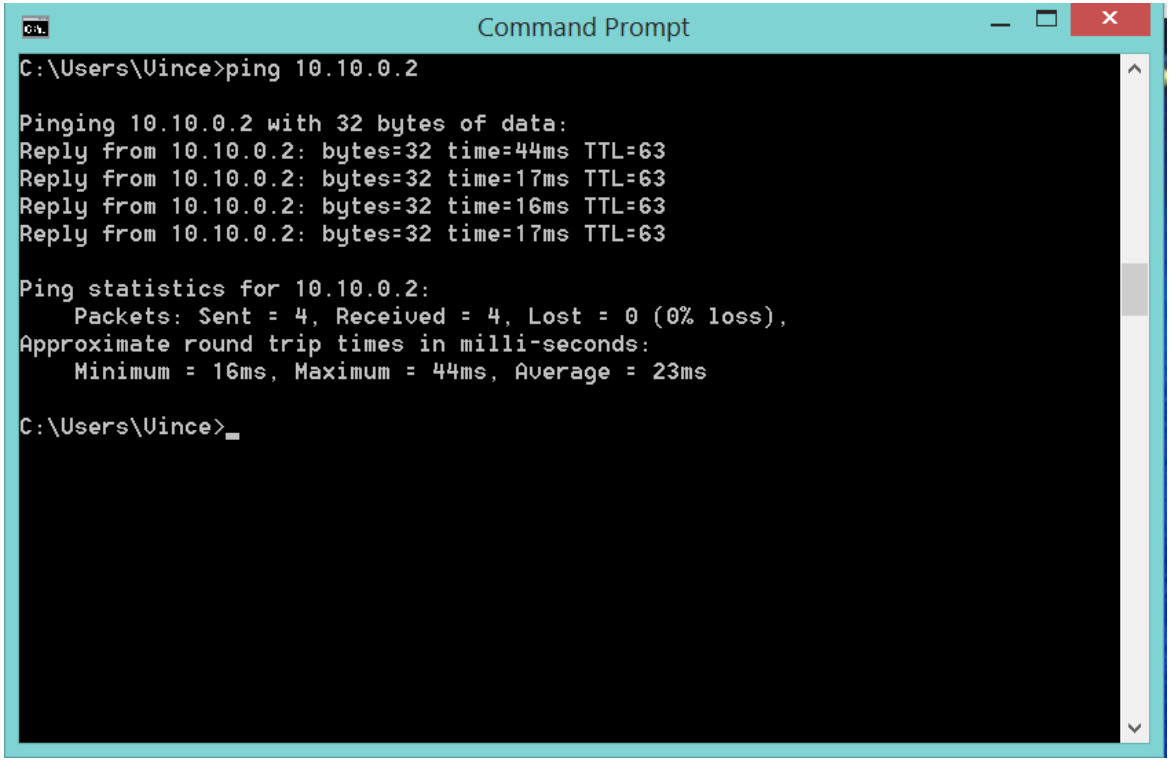
IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik



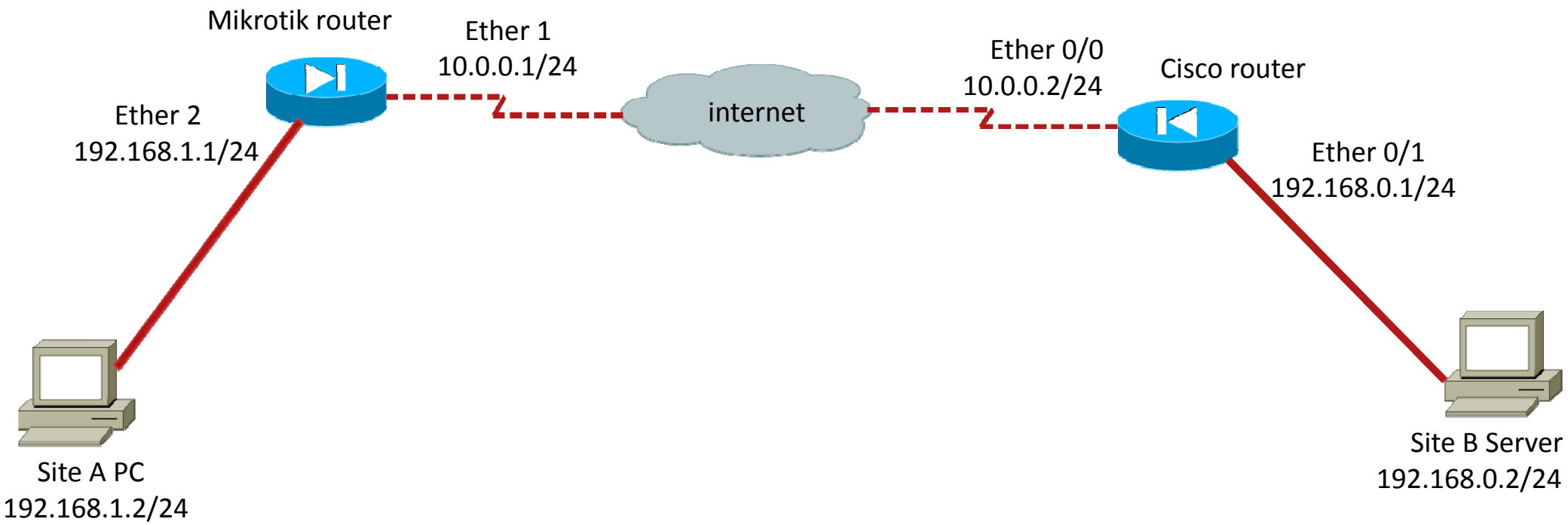
IPSEC Shrew Client To Mikrotik



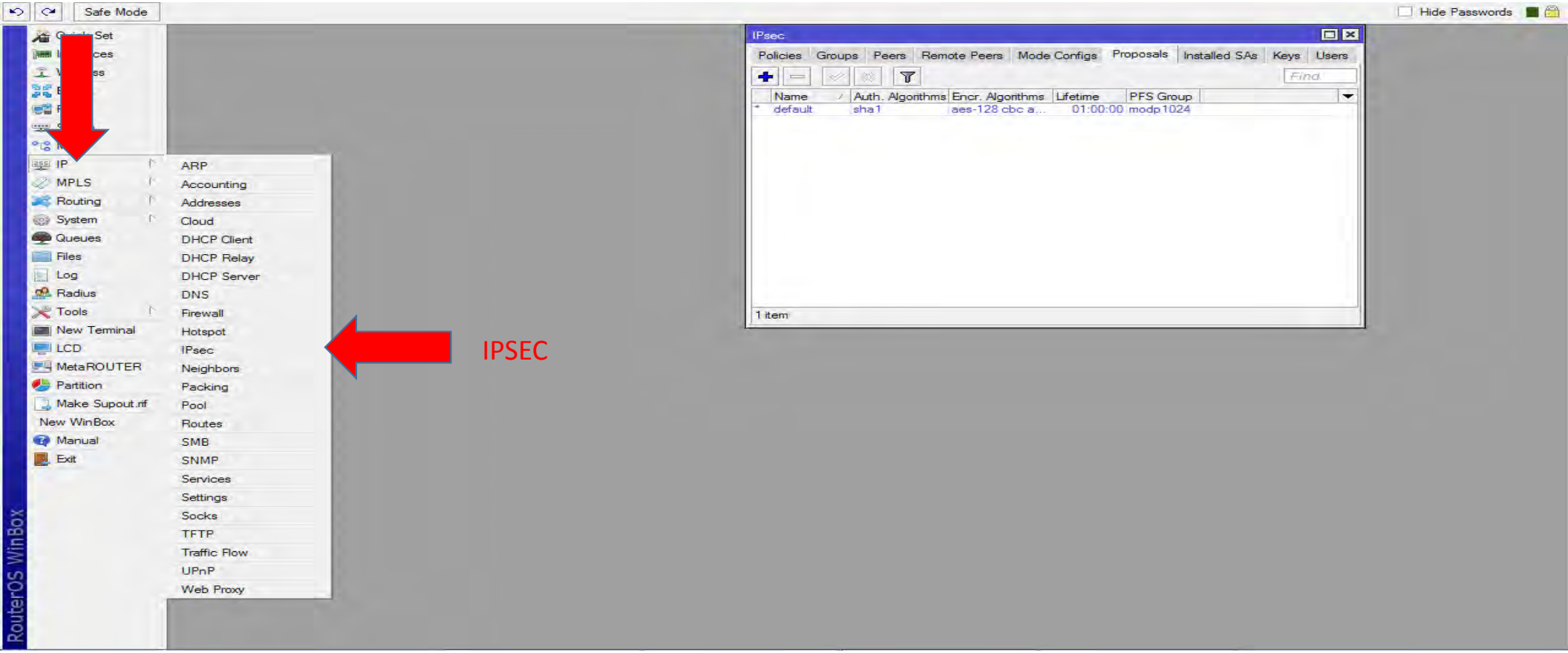
IPSEC Cisco IOS or ASA To Mikrotik

- Configure an IPSEC VPN between a Cisco IOS router or ASA and a Mikrotik router
- Allows replacement of a Cisco branch router or ASA with a MikroTik router without changing or replacing existing Cisco main router

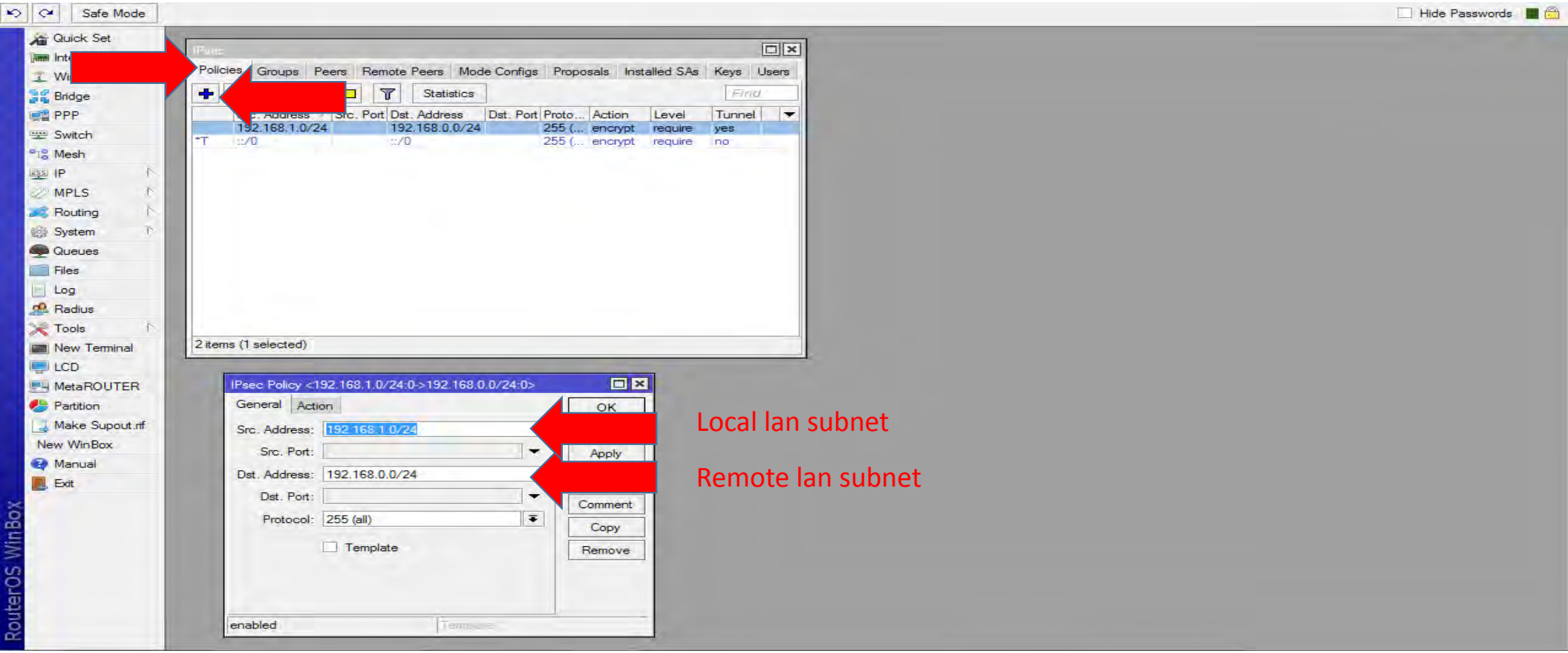
IPSEC Cisco IOS To Mikrotik



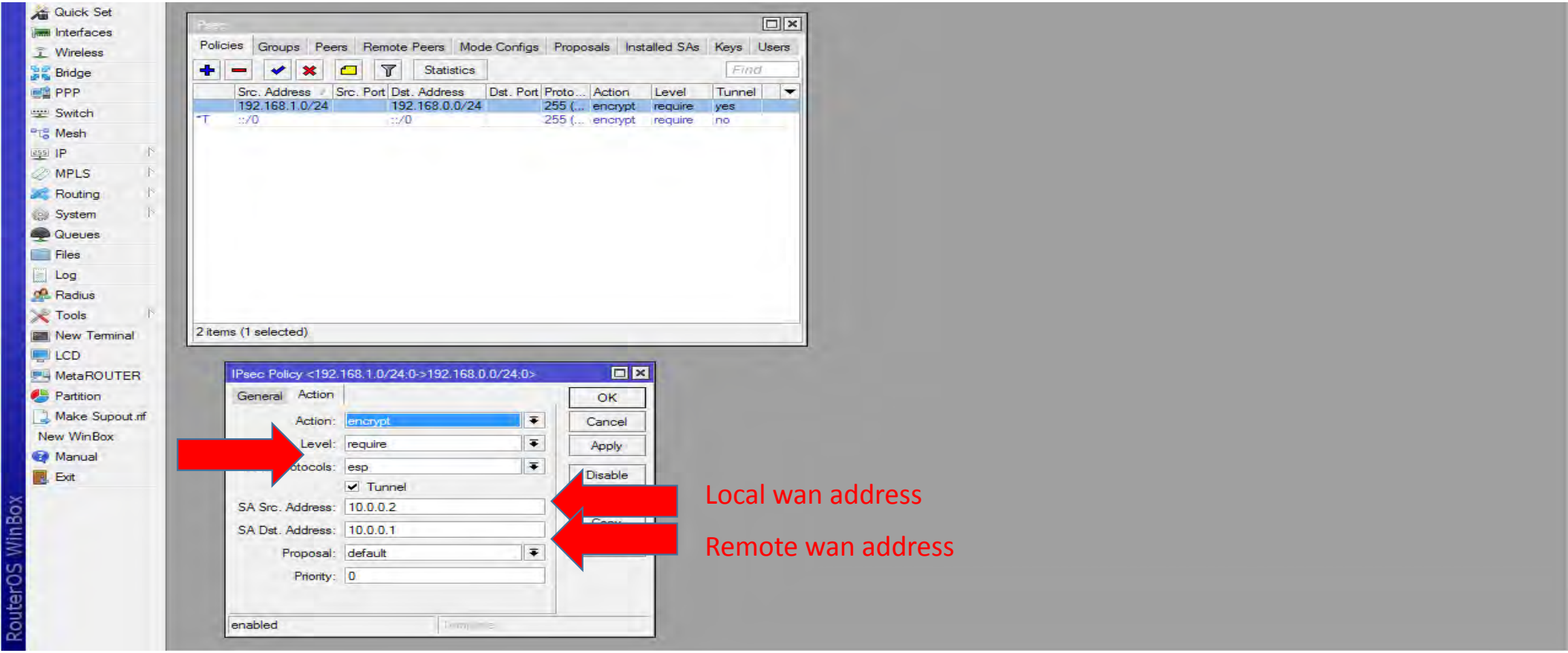
IPSEC Cisco IOS To Mikrotik



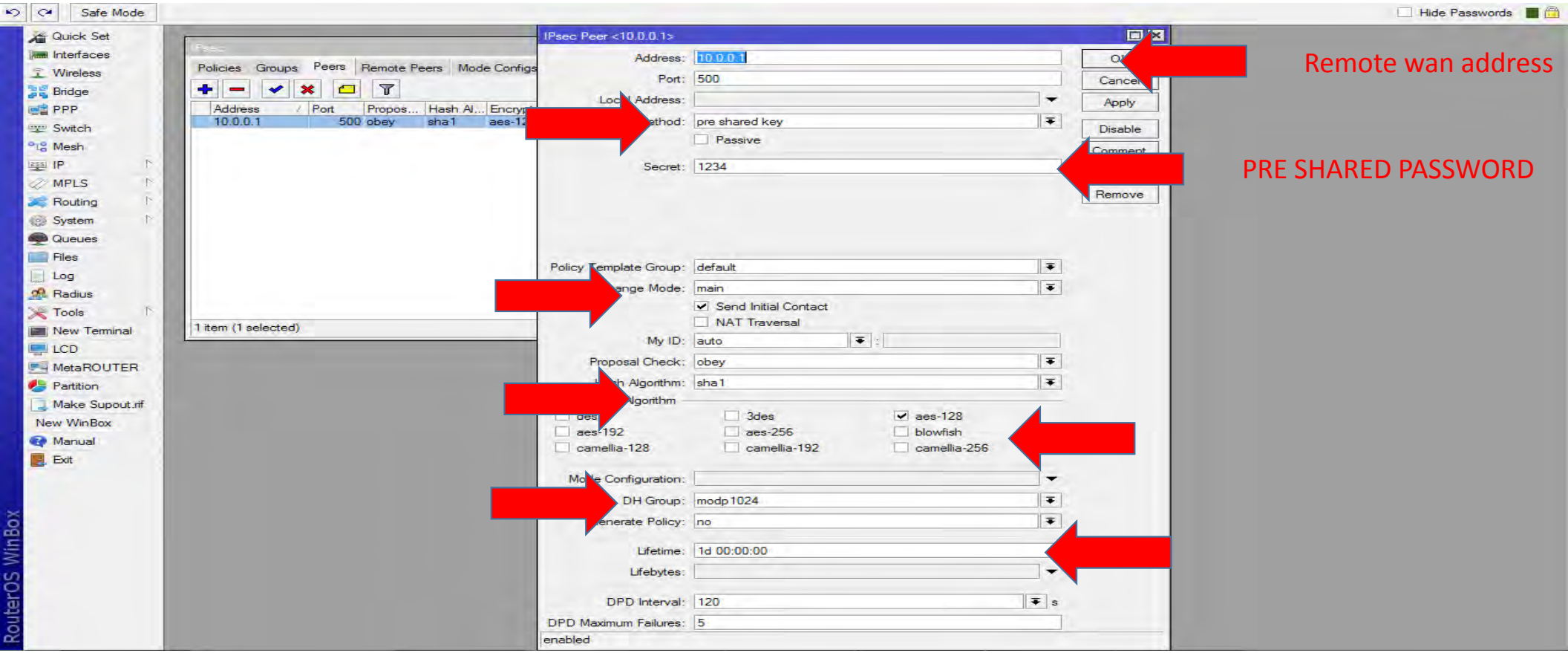
IPSEC Cisco IOS To Mikrotik



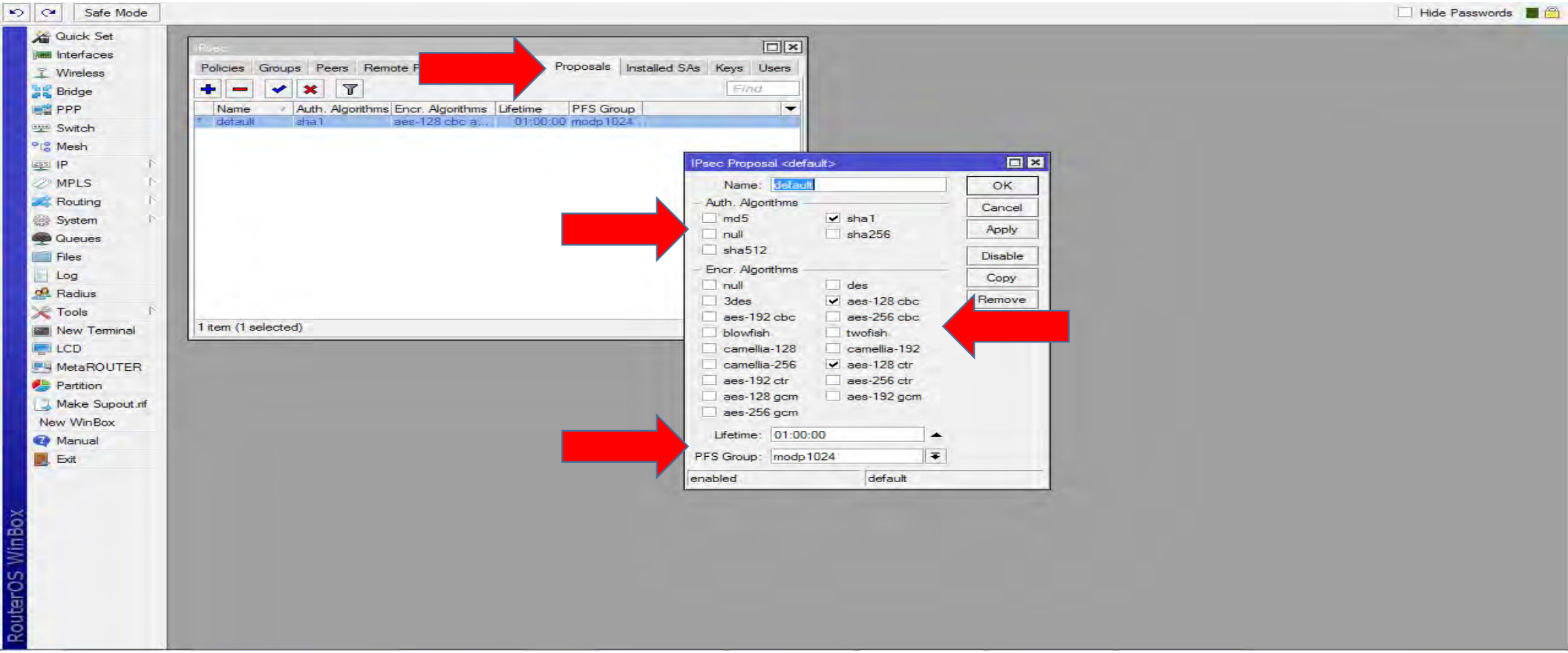
IPSEC Cisco IOS To Mikrotik



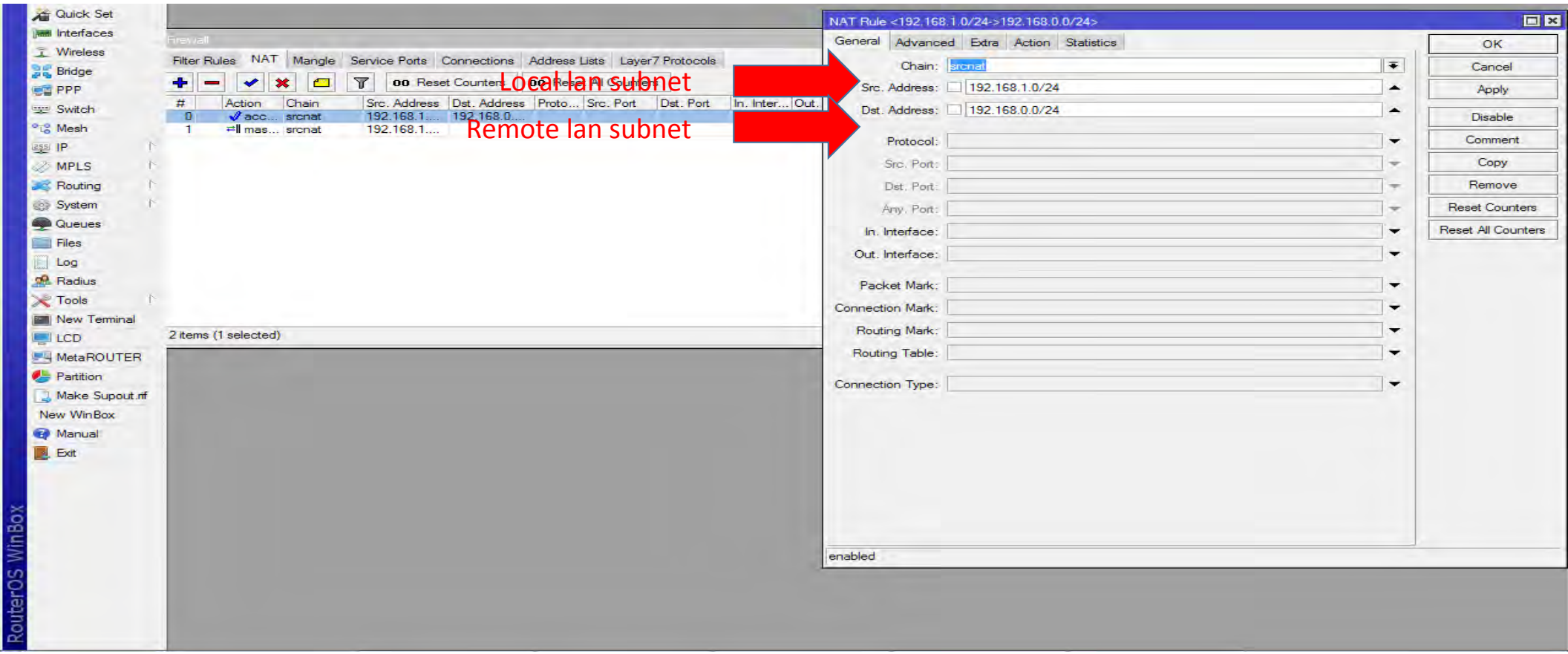
IPSEC Cisco IOS To Mikrotik



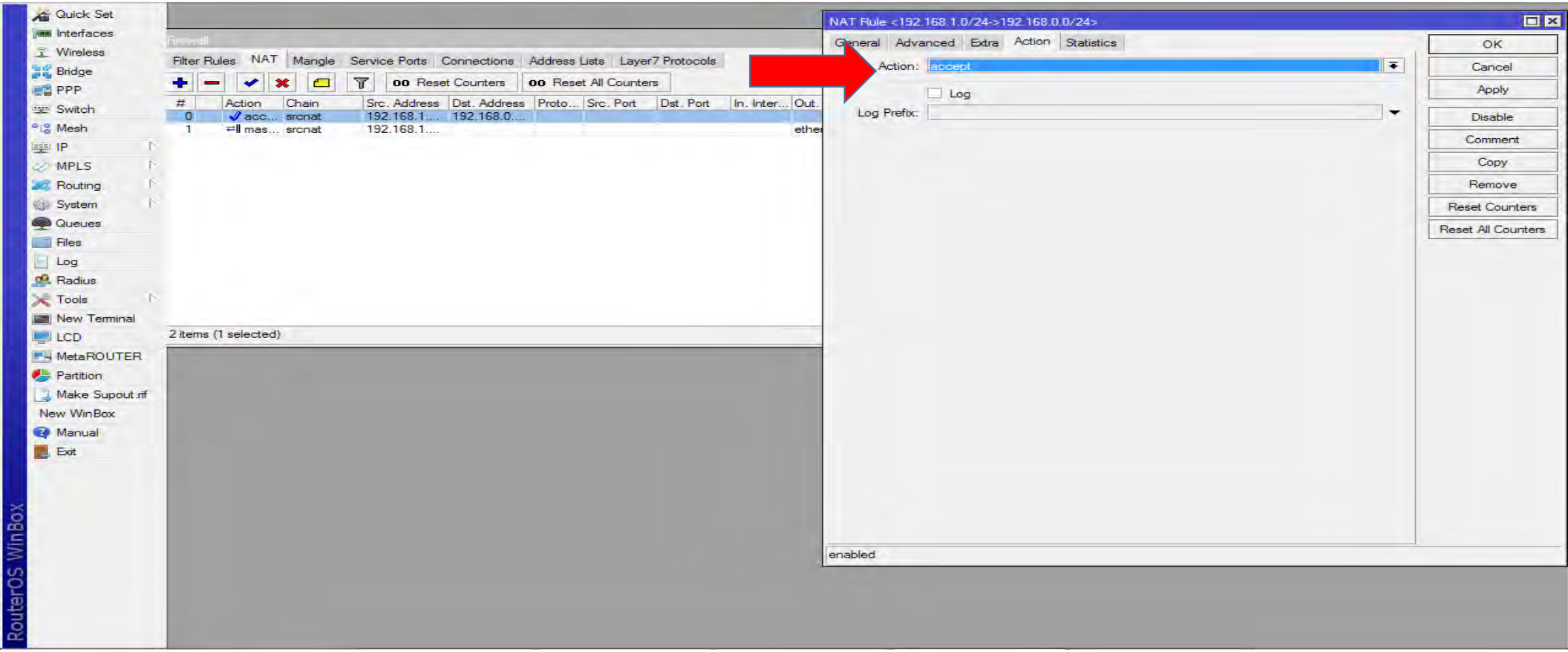
IPSEC Cisco IOS To Mikrotik



IPSEC Cisco IOS To Mikrotik



IPSEC Cisco IOS To Mikrotik



IPSEC Cisco IOS To Mikrotik

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key 1234 address 10.0.0.2 no-xauth
!
!
crypto ipsec transform-set remote esp-aes esp-sha-hmac
!
crypto map remote 5 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set remote
 set pfs group2
 match address remote
!
```

```
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
 crypto map remote
!
ip nat inside source list nonat interface FastEthernet0/0
overload
ip access-list extended nonat
 deny   ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
 permit ip 192.168.0.0 0.0.0.255 any
!
ip access-list extended remote
 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
!
```

IPSEC Cisco IOS To Mikrotik

```
vince_1841#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.0.0.1        10.0.0.2        QM_IDLE           1003 ACTIVE
```

IPSEC Cisco IOS To Mikrotik

- vince_1841#sh crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: remote, local addr 10.0.0.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 124, #pkts decrypt: 124, #pkts verify: 124
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

IPSEC Cisco IOS To Mikrotik

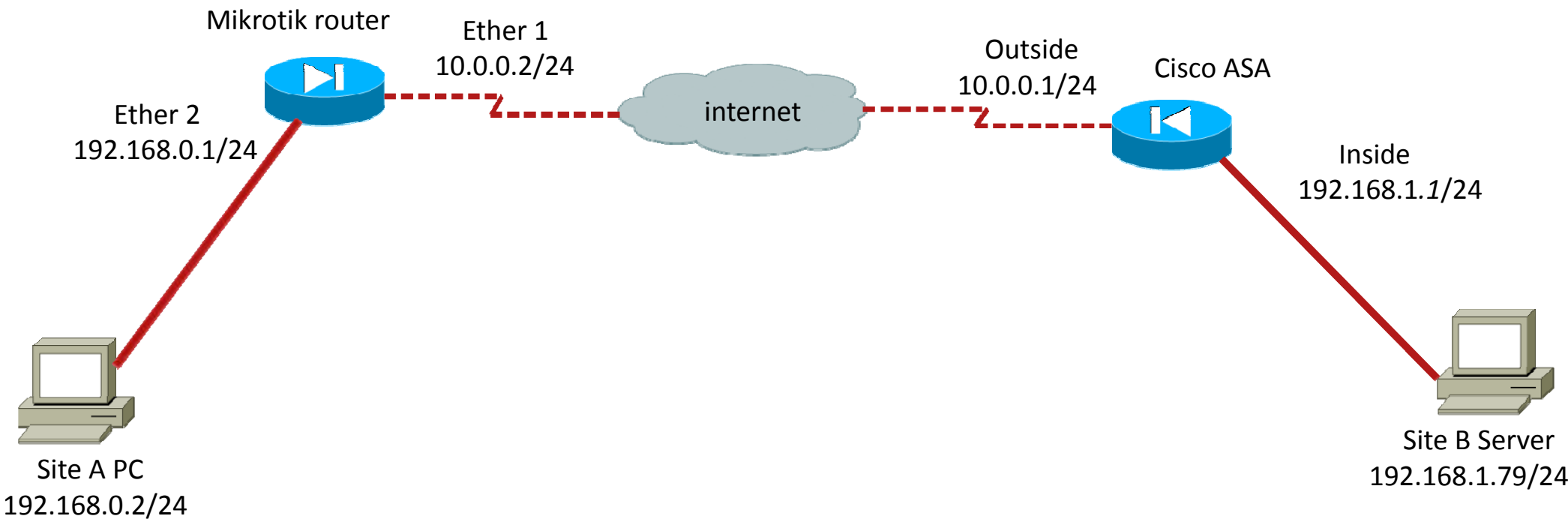
local crypto endpt.: 10.0.0.1, remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x23D508(2348296)
PFS (Y/N): Y, DH group: group2

inbound esp sas:
spi: 0x89A2A46B(2309137515)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: FPGA:3, sibling_flags 80000046, crypto map: remote
sa timing: remaining key lifetime (k/sec): (4533419/2928)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

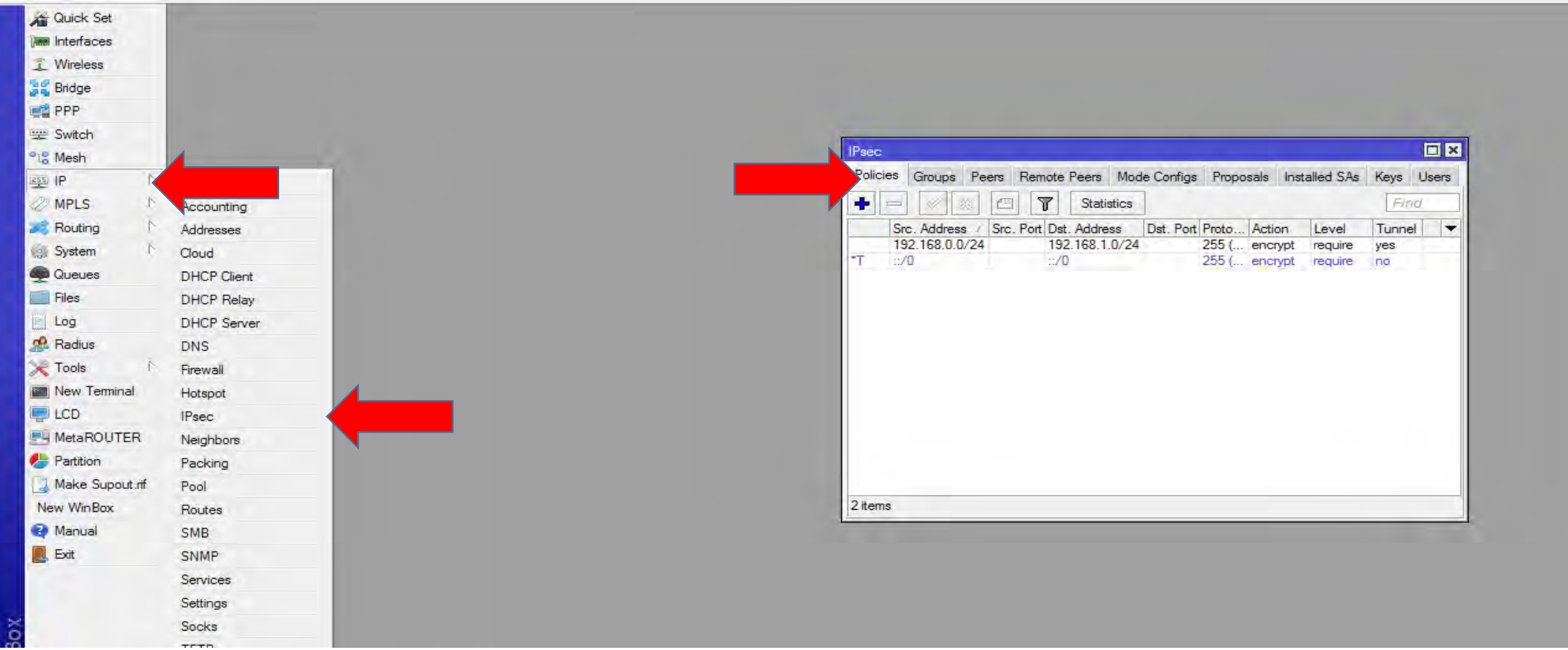
IPSEC Cisco IOS To Mikrotik

```
vince_1841#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.0.0.1        10.0.0.2        QM_IDLE           1003 ACTIVE
```

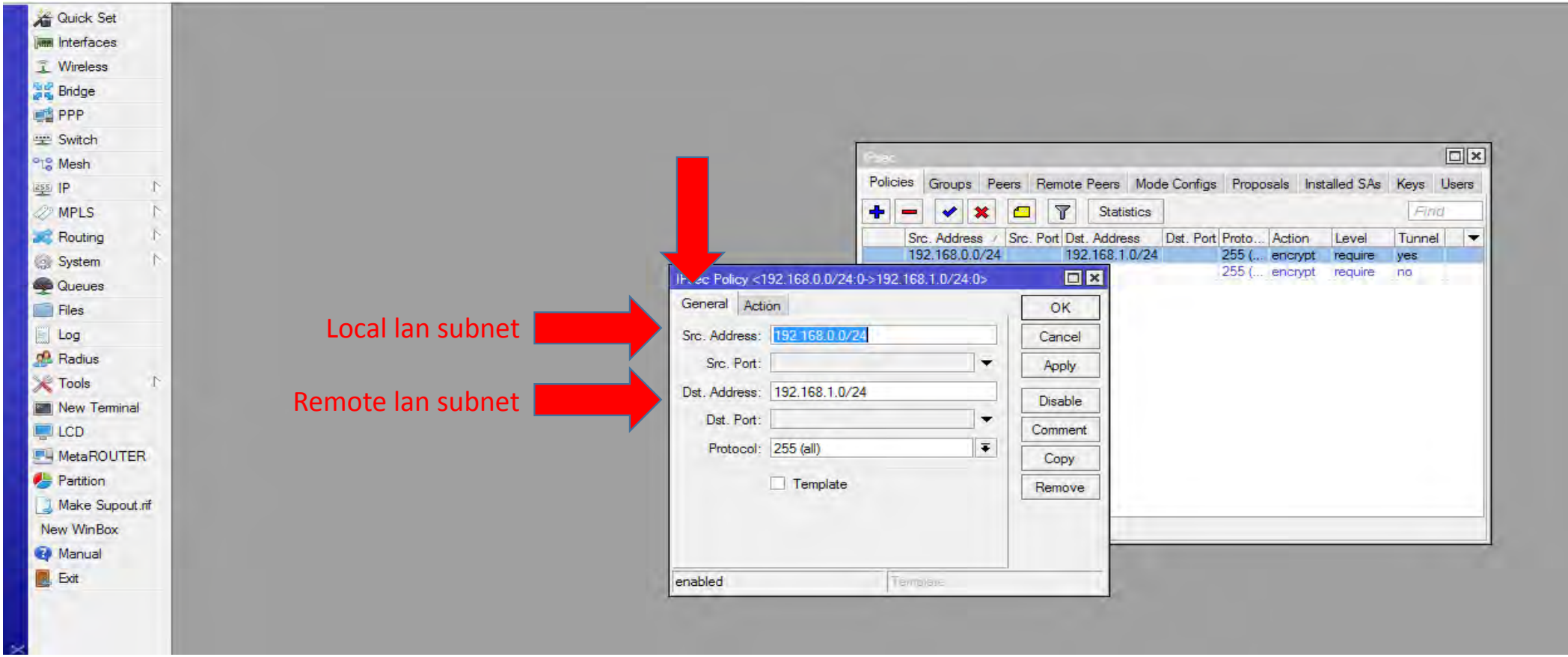
IPSEC Cisco ASA To Mikrotik



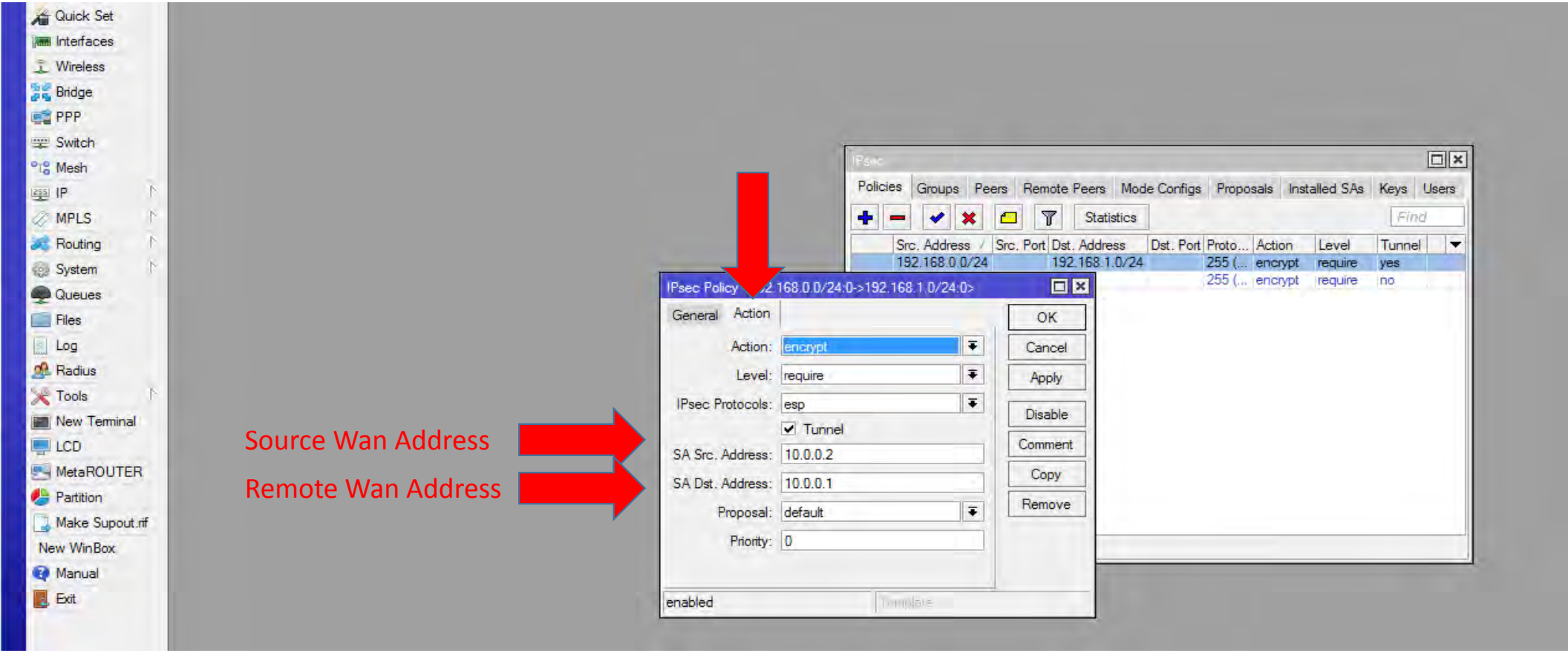
IPSEC Cisco ASA To Mikrotik



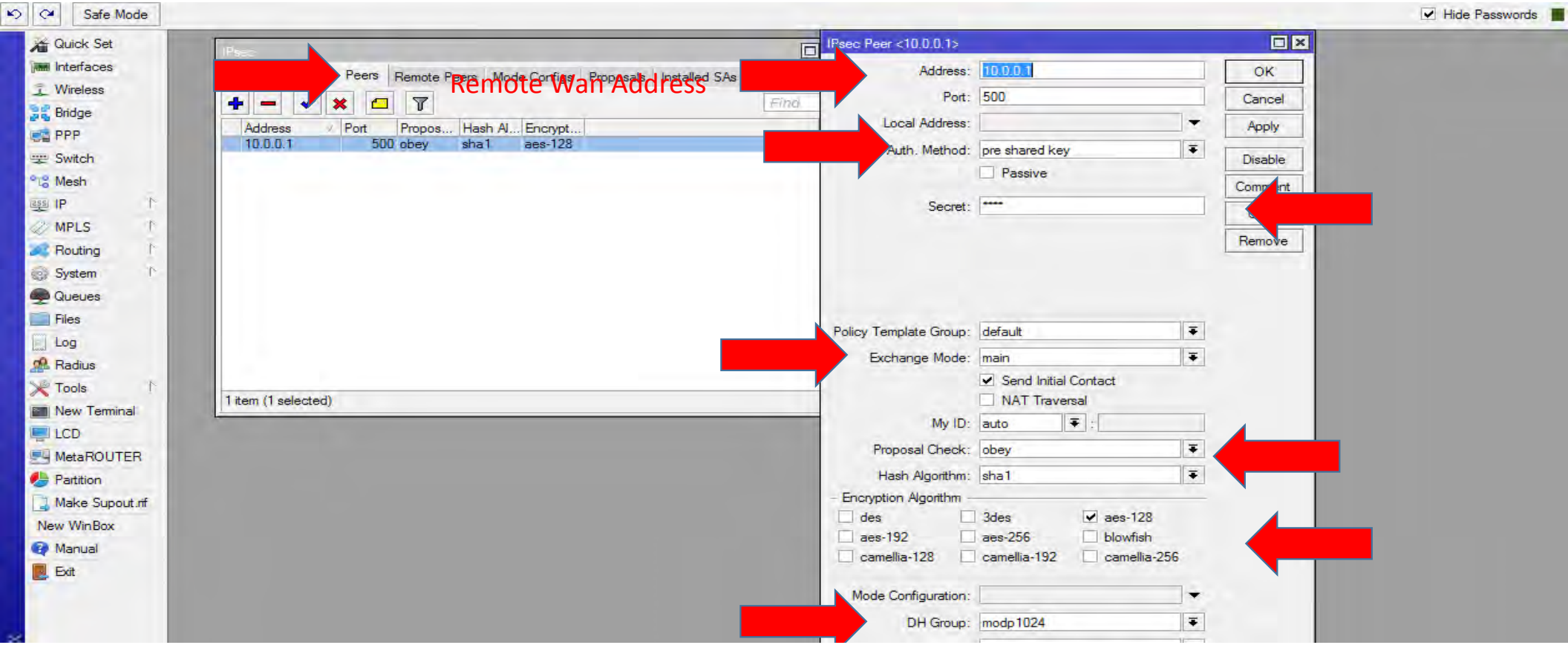
IPSEC Cisco ASA To Mikrotik



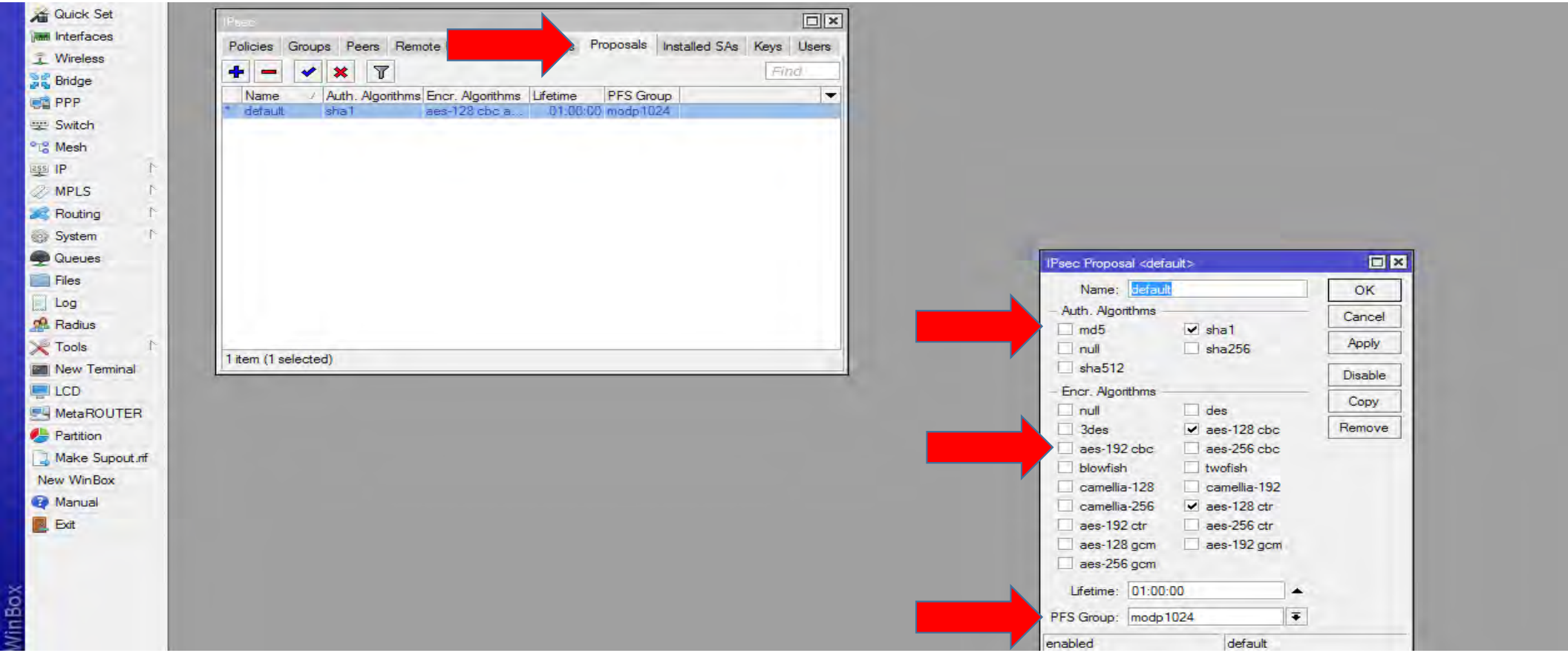
IPSEC Cisco ASA To Mikrotik



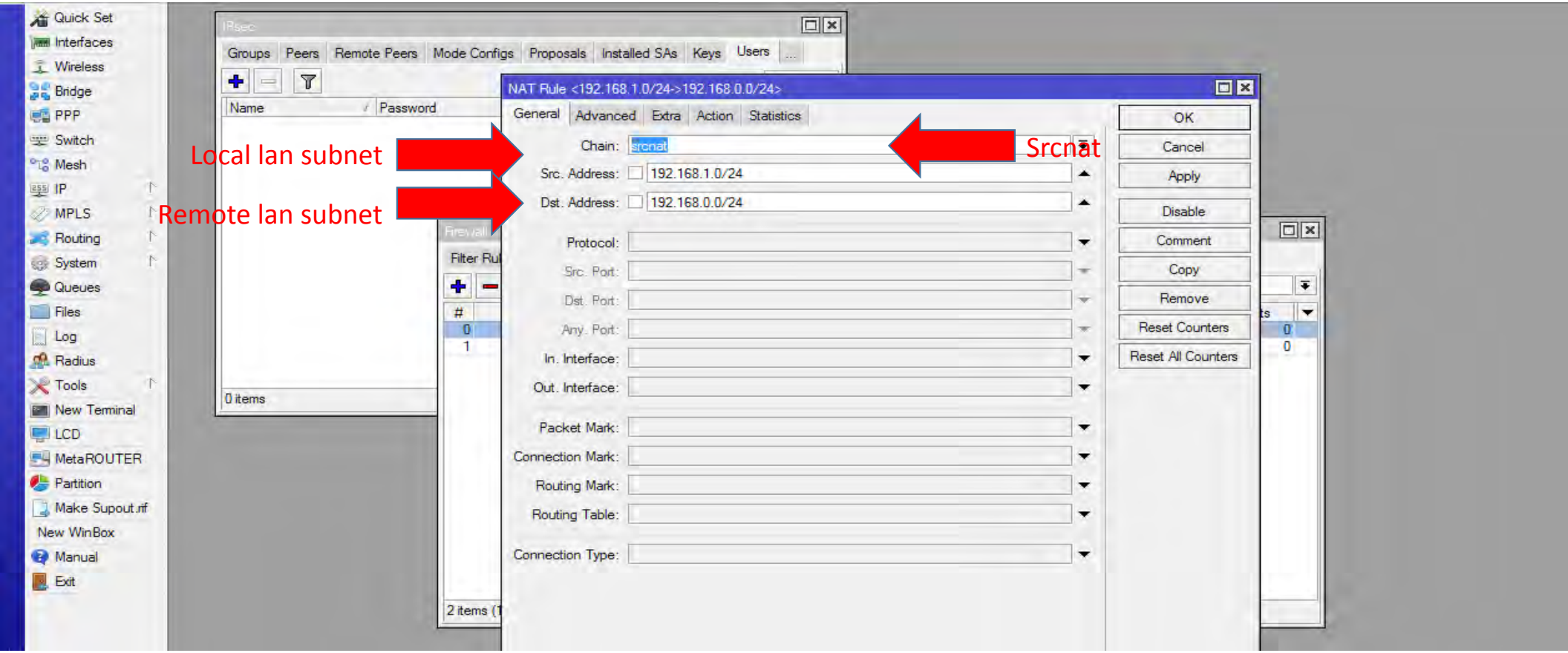
IPSEC Cisco ASA To Mikrotik



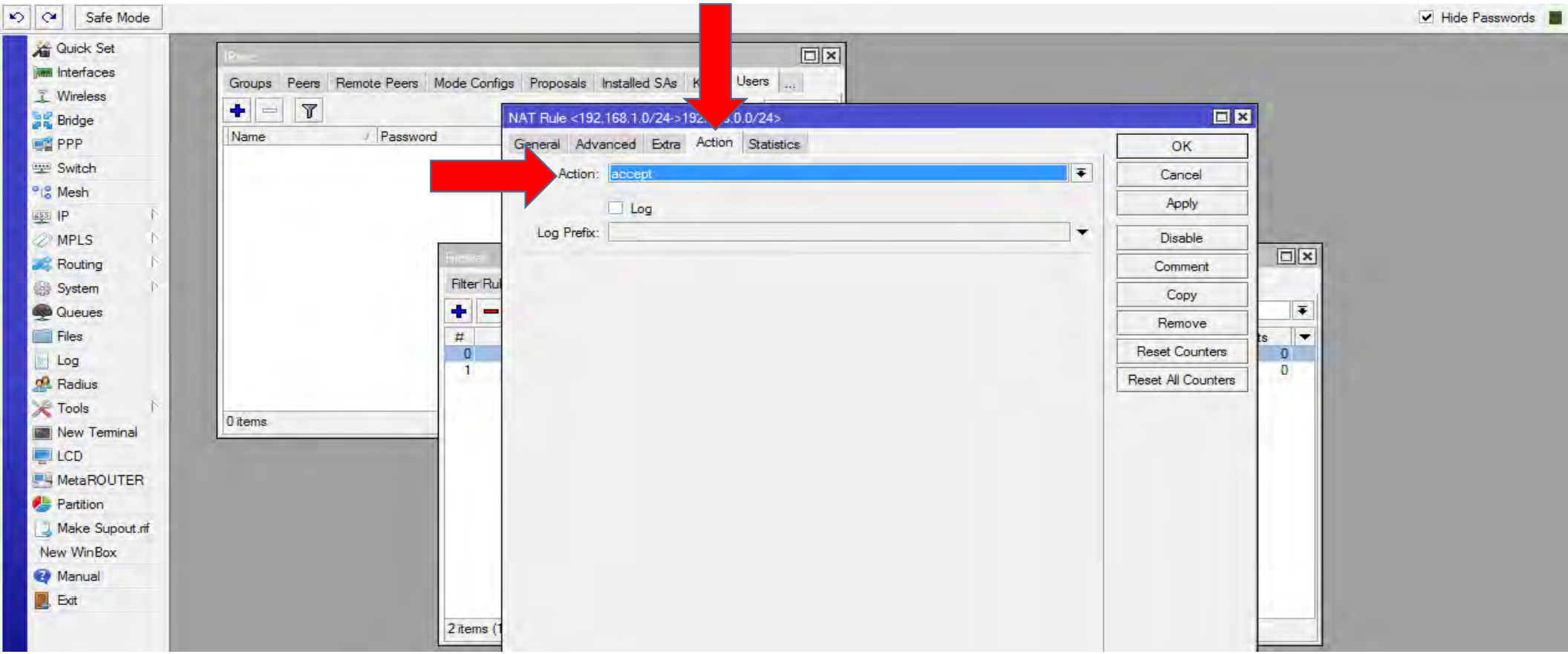
IPSEC Cisco ASA To Mikrotik



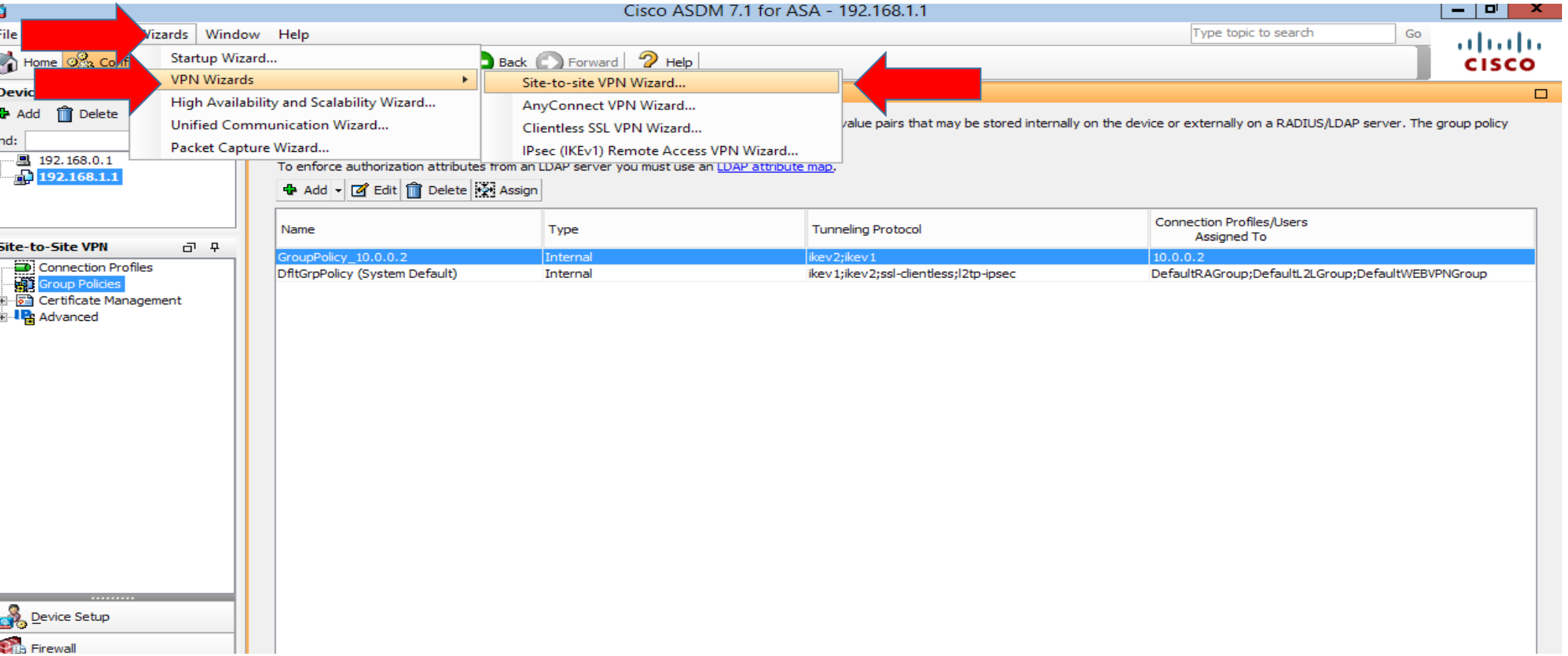
IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik

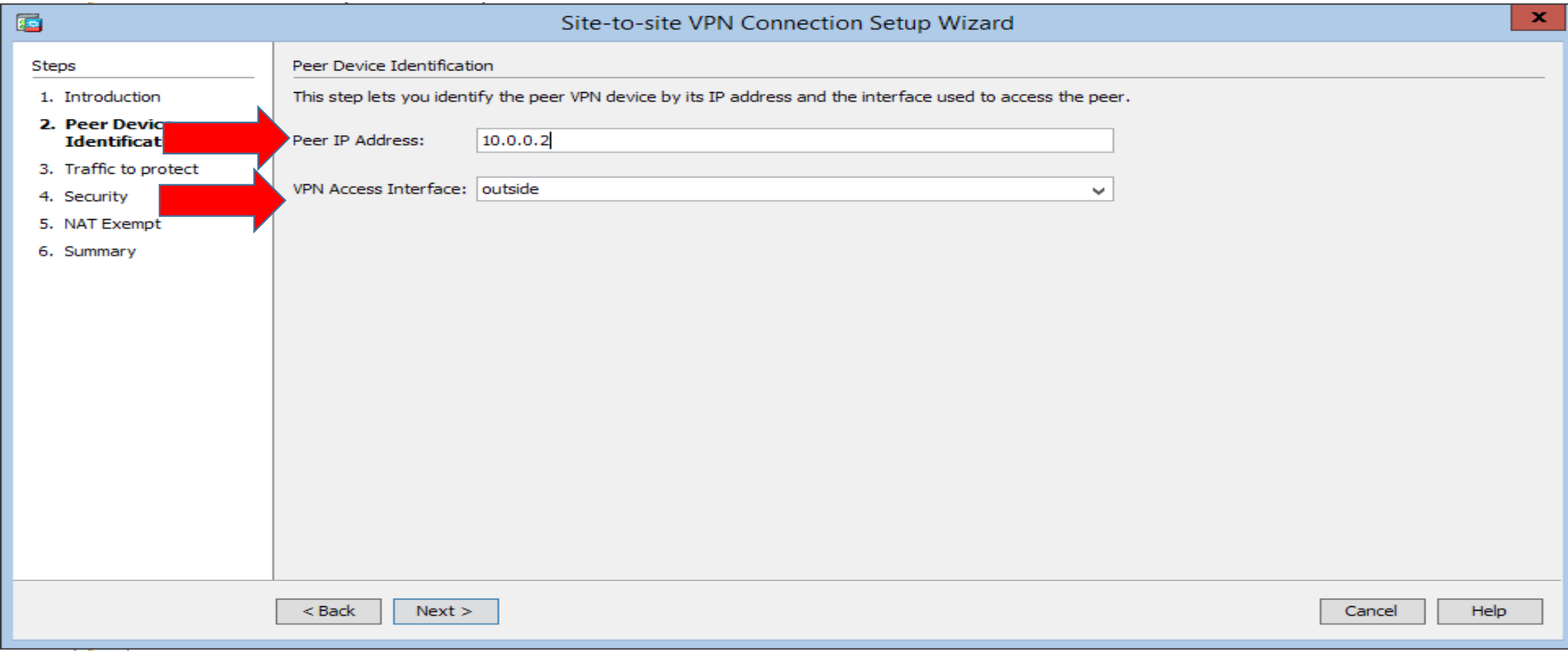


IPSEC Cisco ASA To Mikrotik

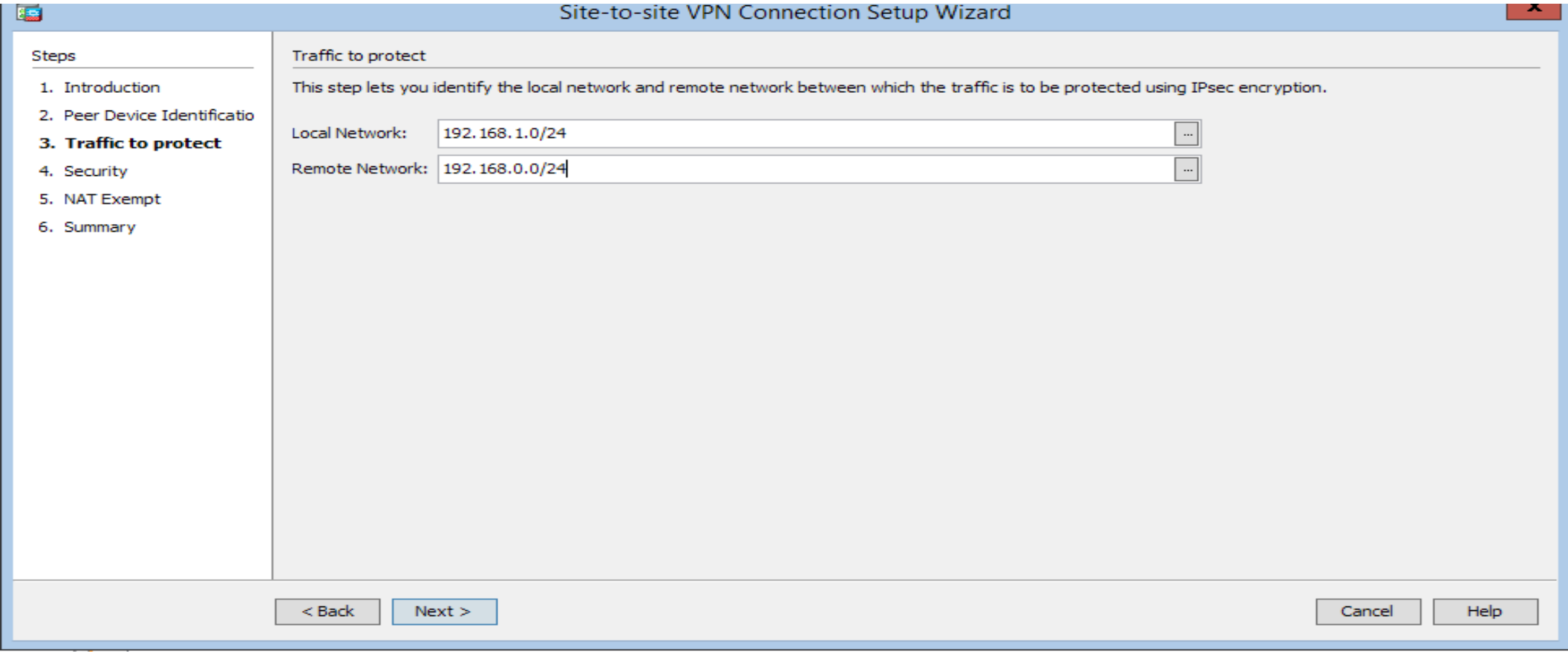


IPSEC Cisco ASA To Mikrotik

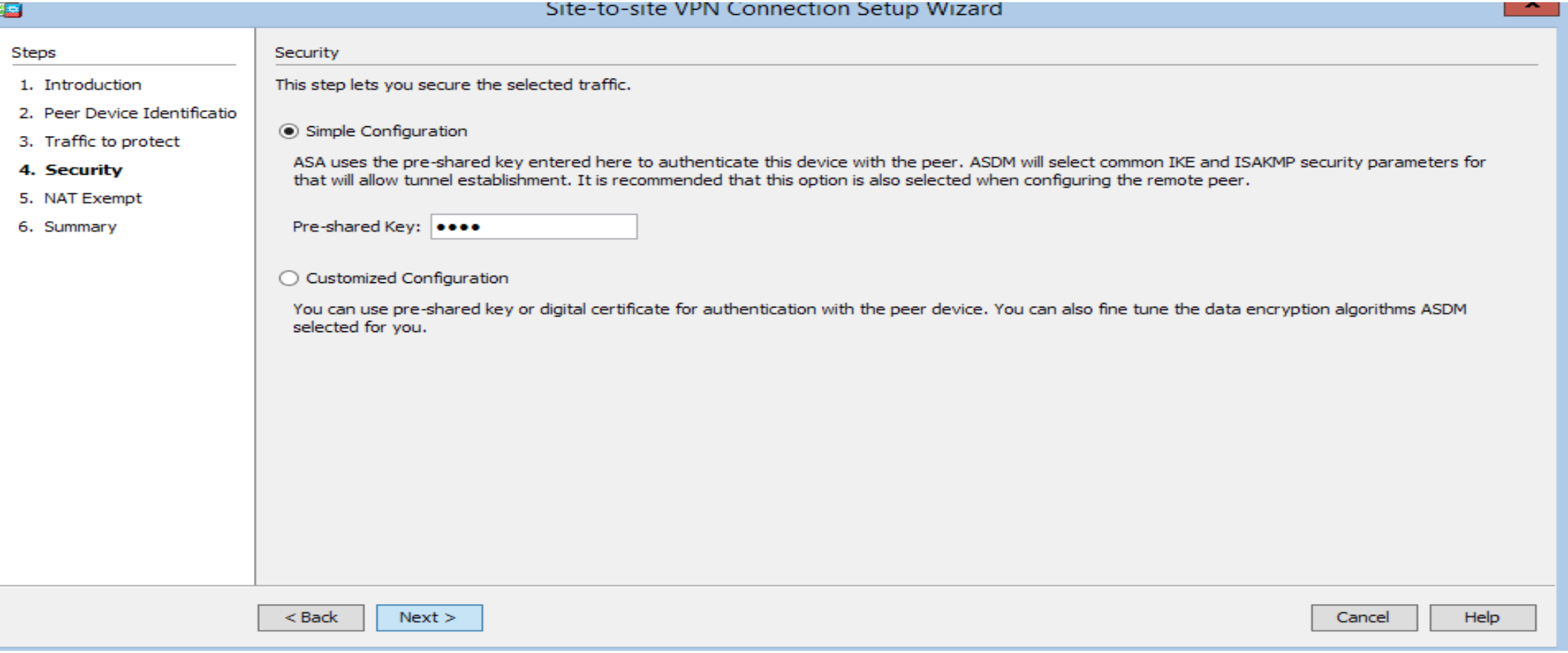
IPSEC Cisco ASA To Mikrotik



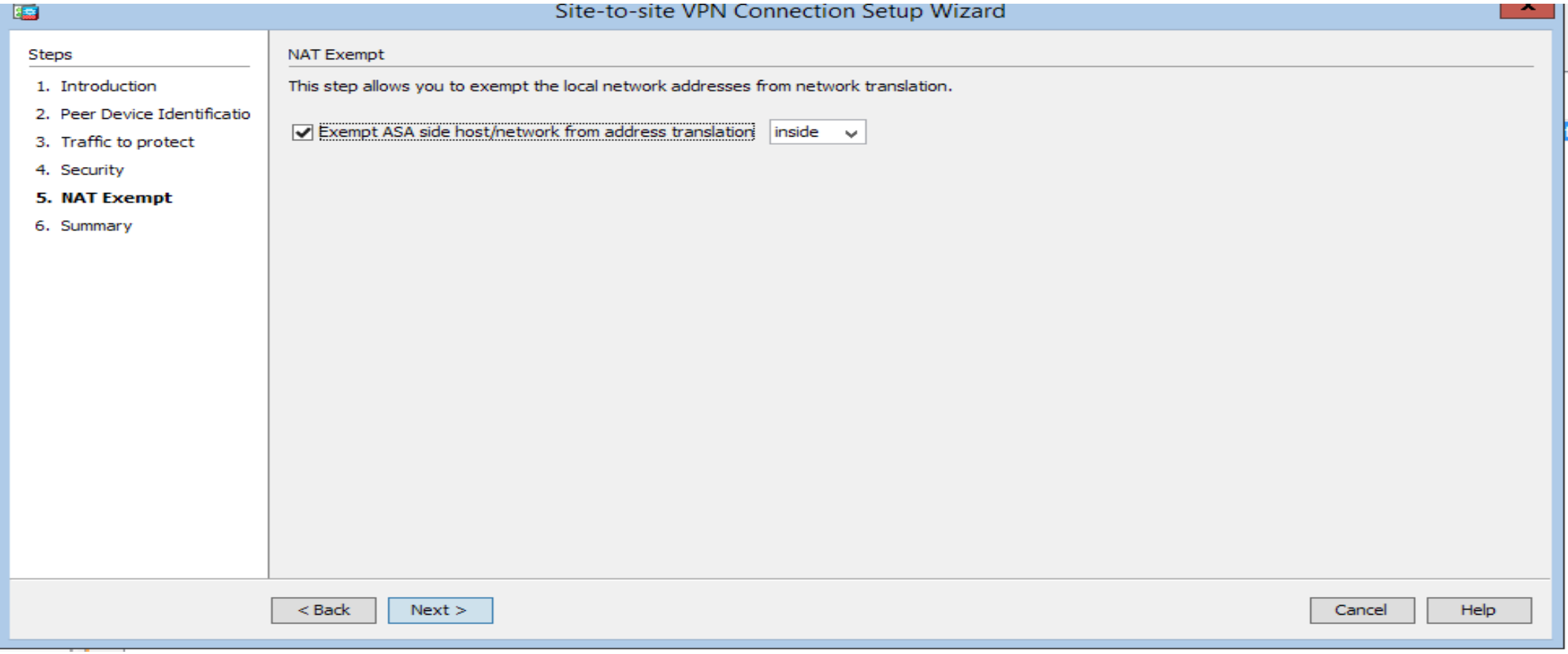
IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik

Site-to-site VPN Connection Setup Wizard

VPN Wizard

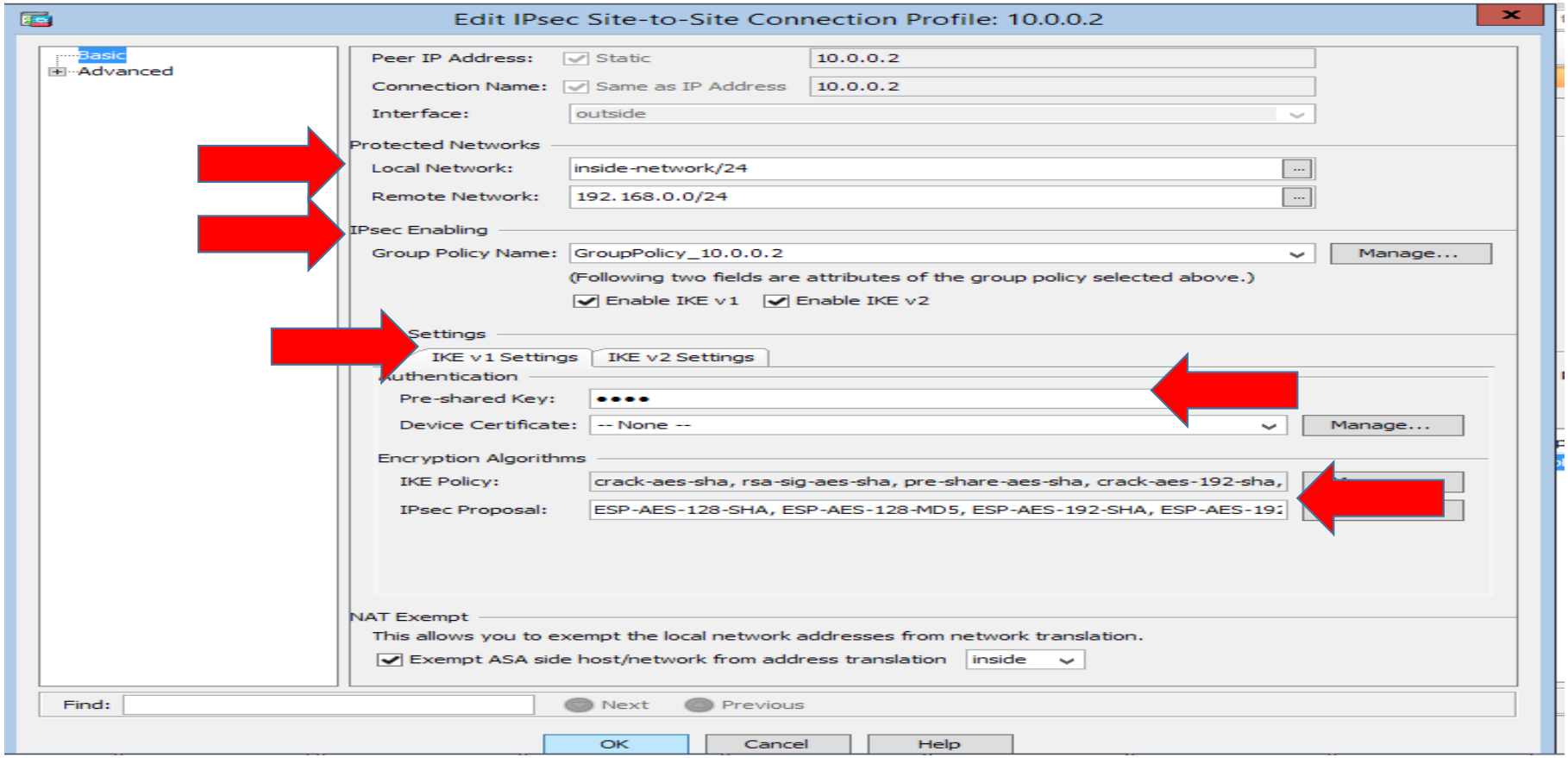
Summary

Here is the summary of the configuration.

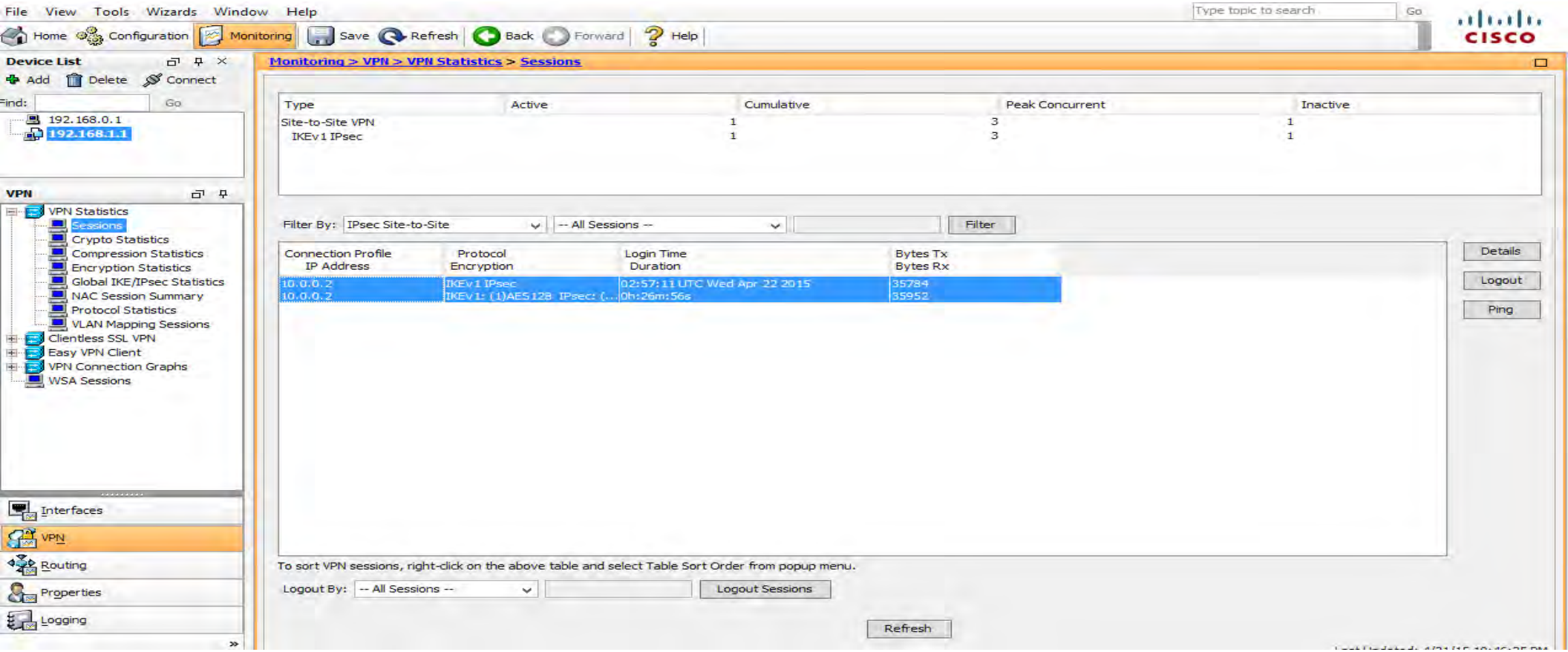
Name	Value
Summary	
Peer Device IP Address	10.0.0.2
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.1.0/24 Remote Network: 192.168.0.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, crack-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-256-sha, crack-3des-sha, rsa-sig-3des-sha, pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
IKE v2	

< Back | Finish | Cancel | Help

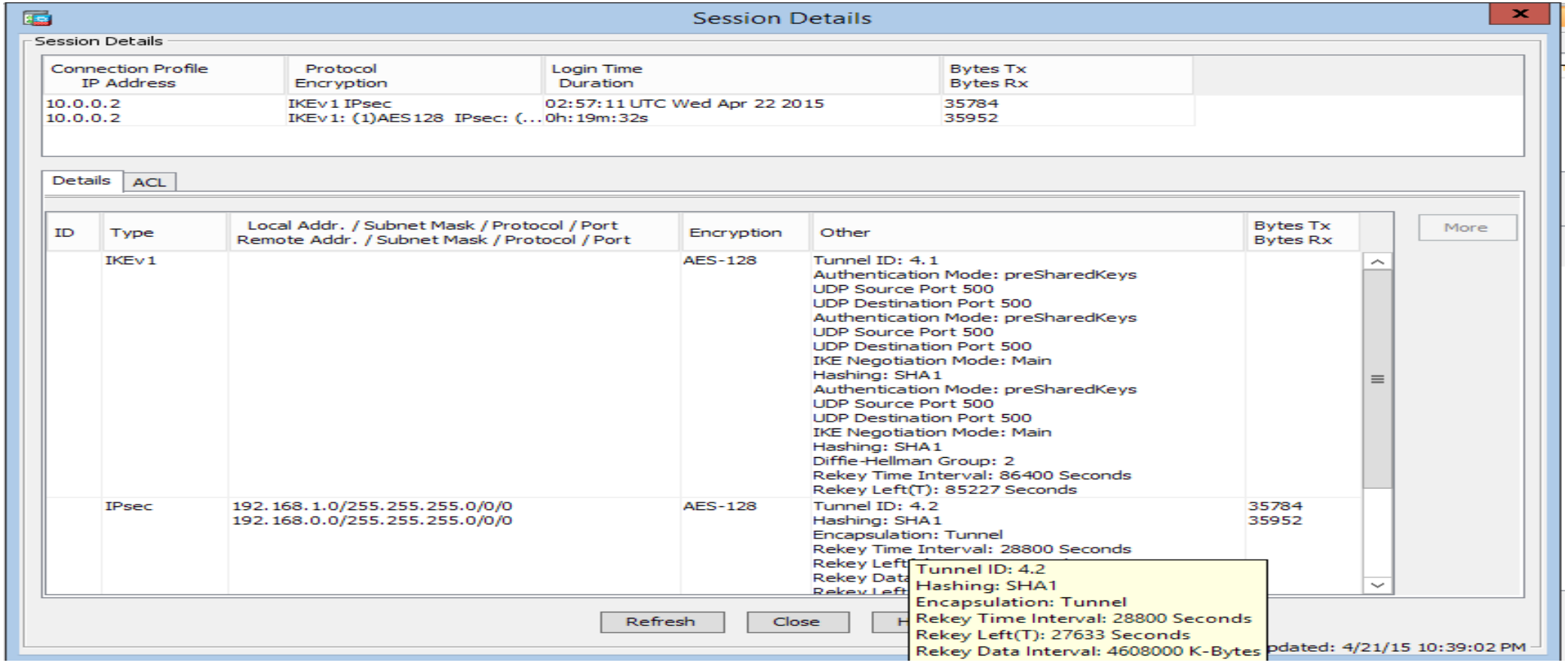
IPSEC Cisco ASA To Mikrotik



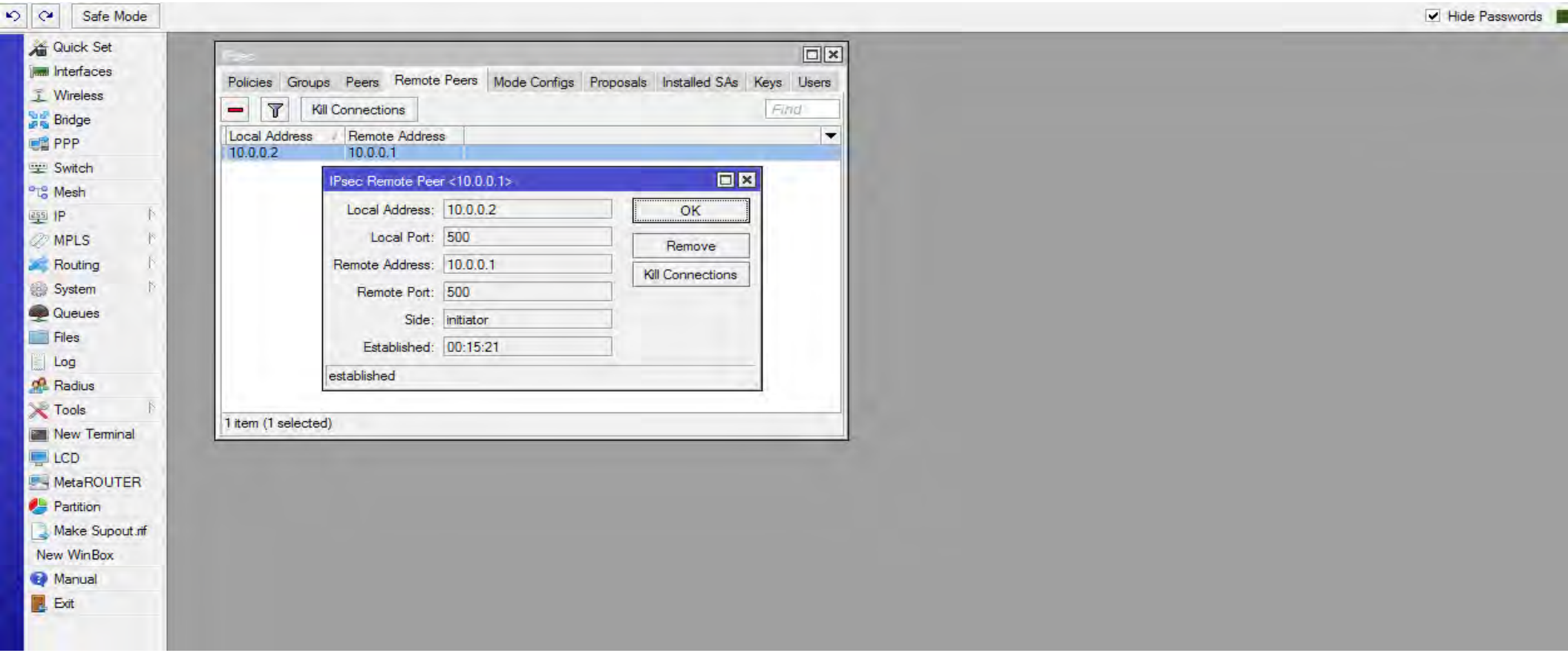
IPSEC Cisco ASA To Mikrotik



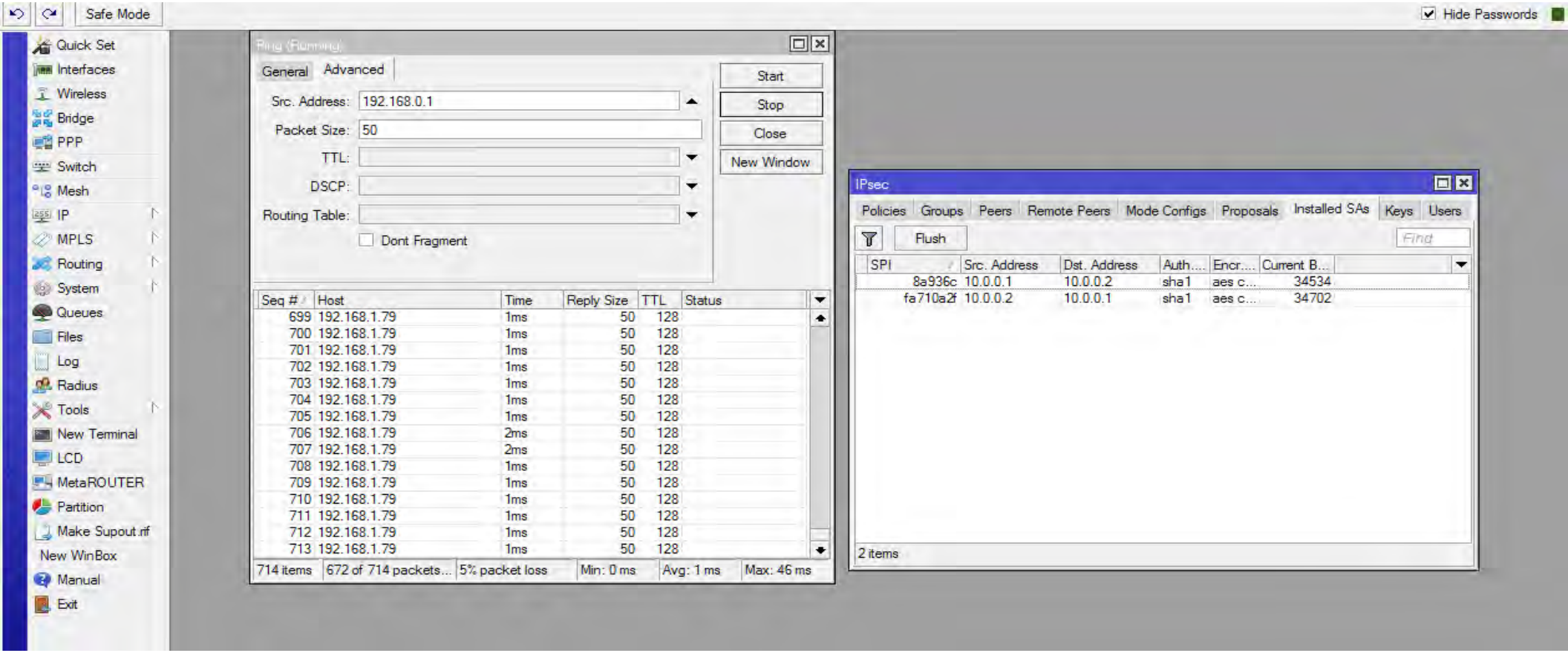
IPSEC Cisco ASA To Mikrotik



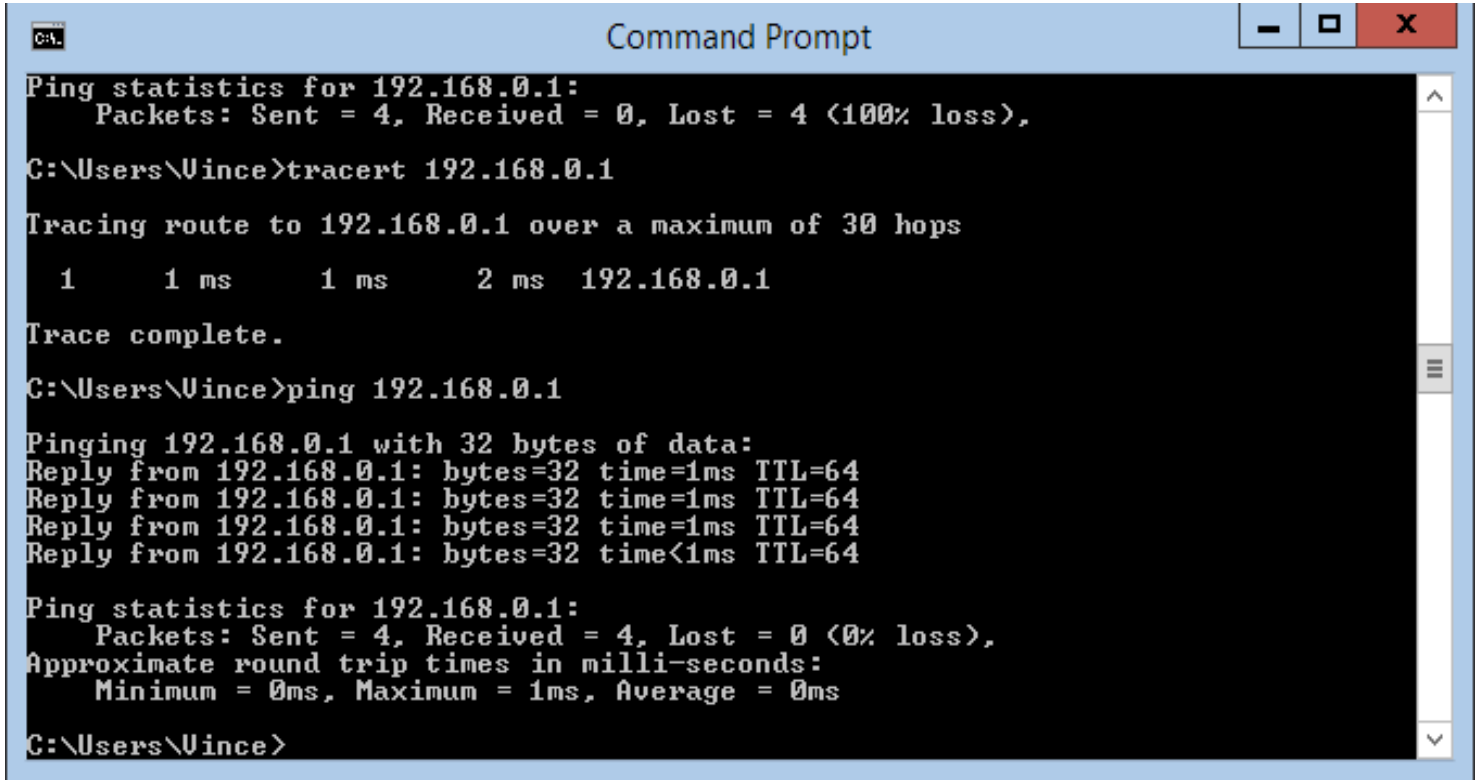
IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik