

Godinich Consulting

VPN's Between Mikrotik and
3rd Party Devices

Vince Godinich

experience

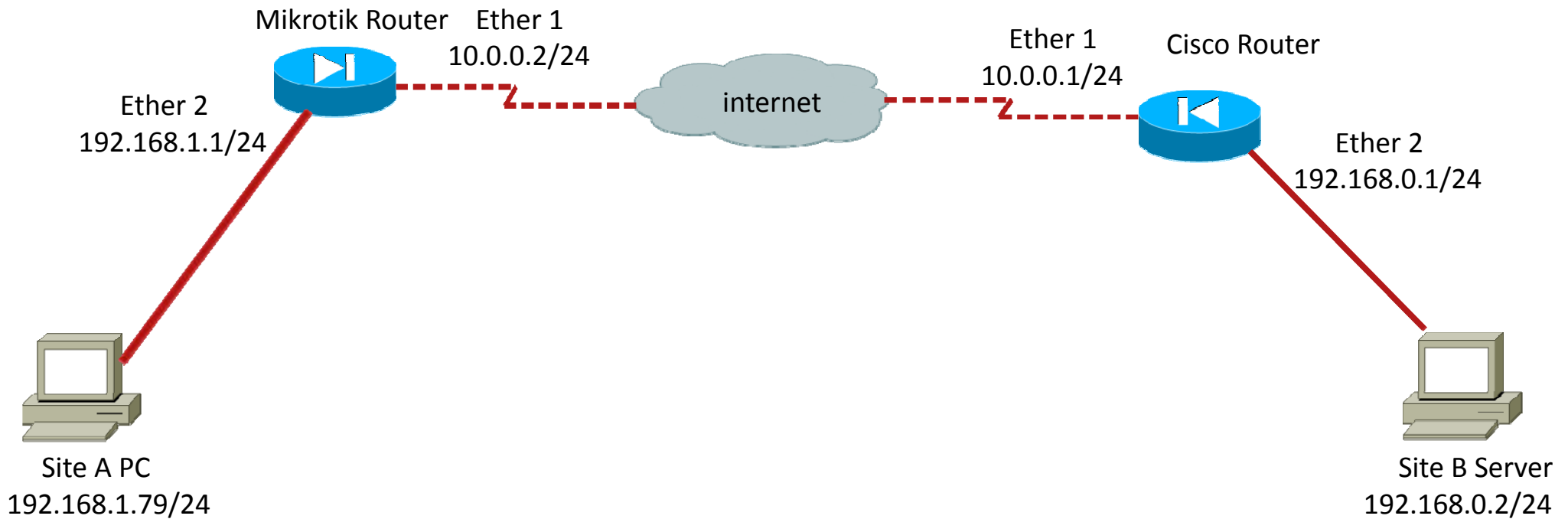
TOPICS

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

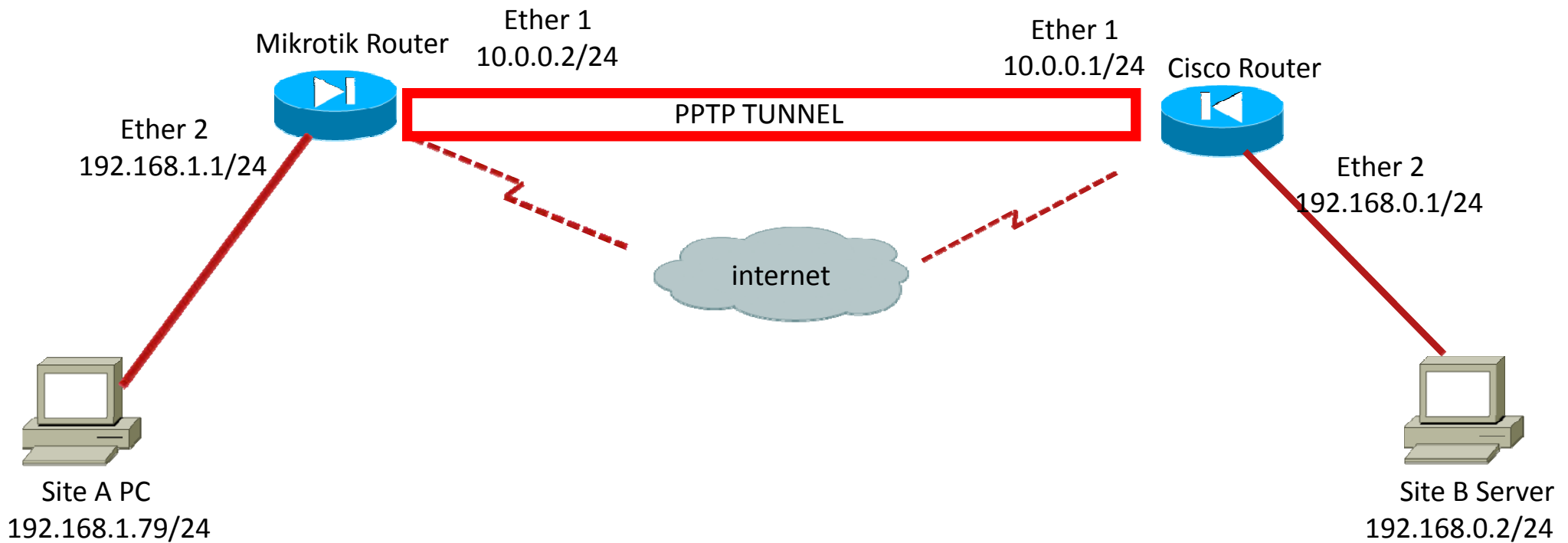
PPTP Mikrotik Client to Cisco Server

- 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

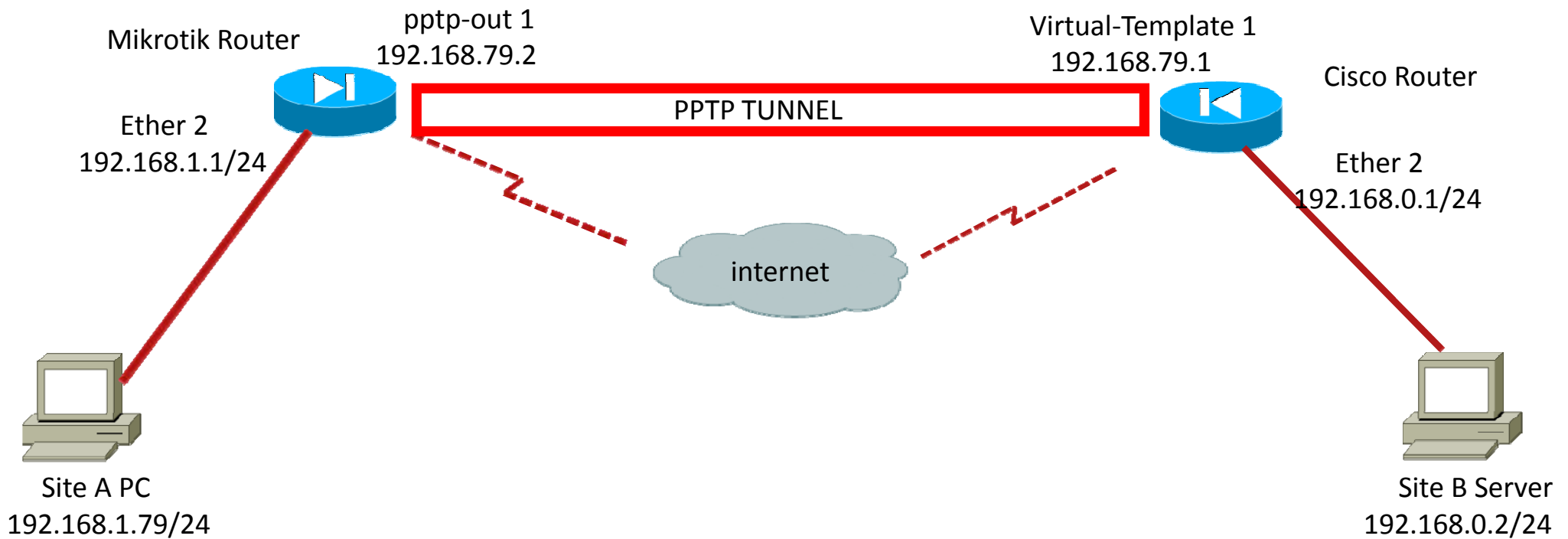
PPTP Mikrotik Client to Cisco Server



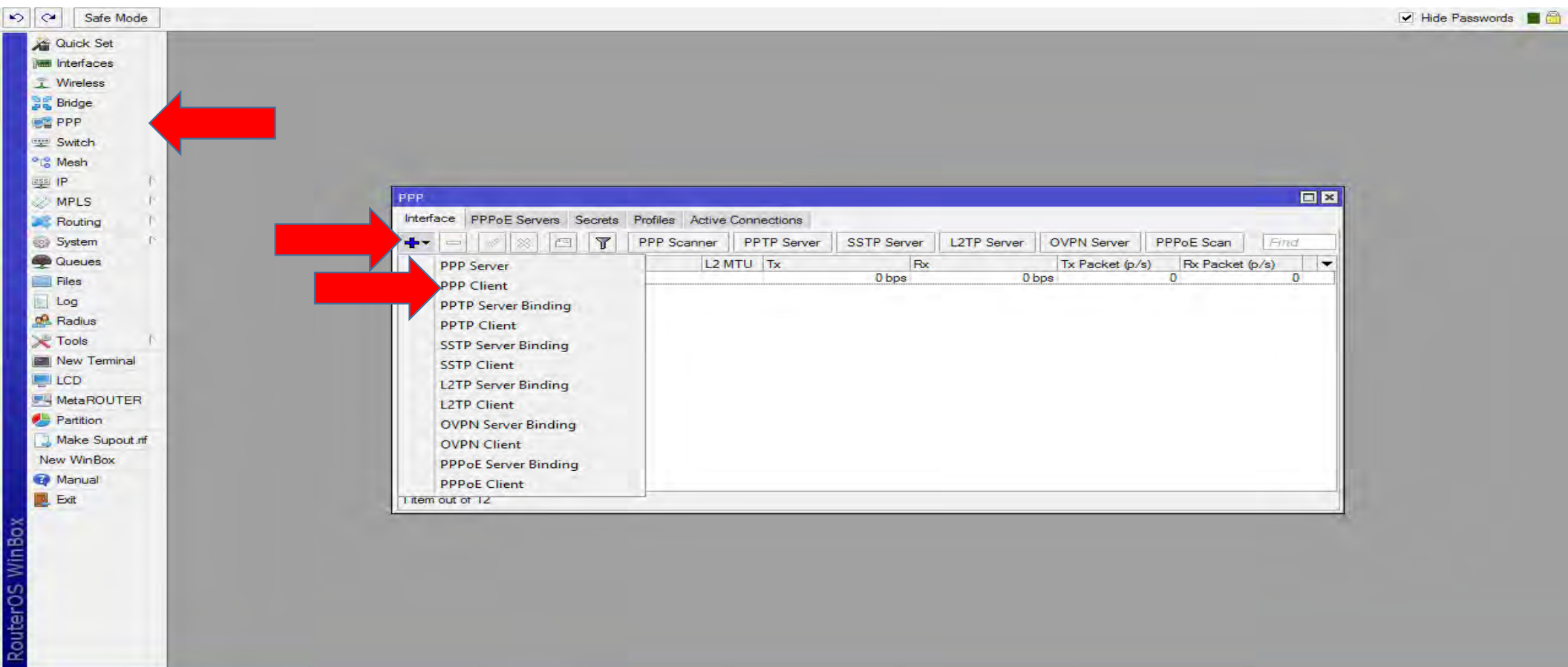
PPTP Mikrotik Client to Cisco Server



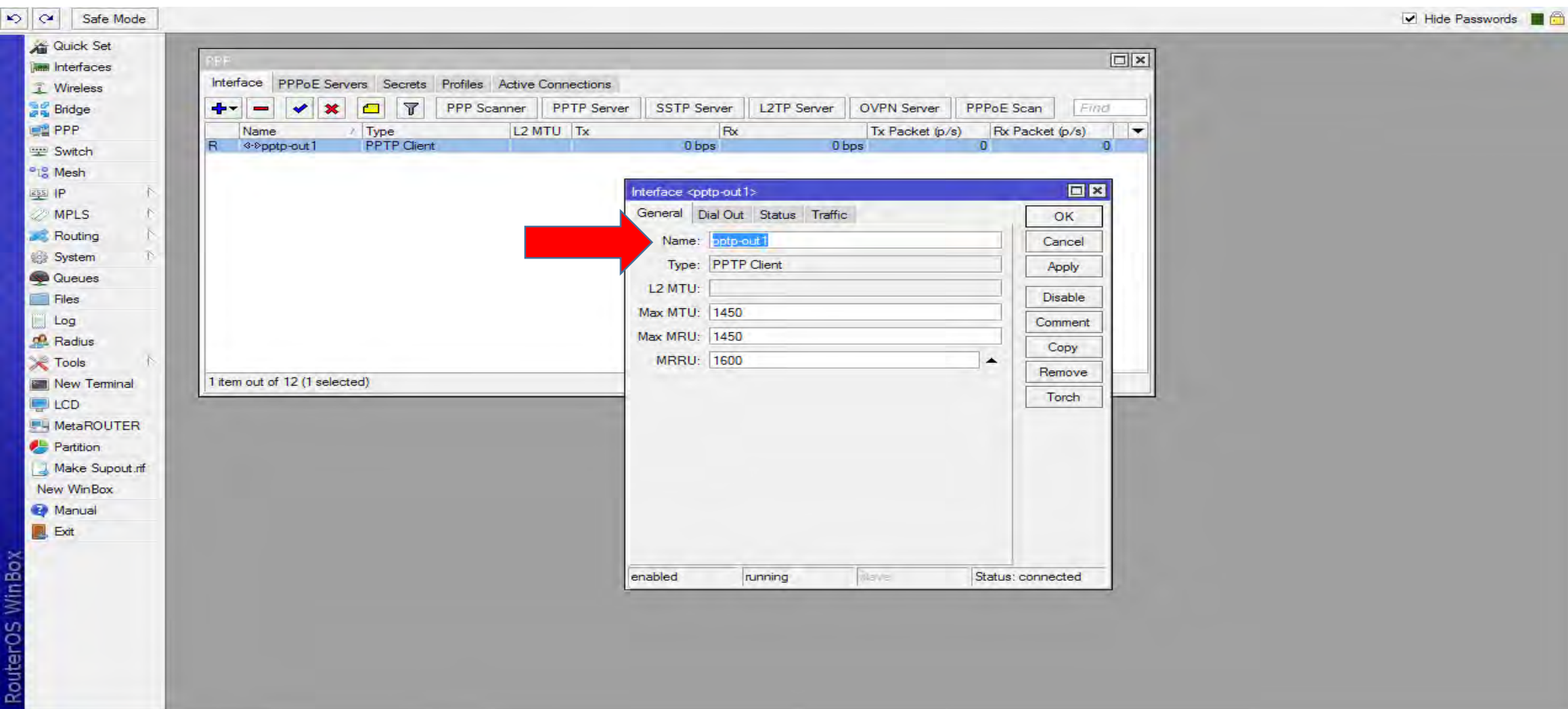
PPTP Mikrotik Client to Cisco Server



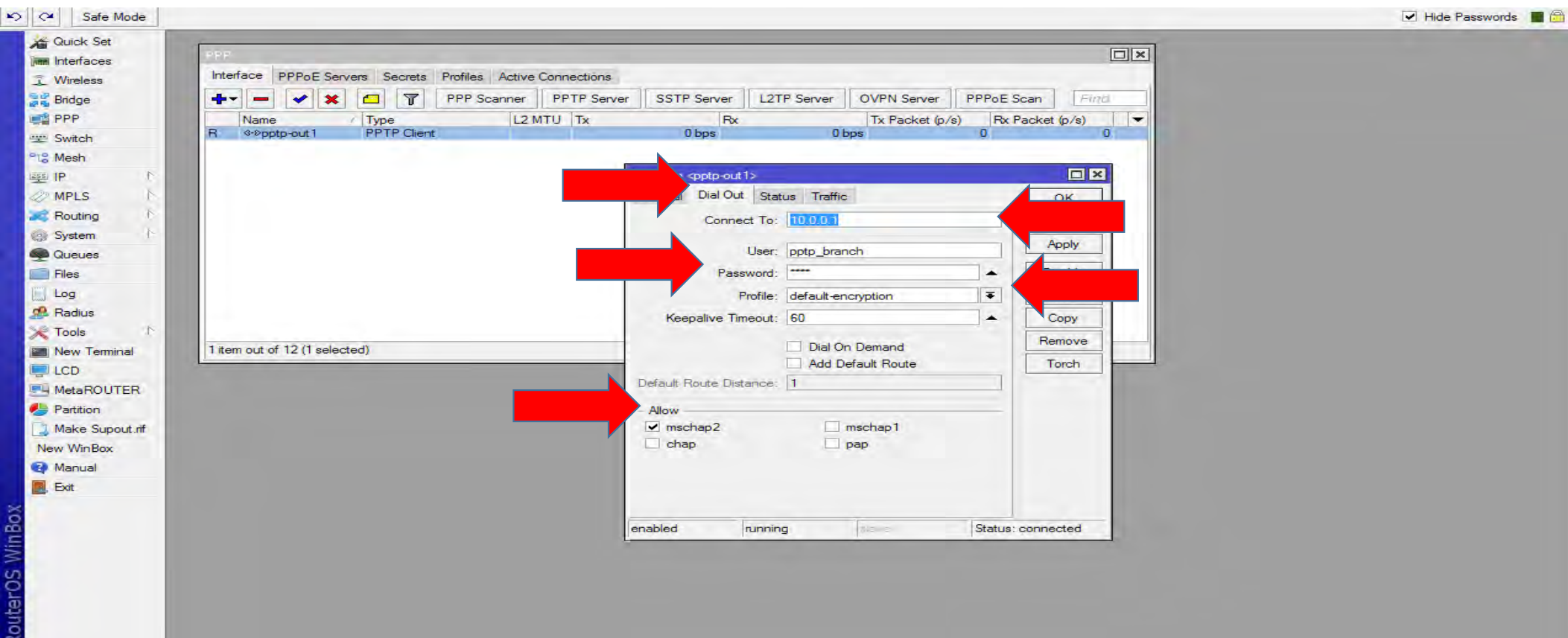
PPTP Mikrotik Client to Cisco Server



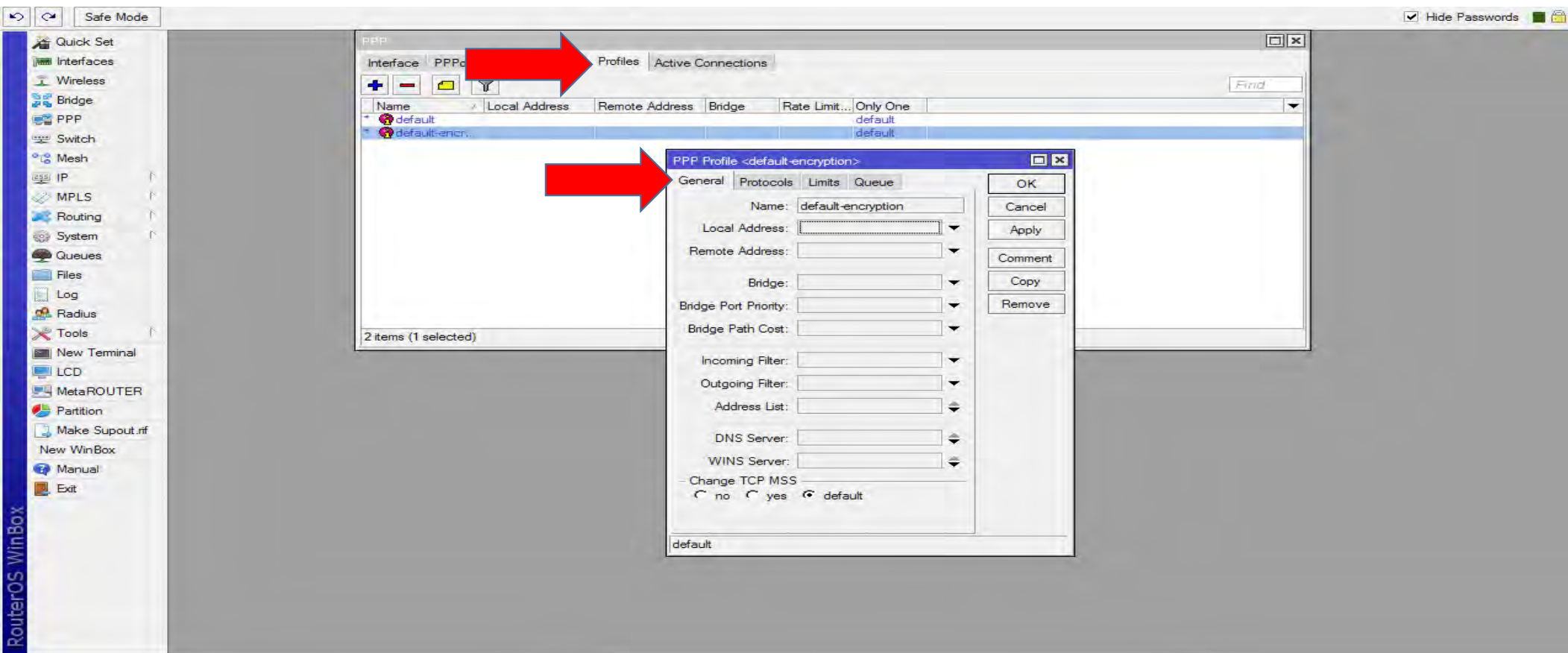
PPTP Mikrotik Client to Cisco Server



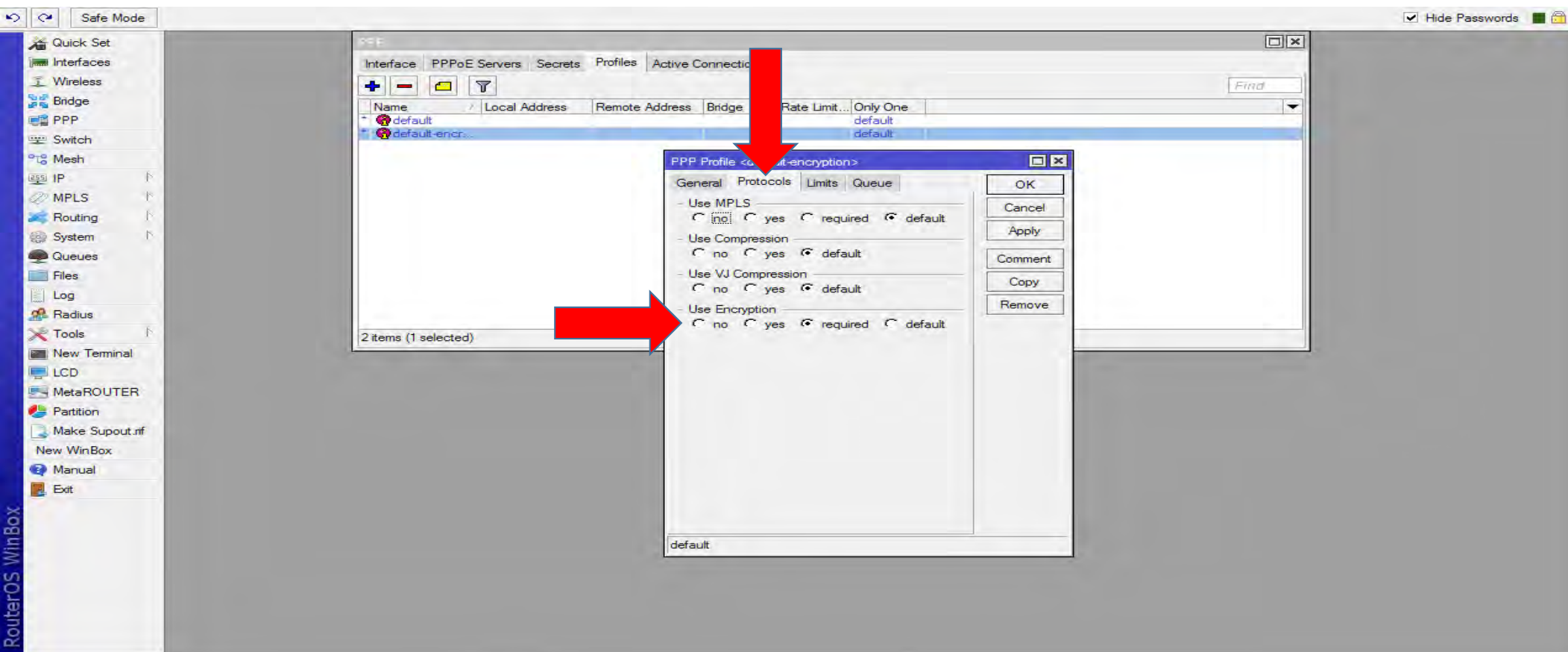
PPTP Mikrotik Client to Cisco Server



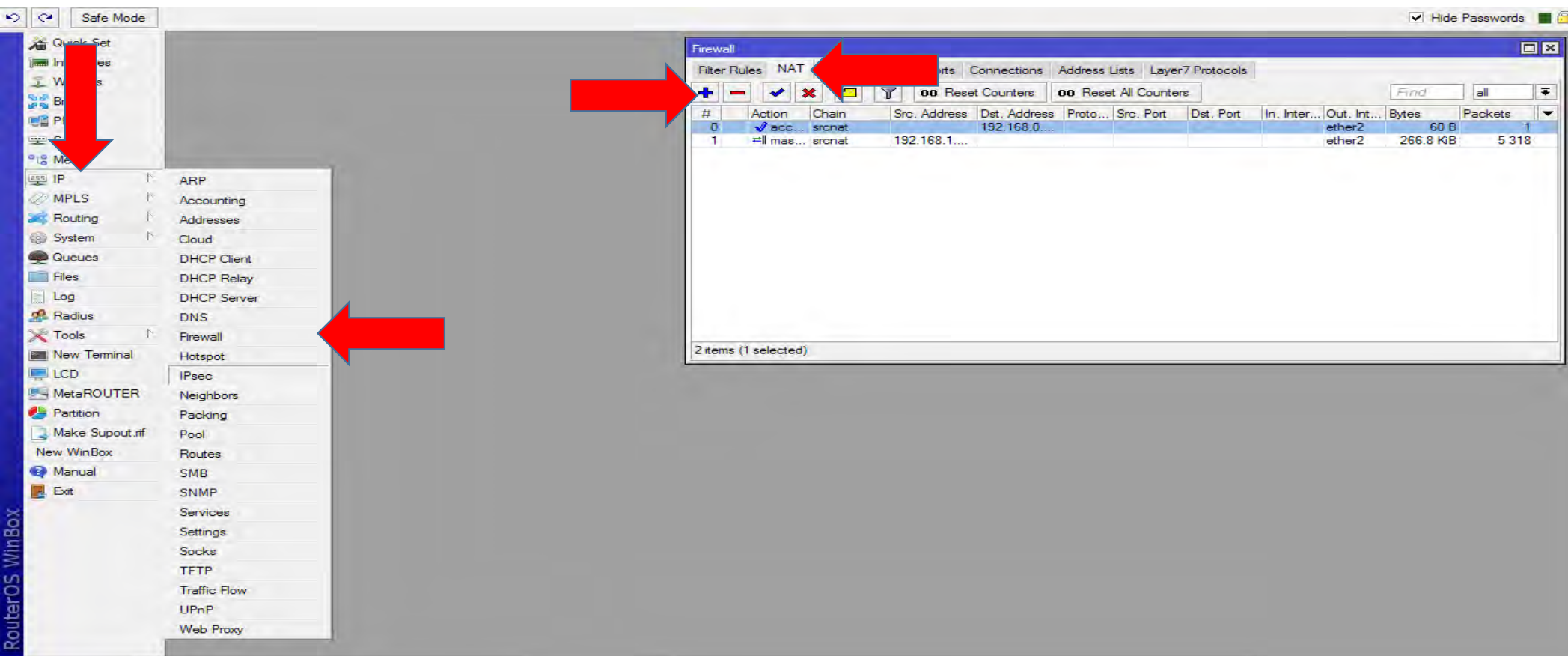
PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server



PPTP Mikrotik Client to Cisco Server

The screenshot displays the Mikrotik WinBox interface with the 'NAT Rule <192.168.0.0/24>' configuration window open. The 'General' tab is selected, showing the following settings:

- Chain: srcnat
- Src. Address: (empty)
- Dst. Address: 192.168.0.0/24
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: ether2
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Routing Table: (empty)
- Connection Type: (empty)

Four red arrows point to the following fields: Chain, Dst. Address, Out. Interface, and the 'srcnat' button. The 'enabled' checkbox is checked at the bottom.

In the background, the 'Filter Rules' window is visible, showing a table with the following data:

Port	In. Inter...	Out. Inter...	Bytes	Packets
	ether2	ether2	60 B	1
	ether2	ether2	268.3 KiB	5 347

PPTP Mikrotik Client to Cisco Server

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with various system configuration options. The main window shows the 'NAT Rule' configuration dialog box, which is currently on the 'General' tab. A red arrow points to the 'Action' dropdown menu, which is set to 'accept'. Another red arrow points to the 'Log' checkbox, which is unchecked. The 'Log Prefix' field is empty. The 'Statistics' tab is also visible. In the background, a table shows network statistics for 'ether2'.

RouterOS WinBox

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.rf
New WinBox
Manual
Exit

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

NAT Rule 193.168.8.8

General Action Statistics

Action: **accept**

☐ Log

Log Prefix:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Port	In. Inter...	Out. Int...	Bytes	Packets
		ether2	60 B	1
		ether2	269.7 KB	5 375

enabled

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`

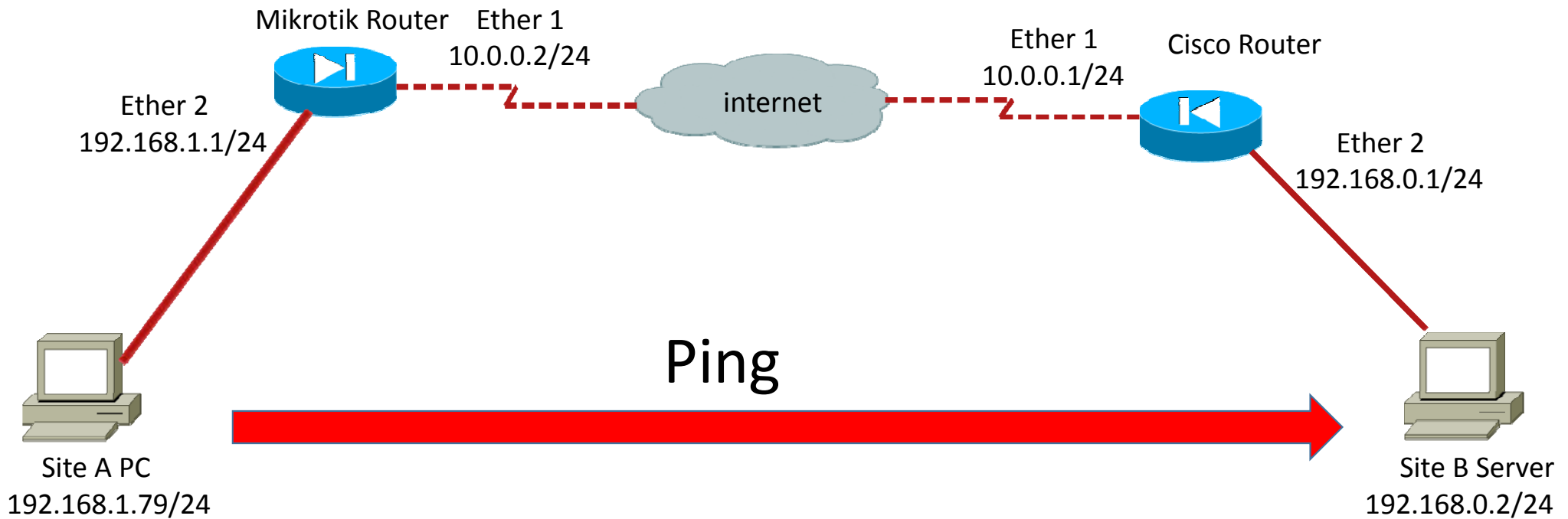
PPTP Mikrotik Client to Cisco Server

- 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
-

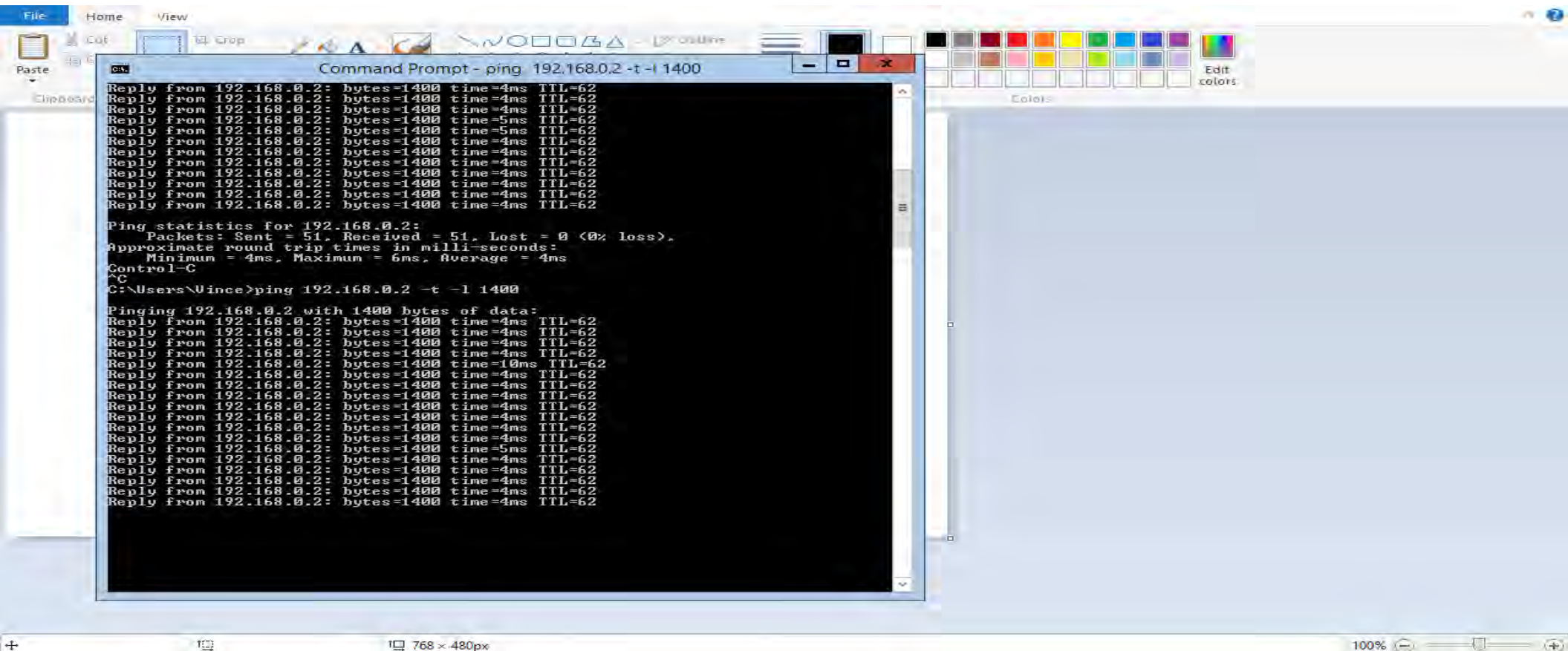
PPTP Mikrotik Client to Cisco Server

- 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



The screenshot shows a Windows desktop with a Command Prompt window open. The window title is "Command Prompt - ping 192.168.0.2 -t -l 1400". The Command Prompt displays the results of a continuous ping command to the IP address 192.168.0.2. The output shows 14 successful replies, each with 1400 bytes, a time of 4ms, and a TTL of 62. Below the replies, the ping statistics are shown: Packets: Sent = 51, Received = 51, Lost = 0 (0% loss), and approximate round trip times in milliseconds: Minimum = 4ms, Maximum = 6ms, Average = 4ms. The Command Prompt is running in a window titled "C:\Users\Vince>ping 192.168.0.2 -t -l 1400". The background of the desktop is a light blue gradient. To the right of the Command Prompt, there is a color palette with various color swatches and an "Edit colors" button. The bottom of the screen shows a taskbar with a search icon, a clock showing 7:00, and a system tray with a volume icon and a 100% zoom level.

```
File Home View
Cut Copy Paste
Clipboard
Command Prompt - ping 192.168.0.2 -t -l 1400
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=5ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Ping statistics for 192.168.0.2:
    Packets: Sent = 51, Received = 51, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 6ms, Average = 4ms
Control-C
^C
C:\Users\Vince>ping 192.168.0.2 -t -l 1400
Pinging 192.168.0.2 with 1400 bytes of data:
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=10ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=5ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
Reply from 192.168.0.2: bytes=1400 time=4ms TTL=62
768 x 480px
100%
```

PPTP Mikrotik Client to Cisco Server

The screenshot displays the Mikrotik WinBox interface with the following components:

- Left Sidebar:** Contains navigation icons for Quick Set, Interfaces, Wireless, Bridge, PPP, Switch, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, LCD, MetaROUTER, Partition, Make Supout.rif, New WinBox, Manual, and Exit.
- Main Window:**
 - Routes Table:** Shows 4 items with columns: Dst. Address, Gateway, Distance, Routing Mark, Pref. Source. The entries are:

Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS 0.0.0.0/0	10.0.0.1 reachable ether2	1		
DAC 10.0.0.0/24	ether2 reachable	0		10.0.0.2
DAC 192.168.1.0/24	ether3 reachable	0		192.168.1.1
DAC 192.168.79.1	pptp-out1 reachable	0		192.168.79.2
 - Address List Window:** Shows 3 items with columns: Address, Network, Interface. The entries are:

Address	Network	Interface
10.0.0.2/24	10.0.0.0	ether2
192.168.1.1/24	192.168.1.0	ether3
192.168.79.2	192.168.79.1	pptp-out1
 - PPP Configuration Window:** Shows 1 item out of 12 with columns: Name, Type, L2 MTU, Tx, Rx, Tx Packet (p/s), Rx Packet (p/s). The entry is:

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
pptp-out1	PPTP Client		0 bps	0 bps	0	0

PPTP Mikrotik Client to Cisco Server

RouterOS WinBox

Safe Mode

Hide Passwords

Router List

Routes

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.0.0.1 reachable ether2	1		
DAC	10.0.0.0/24	ether2 reachable	0		10.0.0.2
DAC	192.168.1.0/24	ether3 reachable	0		192.168.1.1

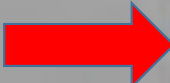
3 items

PPP

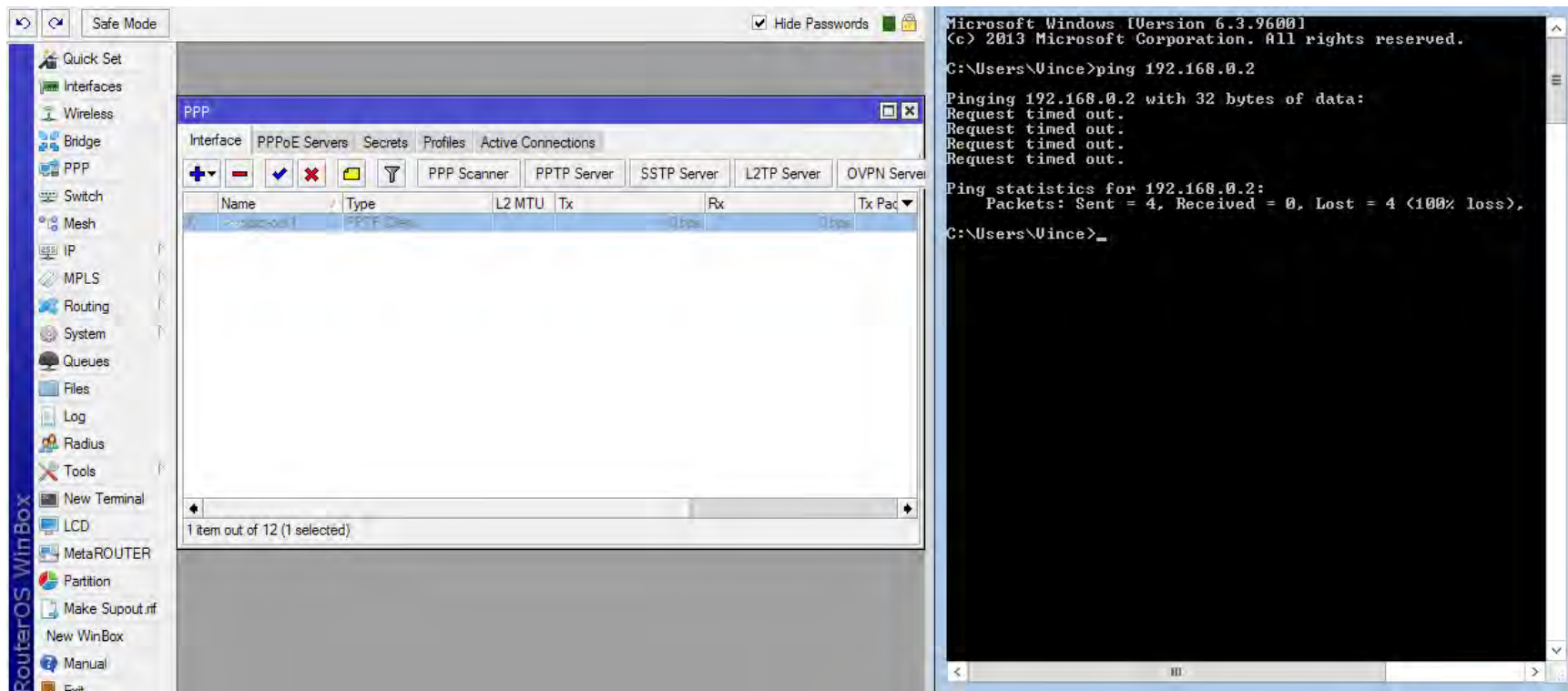
Interface

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
ppp-201	PPTP Client					

1 item out of 12 (1 selected)



PPTP Mikrotik Client to Cisco Server



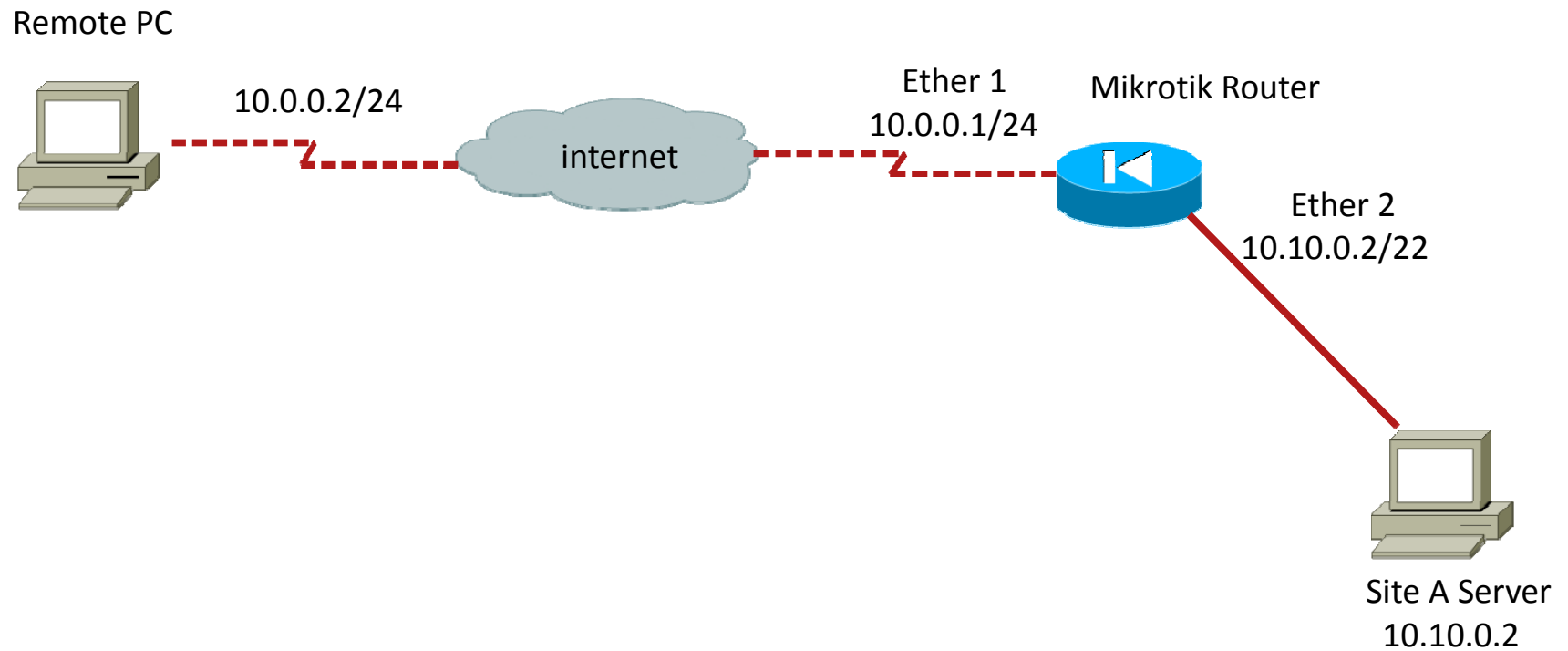
PPTP Mikrotik Client to Cisco Server

- /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

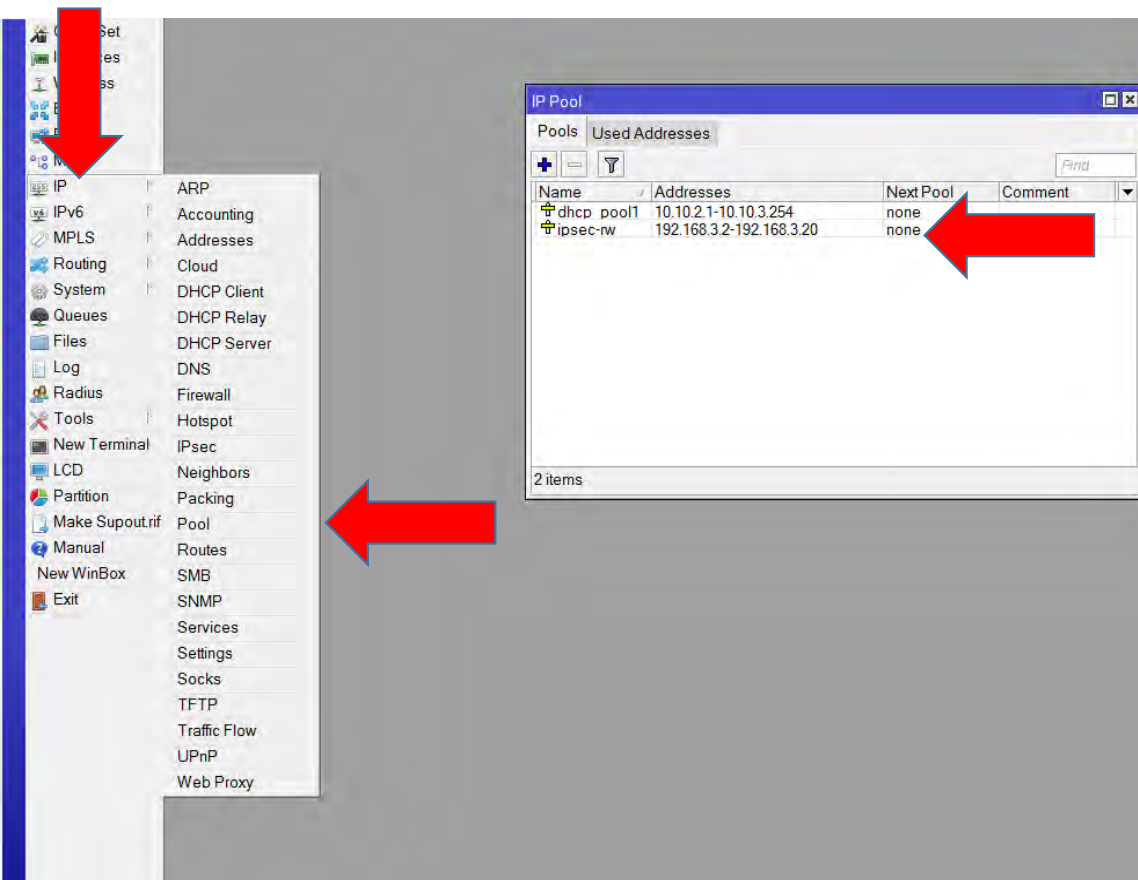
IPSEC Shrew Client To Mikrotik



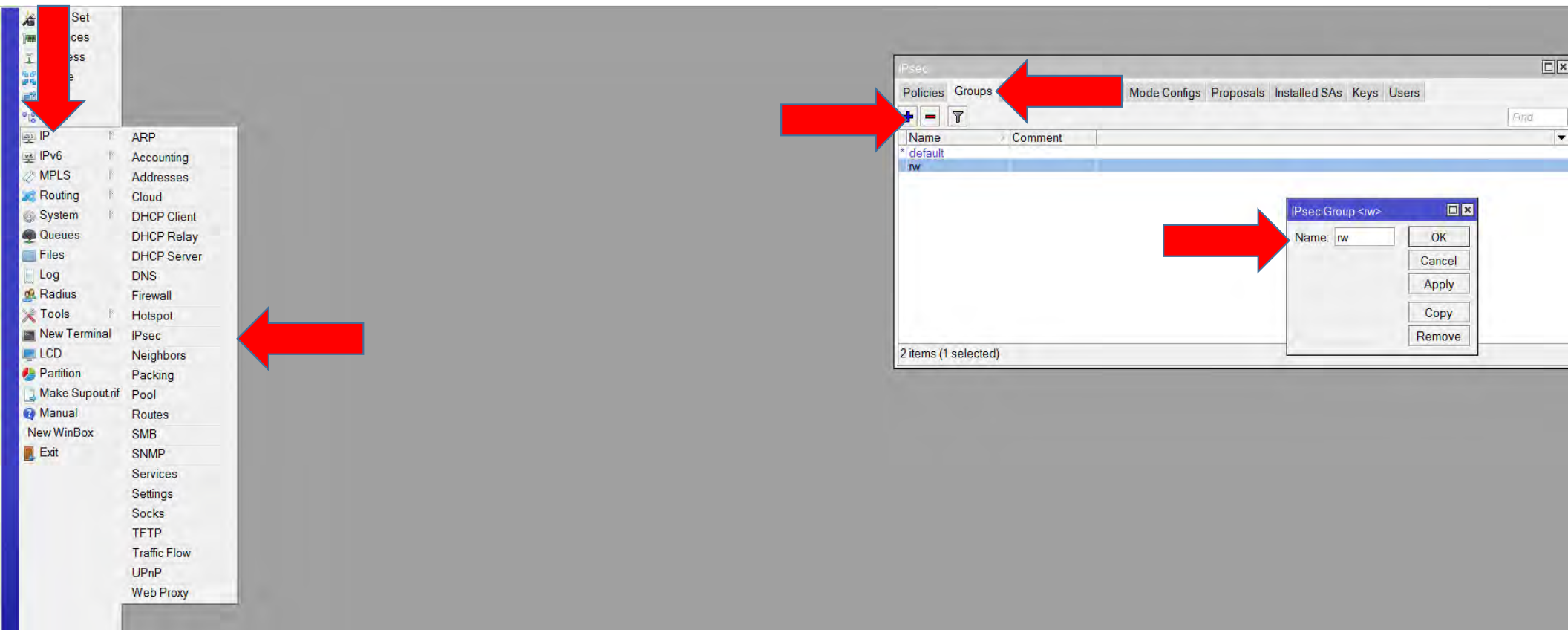
IPSEC Shrew Client To Mikrotik

- www.shrew.net/download/vpn

IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with various configuration options. The main window displays the 'IPsec' configuration page, specifically the 'Policies' tab. A table lists four IPsec policies. The first policy is selected, and its configuration details are shown in a pop-up window on the right. Red arrows highlight the transition from the table to the configuration window and the specific fields within it.

	Src. Addr...	Src. ...	Dst. Address	Dst. ...	Protocol	Action	Level	Tun...	Comment
T	10.10.0.0/22		192.168.3.0/24		255 (all)	encrypt require	no		
T	192.168.3.0/24		10.10.0.0/22		255 (all)	encrypt require	no		
D	192.168.3.20		10.10.0.0/22		255 (all)	encrypt require	yes		
*T	::/0		::/0		255 (all)	encrypt require	no		

4 items (1 selected)

IPsec Policy <10.10.0.0/22.0->192.168.3.0/24.0>

General Action

Src. Address: 10.10.0.0/22

Src. Port: [dropdown]

Dst. Address: 192.168.3.0/24

Dst. Port: [dropdown]

Protocol: 255 (all)

☒ Template

Group: nw

OK Cancel Apply Disable Comment Copy Remove

IPSEC Shrew Client To Mikrotik

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with various system tools. The main window shows the 'IPsec' configuration tab, specifically the 'Policies' sub-tab. A table lists four IPsec policies. A red arrow points from the first policy row to a detailed configuration dialog box for that policy.

IPsec Policies Table:

	Src. Addr...	Src...	Dst Address	Dst...	Protocol	Action	Level	Tun...	Comment
T	10.10.0.0/22		192.168.3.0/24		255 (all)	encrypt	require	no	
T	192.168.3.0/24		10.10.0.0/22		255 (all)	encrypt	require	no	
D	192.168.3.0/24		10.10.0.0/22		255 (all)	encrypt	require	yes	
*T	10.10.0.0/22		10.10.0.0/22		255 (all)	encrypt	require	no	

IPsec Policy Configuration Dialog:

IPsec Policy: 10.10.0.0/22.0->192.168.3.0/24.0

General | Action

Action: encrypt

Level: require

IPsec Protocols: esp

☐ Tunnel

SA Src. Address: 0.0.0.0

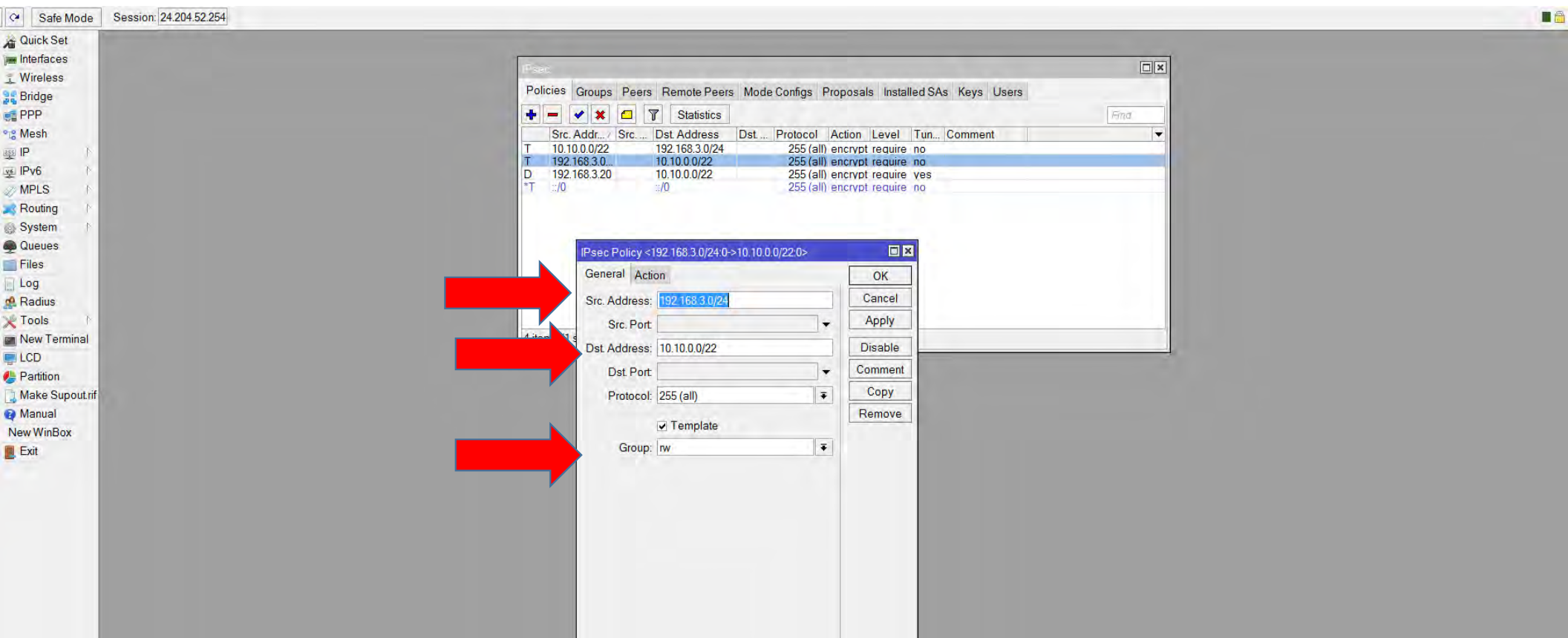
SA Dst. Address: 0.0.0.0

Proposal: default

Priority: 0

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik

The screenshot displays the Mikrotik WinBox interface with the IPsec Peer configuration window open. The left sidebar shows the navigation menu with options like Quick Set, Interfaces, Wireless, Bridge, PPP, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, LCD, Partition, Make Supout.rif, Manual, New WinBox, and Exit.

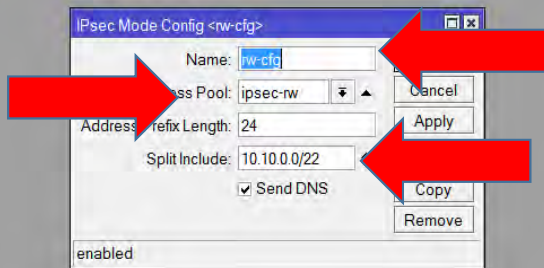
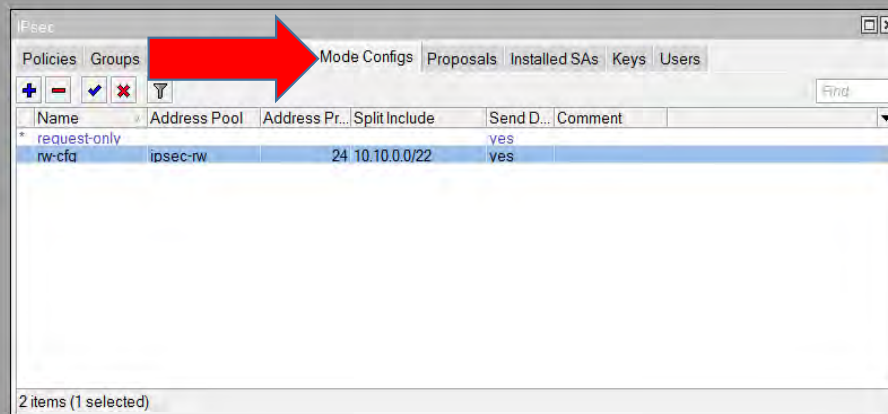
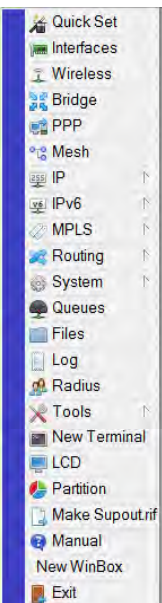
The IPsec Peer configuration window is titled "IPsec Peer <0.0.0.0/0>". It contains the following fields and settings:

- Address:** 0.0.0.0/0
- Port:** 500
- Local Address:** (empty)
- Method:** pre shared key
- Passive:** ☒
- Secret:** 1234
- Policy Template Group:** nw
- Exchange Mode:** main
- Send Initial Contact:** ☒
- NAT Traversal:** ☒
- My ID:** auto
- Proposal Check:** exact
- Hash Algorithm:** sha1
- Encryption Algorithm:** ☐ des ☐ 3des ☒ aes-128 ☐ aes-192 ☐ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256
- Mode Configuration:** nw-cfg
- DH Group:** modp1024
- Generate Policy:** port strict
- Lifetime:** 1d 00:00:00
- Lifebytes:** (empty)
- DPD Interval:** 120 s
- DPD Maximum Failures:** 5

Red arrows indicate the following fields are highlighted or pointed to:

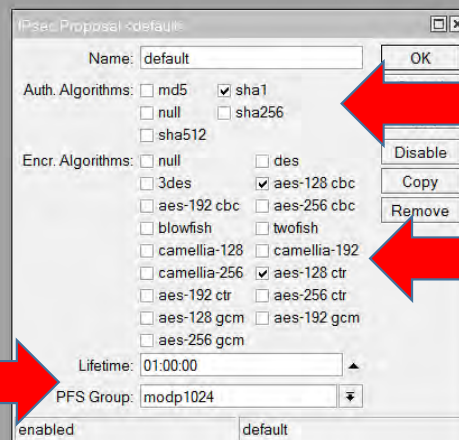
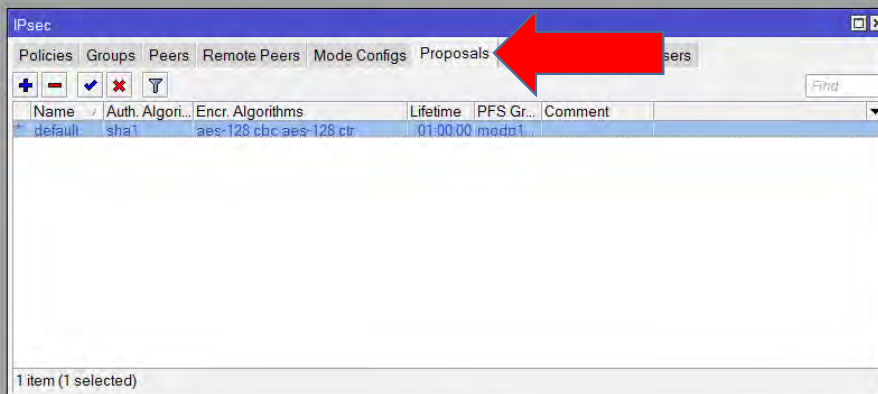
- Address
- Port
- Local Address
- Method
- Secret
- Policy Template Group
- Exchange Mode
- Proposal Check
- Hash Algorithm
- Encryption Algorithm
- Mode Configuration
- DH Group
- Generate Policy
- Lifetime
- Lifebytes
- DPD Interval
- DPD Maximum Failures

IPSEC Shrew Client To Mikrotik

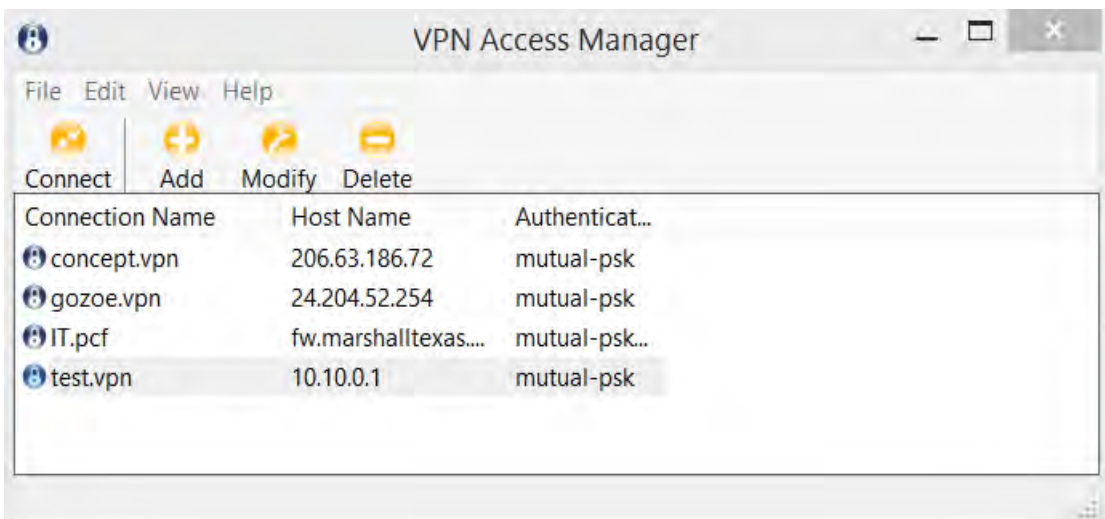


IPSEC Shrew Client To Mikrotik

Quick Set
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
Partition
Make Supout.rif
Manual
New WinBox
Exit



IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik

The image displays three sequential screenshots of the 'VPN Site Configuration' window, showing different tabs in the configuration interface.

First Screenshot (General Tab):

- Remote Host:**
 - Host Name or IP Address: 10.10.0.1
 - Port: 500
 - Auto Configuration: ike config pull
- Local Host:**
 - Adapter Mode: Use a virtual adapter and assigned address
 - MTU: 1380
 - Obtain Automatically: ☒
 - Address: . . .
 - Netmask: . . .

Second Screenshot (Firewall Options Tab):

- Firewall Options:**
 - NAT Traversal: disable
 - NAT Traversal Port: 4500
 - Keep-alive packet rate: 15 Secs
 - IKE Fragmentation: disable
 - Maximum packet size: 540 Bytes
- Other Options:**
 - ☐ Enable Dead Peer Detection
 - ☐ Enable ISAKMP Failure Notifications
 - ☐ Enable Client Login Banner

Third Screenshot (DNS/WINS Tab):

- DNS:**
 - ☐ Enable DNS
 - Obtain Automatically: ☐
 - Server Address #1: . . .
 - Server Address #2: . . .
 - Server Address #3: . . .
 - Server Address #4: . . .
 - DNS Suffix: . . .

IPSEC Shrew Client To Mikrotik

VPN Site Configuration

General Client Name Resolution Authentication P

DNS WINS

☐ Enable WINS ☒ Obtain Automatically

Server Address #1

Server Address #2

Save Cancel

VPN Site Configuration

General Client Name Resolution Authentication P

Authentication Method Mutual PSK

Local Identity Remote Identity Credentials

Identification Type IP Address

Address String

☒ Use a discovered local host address

Save Cancel

VPN Site Configuration

General Client Name Resolution Authentication P

Authentication Method Mutual PSK

Local Identity Remote Identity Credentials

Identification Type IP Address

Address String

☒ Use a discovered remote host address

Save Cancel

IPSEC Shrew Client To Mikrotik

VPN Site Configuration

General Client Name Resolution Authentication P < >

Authentication Method: Mutual PSK

Local Identity Remote Identity Credentials

Server Certificate Authority File

Client Certificate File

Client Private Key File

Pre Shared Key

Save Cancel

VPN Site Configuration

Name Resolution Authentication Phase 1 Phase 2 < >

Proposal Parameters

Exchange Type: main

DH Exchange: group 2

Cipher Algorithm: aes

Cipher Key Length: 128 Bits

Hash Algorithm: sha1

Key Life Time limit: 86400 Secs

Key Life Data limit: 0 Kbytes

☐ Enable Check Point Compatible Vendor ID

Save Cancel

VPN Site Configuration

Name Resolution Authentication Phase 1 Phase 2 < >

Proposal Parameters

Transform Algorithm: esp-aes

Transform Key Length: 128 Bits

HMAC Algorithm: sha1

PFS Exchange: group 2

Compress Algorithm: disabled

Key Life Time limit: 3600 Secs

Key Life Data limit: 0 Kbytes

Save Cancel

IPSEC Shrew Client To Mikrotik

VPN Site Configuration

Authentication Phase 1 Phase 2 Policy

IPSEC Policy Configuration

Policy Generation Level require

☐ Maintain Persistent Security Associations

☐ Obtain Topology Automatically or Tunnel All

Remote Network Resource

↔ 10.10.0.0 / 255.255.252.0

Add Modify Delete

Save Cancel

Topology Entry

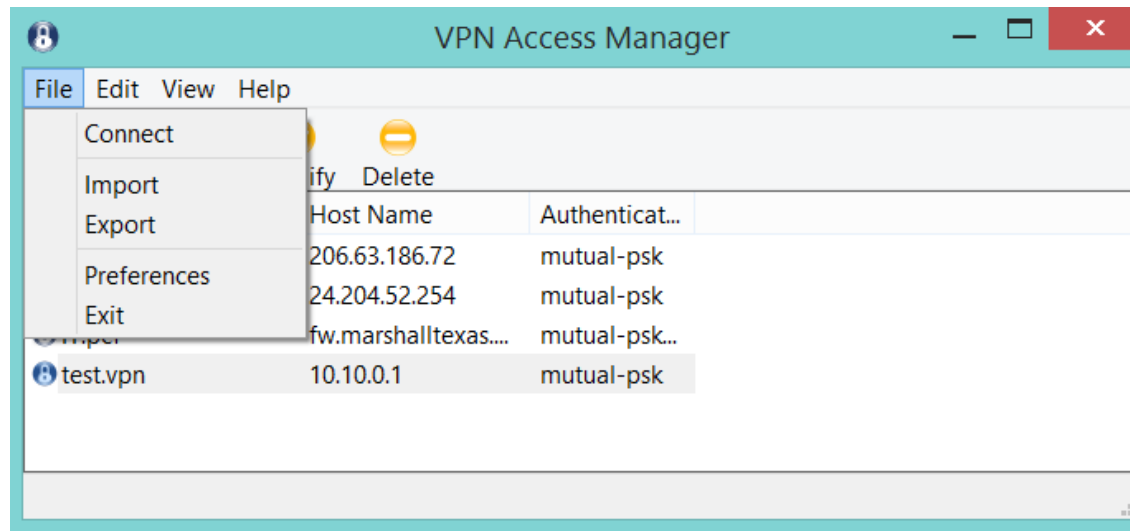
Type Include

Address 10 . 10 . 0 . 0

Netmask 255 . 255 . 252 .

Ok Cancel

IPSEC Shrew Client To Mikrotik



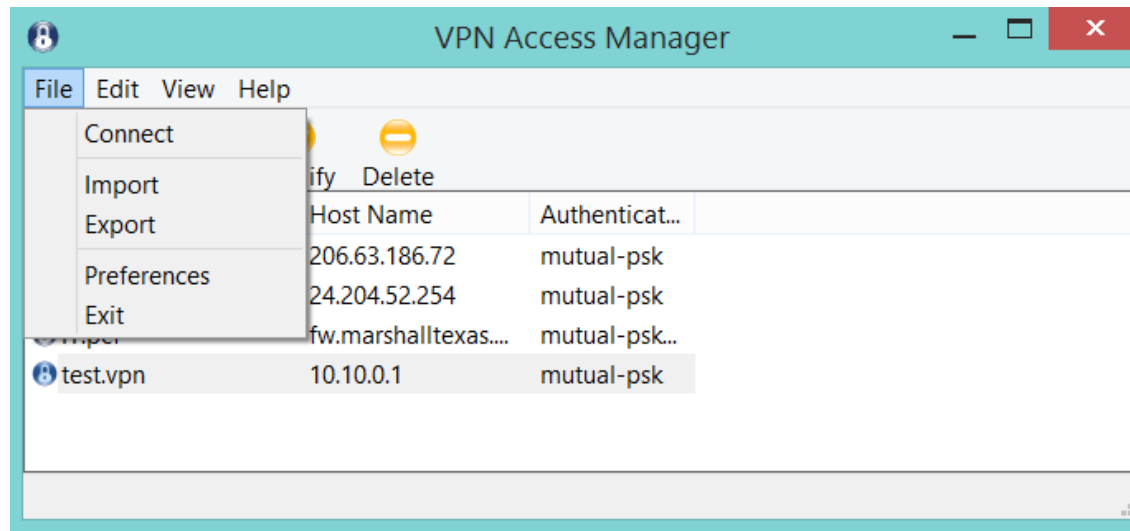
IPSEC Shrew Client To Mikrotik

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:0
n:client-wins-used:0
n:client-wins-auto:1
n:phase1-dhgroup:2
n:phase1-life-secs:86400

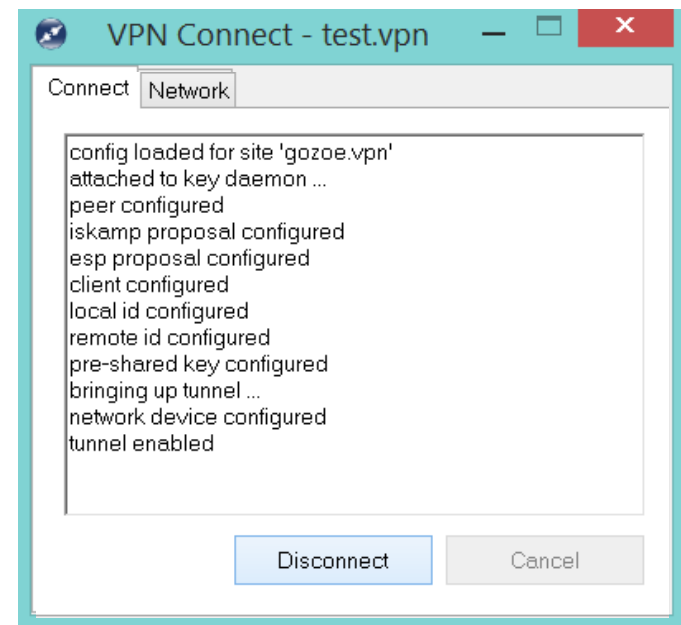
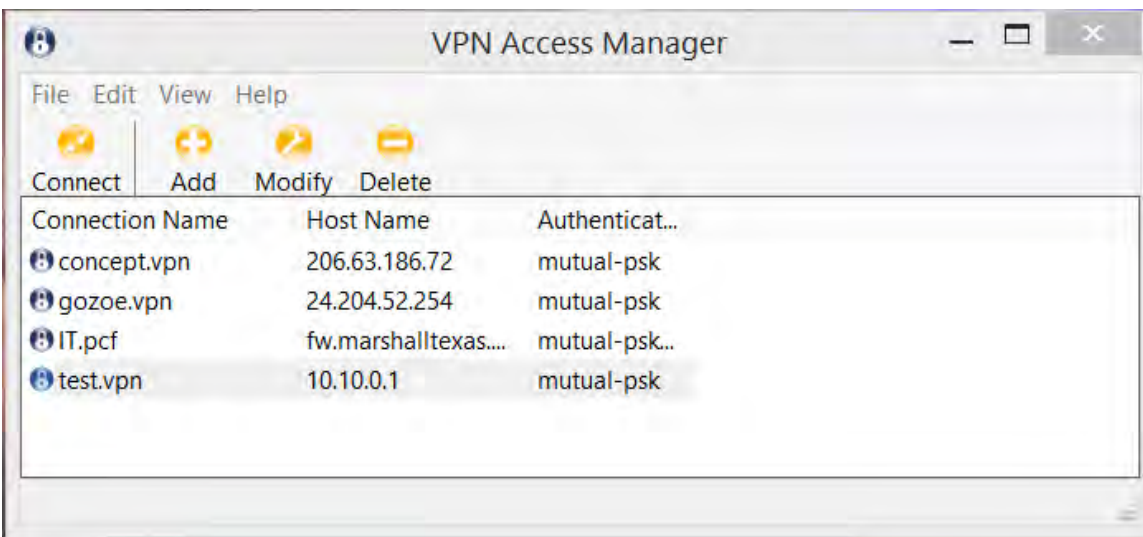
n:phase1-life-kbytes:0
n:vendor-chkpt-enable:0
n:phase2-life-secs:3600
n:phase2-life-kbytes:0
n:policy-nailed:0
n:policy-list-auto:0
n:phase1-keylen:128
n:phase2-keylen:128
s:network-host:10.10.0.1
s:client-auto-mode:pull
s:client-iface:virtual
s:network-natt-mode:disable
s:network-frag-mode:disable

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

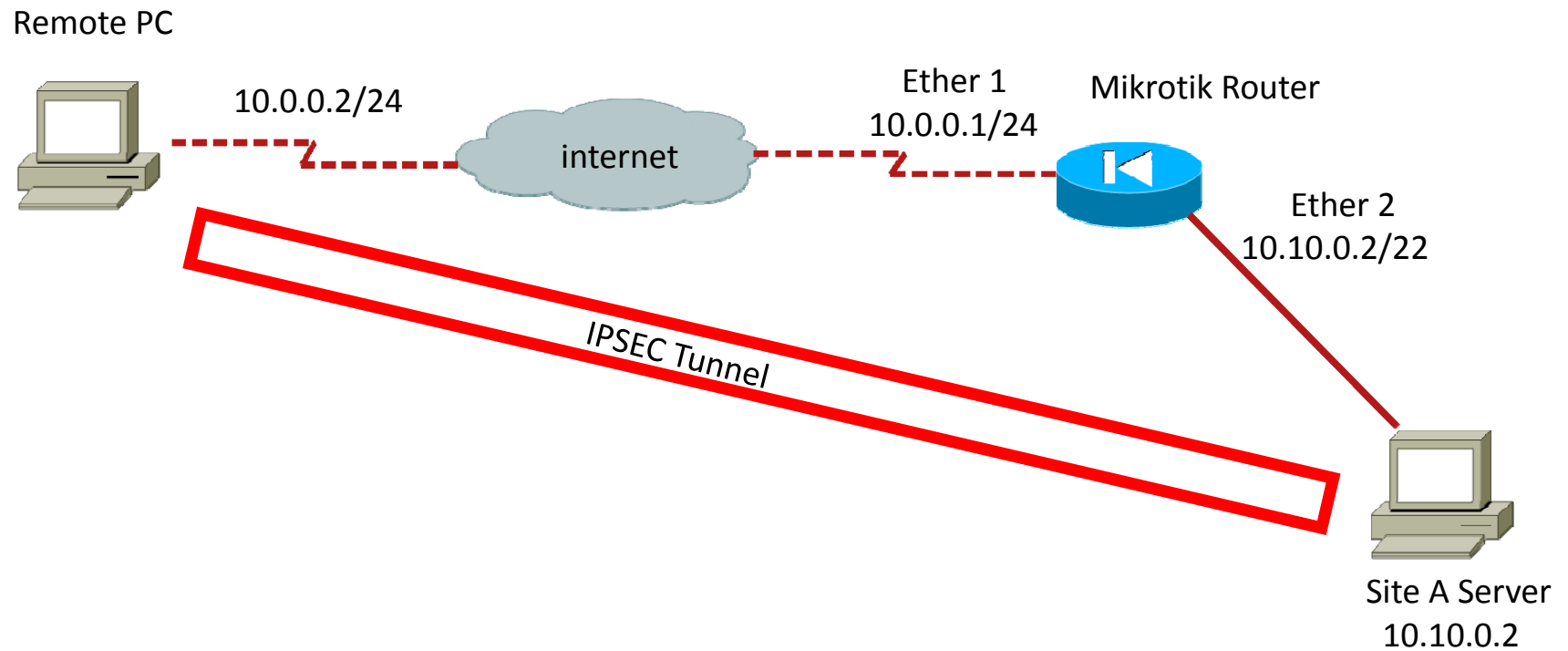
IPSEC Shrew Client To Mikrotik



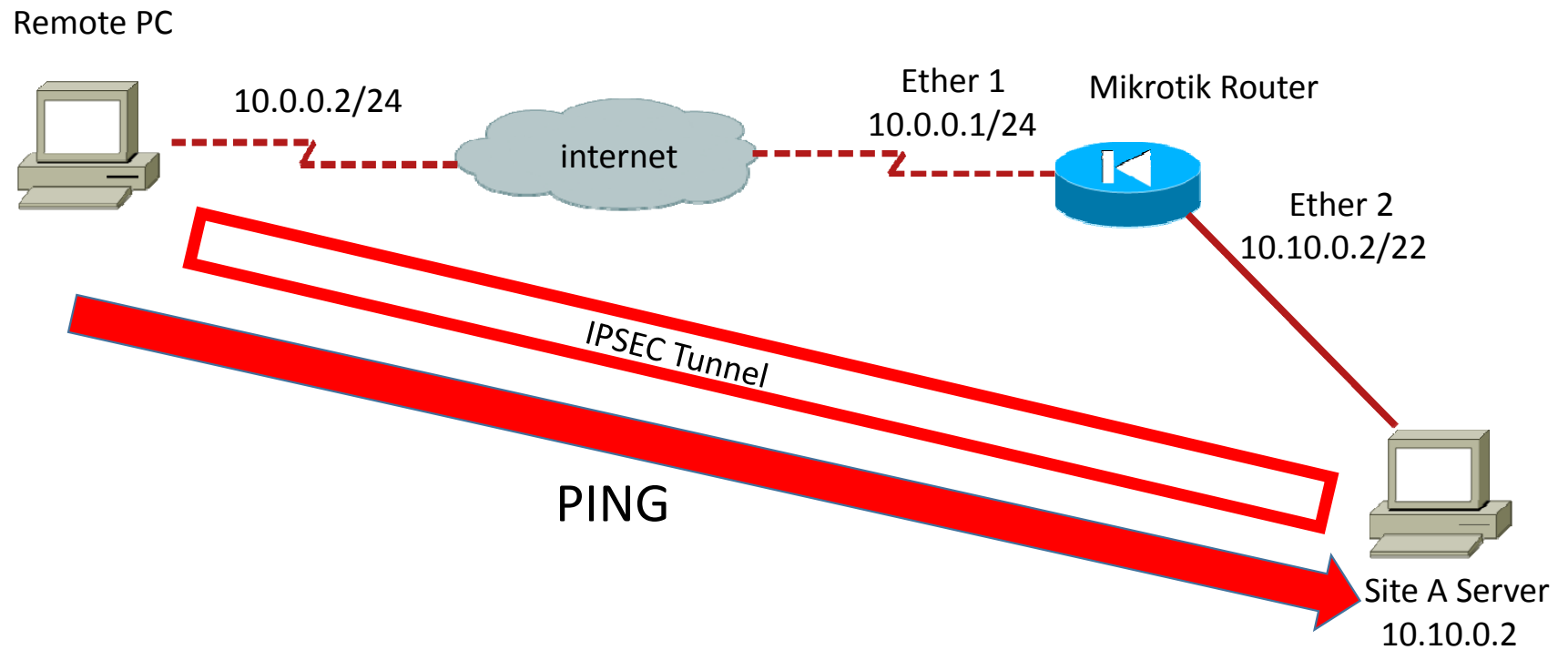
IPSEC Shrew Client To Mikrotik



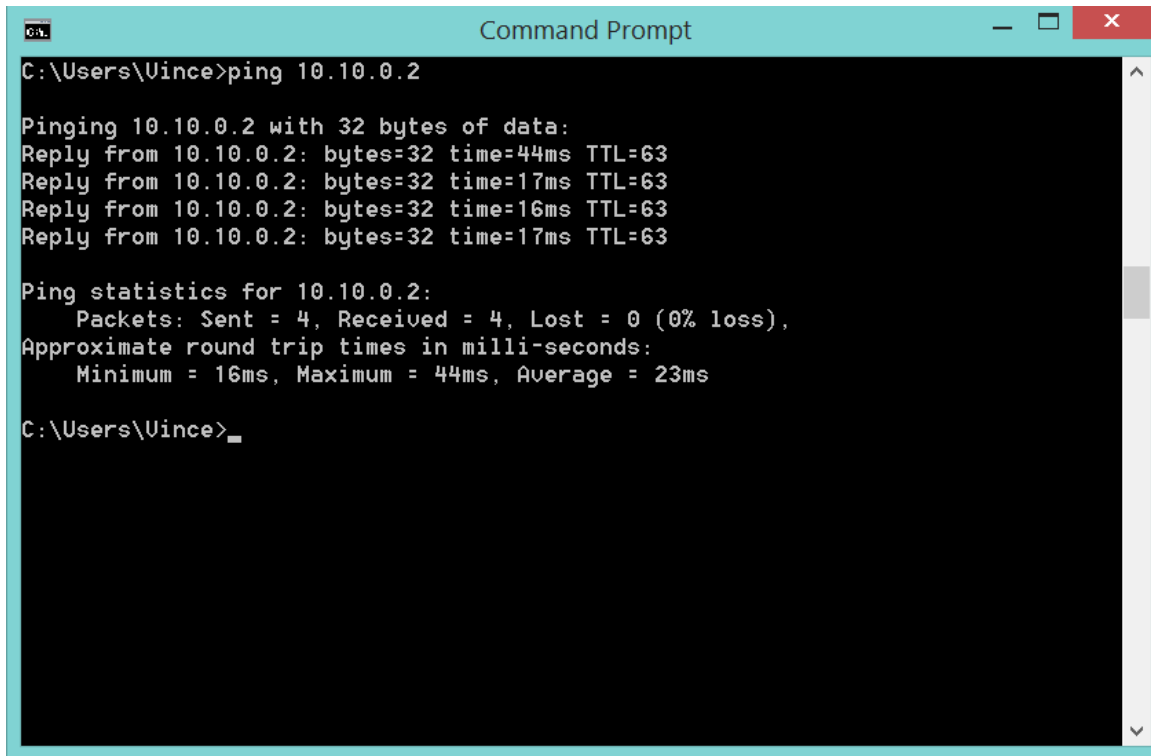
IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik



IPSEC Shrew Client To Mikrotik



```
Command Prompt
C:\Users\Vince>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:
Reply from 10.10.0.2: bytes=32 time=44ms TTL=63
Reply from 10.10.0.2: bytes=32 time=17ms TTL=63
Reply from 10.10.0.2: bytes=32 time=16ms TTL=63
Reply from 10.10.0.2: bytes=32 time=17ms TTL=63

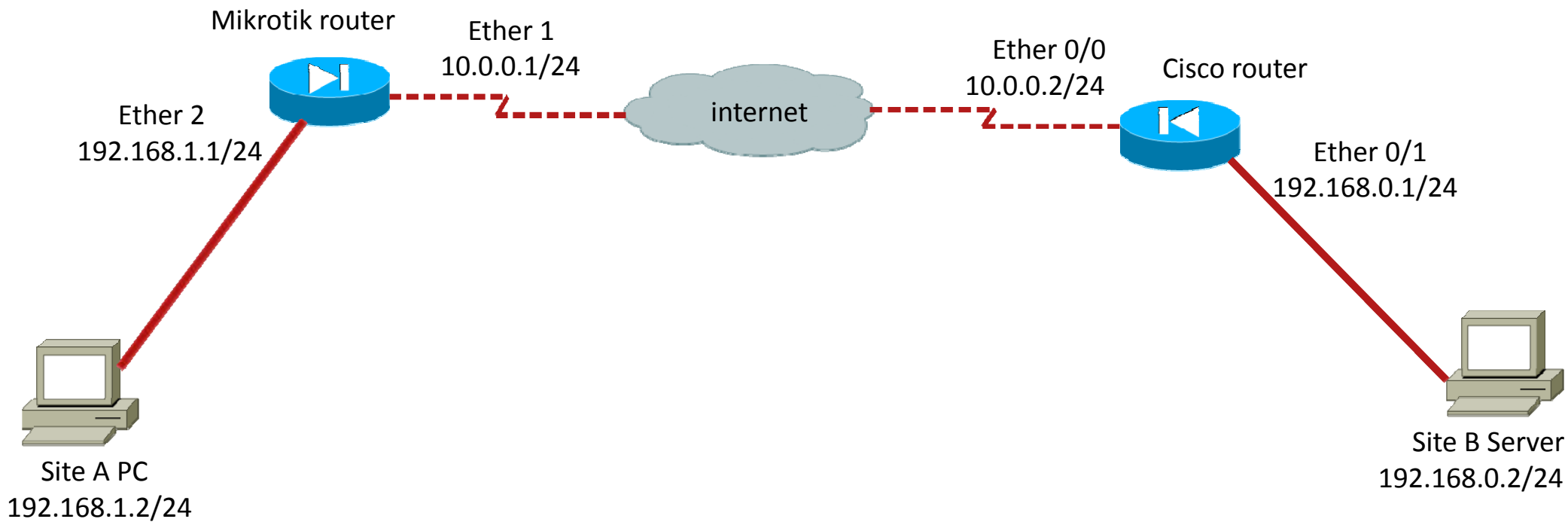
Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 44ms, Average = 23ms

C:\Users\Vince>
```

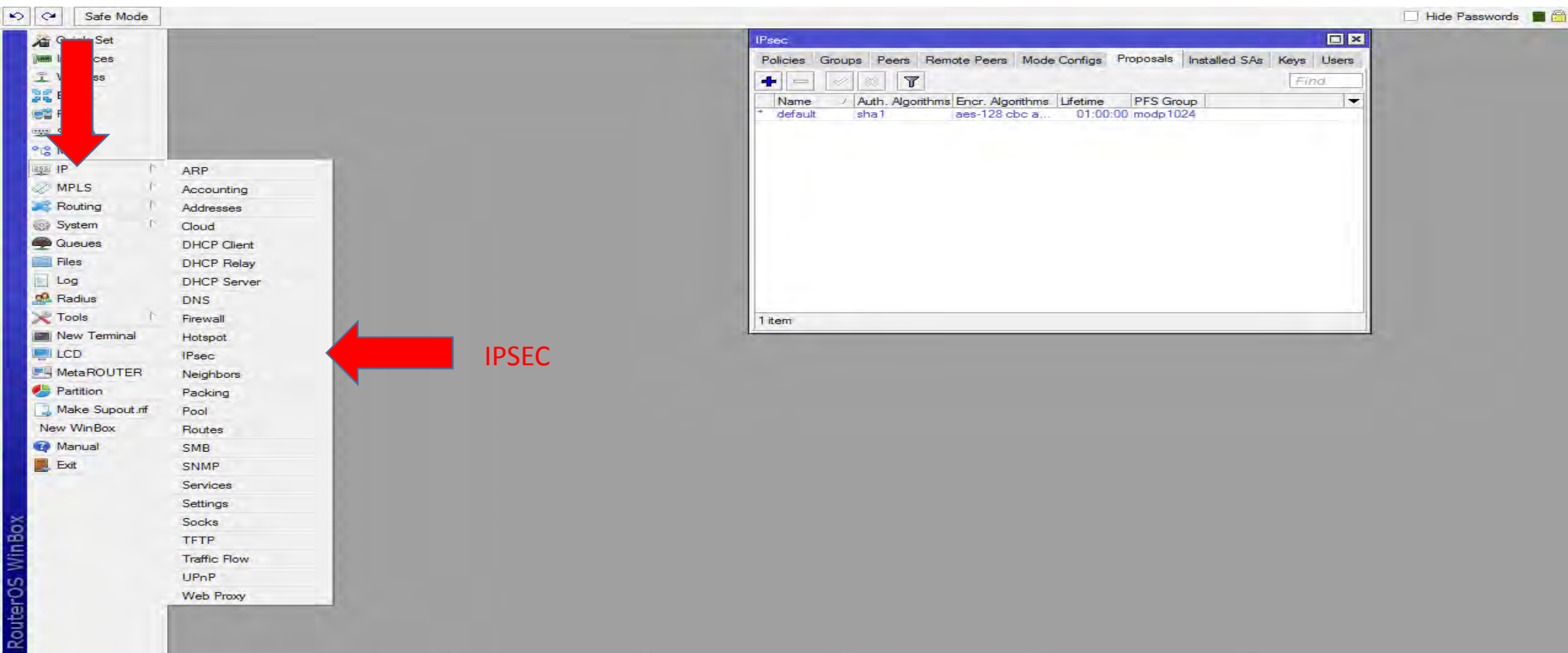
IPSEC Cisco IOS or ASA To Mikrotik

- 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

RouterOS WinBox

Safe Mode

Quick Set

IPsec

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users

Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
192.168.1.0/24		192.168.0.0/24		255 (...)	encrypt	require	yes
:::0		:::0		255 (...)	encrypt	require	no

2 items (1 selected)

IPsec Policy <192.168.1.0/24->192.168.0.0/24:0>

General Action

Src. Address: 192.168.1.0/24

Src. Port: [dropdown]

Dst. Address: 192.168.0.0/24

Dst. Port: [dropdown]

Protocol: 255 (all)

☐ Template

OK Apply Comment Copy Remove

enabled

Local lan subnet

Remote lan subnet

IPSEC Cisco IOS To Mikrotik

2 items (1 selected)

	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
1	192.168.1.0/24		192.168.0.0/24		255 (...)	encrypt	require	yes
2	::/0		::/0		255 (...)	encrypt	require	no

IPsec Policy <192.168.1.0/24:0>192.168.0.0/24:0>

General Action

Action: encrypt

Level: require

Protocols: esp

☒ Tunnel

SA Src. Address: 10.0.0.2

SA Dst. Address: 10.0.0.1

Proposal: default

Priority: 0

enabled

OK Cancel Apply Disable

Local wan address

Remote wan address

IPSEC Cisco IOS To Mikrotik

The screenshot shows the Mikrotik WinBox interface with the IPsec Peer configuration window open for the peer 10.0.0.1. The left sidebar shows the RouterOS WinBox menu. The main window displays the IPsec Peer configuration for 10.0.0.1. Red arrows point to the following fields:

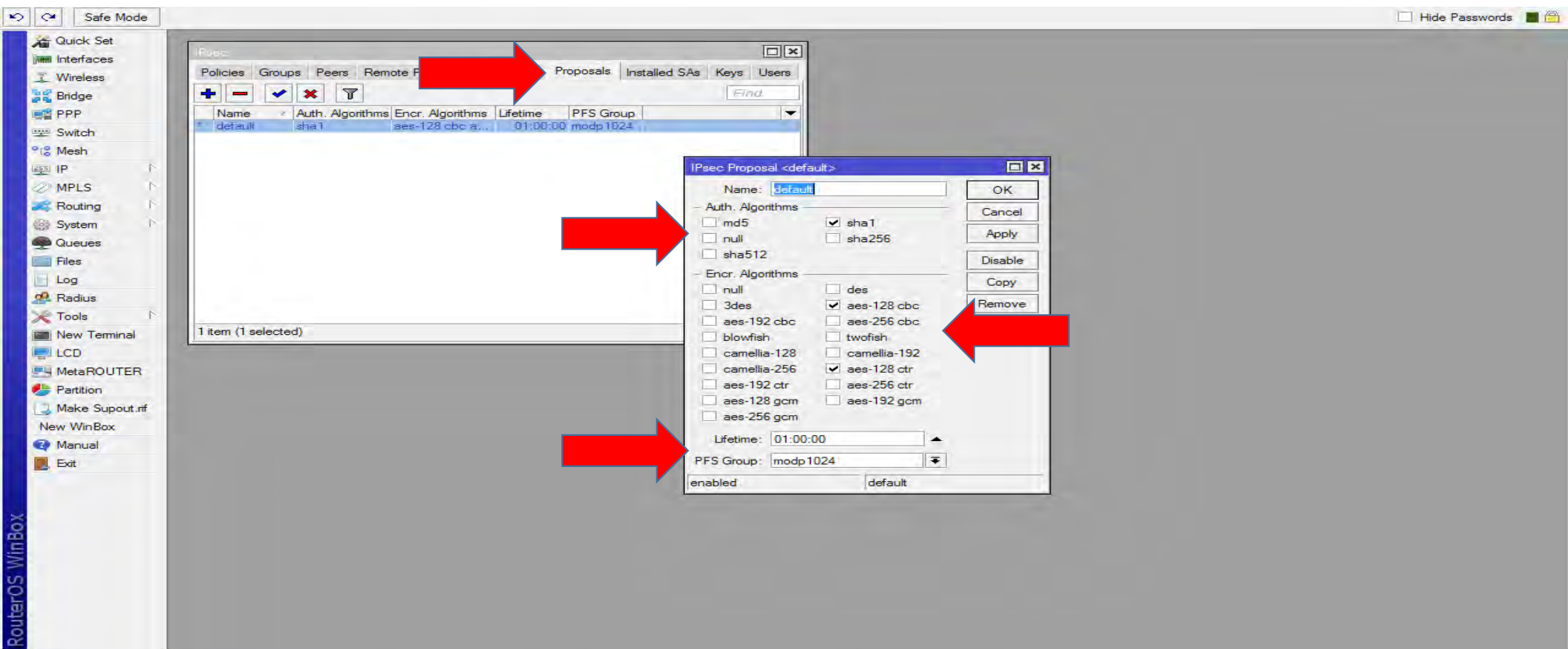
- Address: 10.0.0.1
- Port: 500
- Method: pre shared key
- Secret: 1234
- Policy Template Group: default
- Change Mode: main
- Send Initial Contact: ☒ Send Initial Contact
- NAT Traversal: ☐ NAT Traversal
- My ID: auto
- Proposal Check: obey
- Hash Algorithm: sha1
- Encryption Algorithm: aes-128
- DH Group: modp1024
- Generate Policy: no
- Lifetime: 1d 00:00:00
- DPD Interval: 120 s
- DPD Maximum Failures: 5

Buttons on the right include: OK, Cancel, Apply, Disable, Comment, and Remove.

Annotations on the right side of the image:

- Remote wan address (pointing to the Address field)
- PRE SHARED PASSWORD (pointing to the Secret field)

IPSEC Cisco IOS To Mikrotik



IPSEC Cisco IOS To Mikrotik

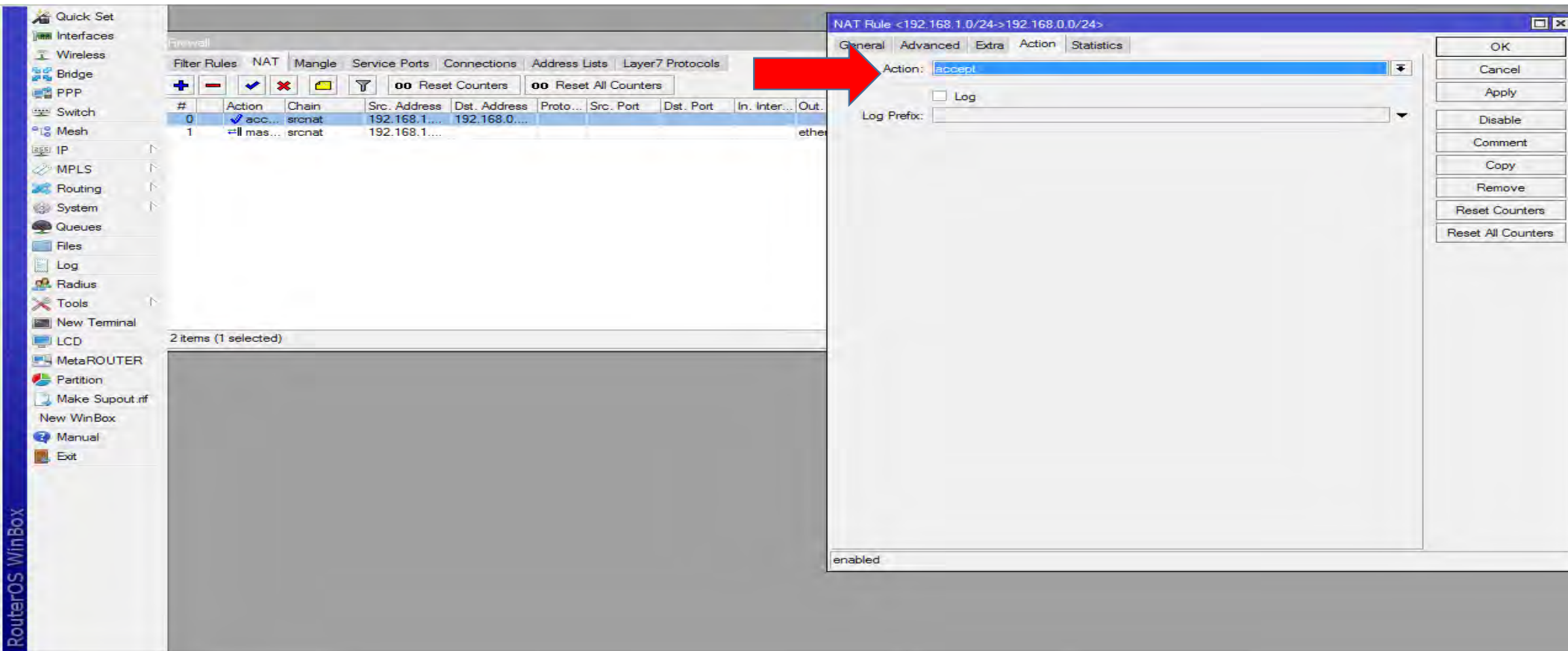
The screenshot displays the Mikrotik WinBox interface. On the left, a sidebar lists various configuration options: Quick Set, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, LCD, MetaROUTER, Partition, Make Supout.rf, New WinBox, Manual, and Exit. The main window shows the 'NAT' tab under the 'Filter Rules' section. A table lists two NAT rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out...
0	✓ acc...	srcnat	192.168.1...	192.168.0...					
1	≡ll mas...	srcnat	192.168.1...						

Two red arrows point from the table to the 'NAT Rule <192.168.1.0/24>192.168.0.0/24>' configuration window. The first arrow points to the 'Chain' field, which is set to 'srcnat'. The second arrow points to the 'Src. Address' field, which is set to '192.168.1.0/24'. The 'Dst. Address' field is set to '192.168.0.0/24'. The 'Protocol' field is set to 'IPsec'. The 'In. Interface' and 'Out. Interface' fields are empty. The 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', and 'Connection Type' fields are also empty. The 'enabled' checkbox is checked.

RouterOS WinBox

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

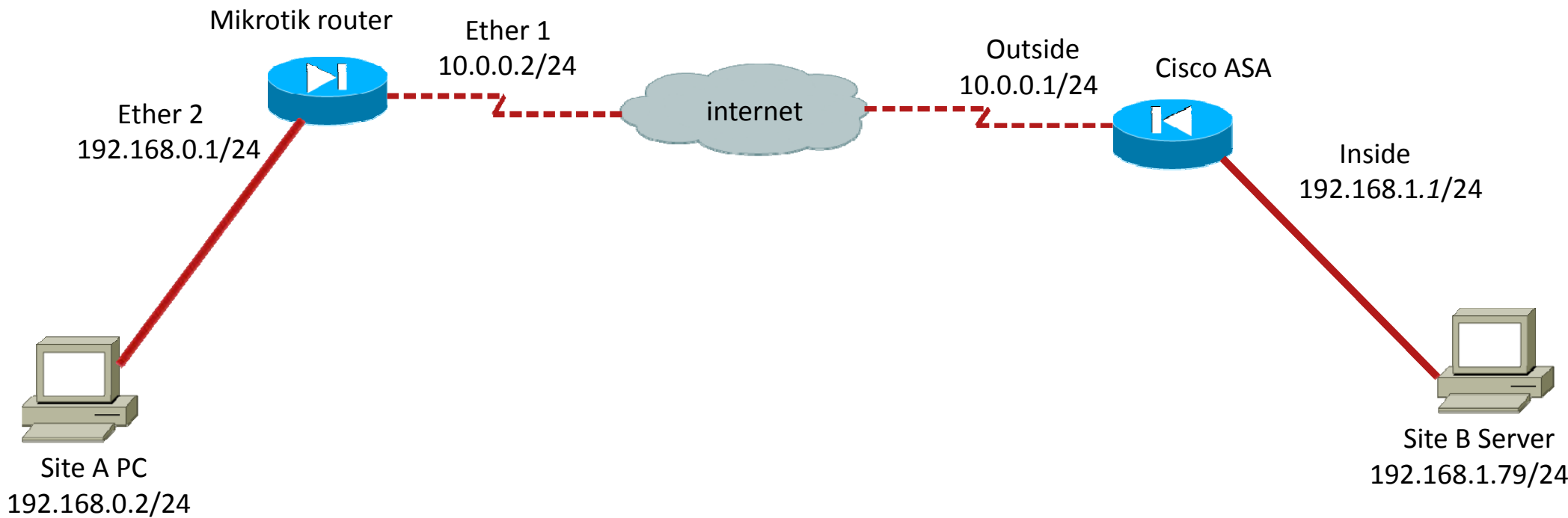
IPSEC Cisco IOS To Mikrotik

```
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

The screenshot shows the Mikrotik WinBox interface. On the left, the 'IPsec' option is highlighted in the sidebar menu, indicated by a red arrow. The main window displays the 'IPsec' configuration page, also indicated by a red arrow. The 'Policies' tab is active, showing a table with two entries:

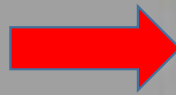
	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
	192.168.0.0/24		192.168.1.0/24		255 (...)	encrypt	require	yes
*T	::/0		::/0		255 (...)	encrypt	require	no

The status bar at the bottom of the window indicates '2 items'.

IPSEC Cisco ASA To Mikrotik

Local lan subnet

Remote lan subnet



IPsec Policy <192.168.0.0/24>192.168.1.0/24>

General	Action
Src. Address: 192.168.0.0/24	
Src. Port: [dropdown]	
Dst. Address: 192.168.1.0/24	
Dst. Port: [dropdown]	
Protocol: 255 (all)	
<input type="checkbox"/> Template	

enabled [] Temp[]

IPsec									
Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users									
+ - [check] [x] [icon] [filter] Statistics Find									
Src. Address /	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel		
192.168.0.0/24		192.168.1.0/24		255 (...)	encrypt	require	yes		
				255 (...)	encrypt	require	no		

IPSEC Cisco ASA To Mikrotik

Source Wan Address

Remote Wan Address

IPsec Policy 192.168.0.0/24->192.168.1.0/24

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

☒ Tunnel

SA Src. Address: 10.0.0.2

SA Dst. Address: 10.0.0.1

Proposal: default

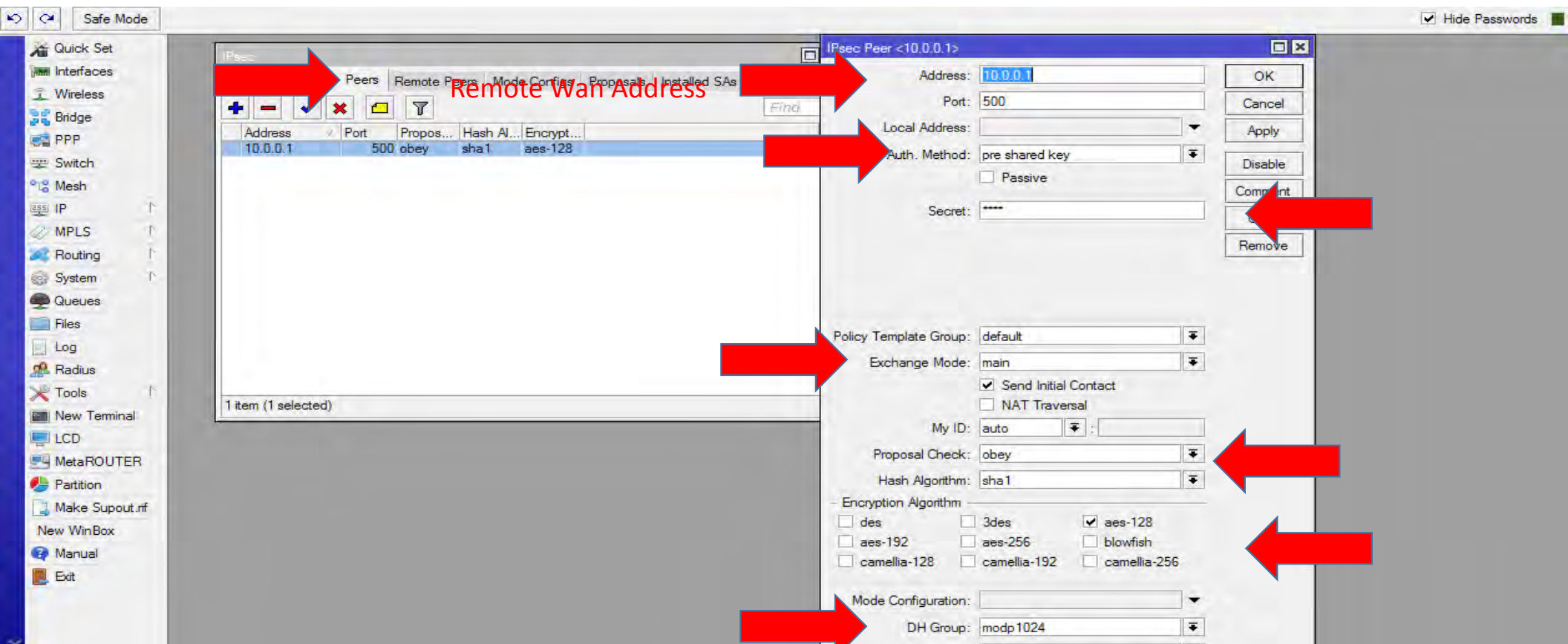
Priority: 0

enabled

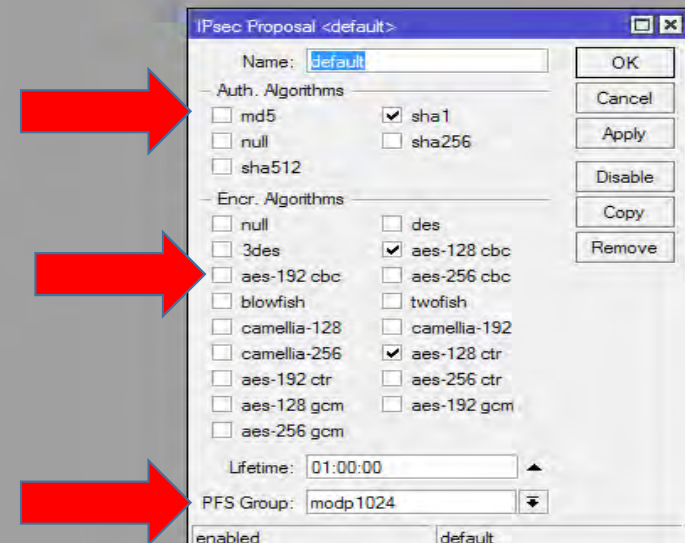
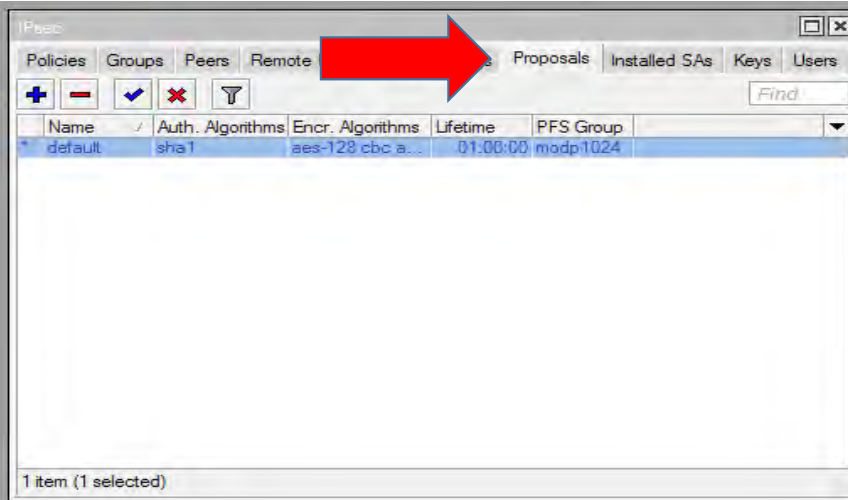
IPsec

Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
192.168.0.0/24		192.168.1.0/24		255 (...)	encrypt	require	yes
				255 (...)	encrypt	require	no

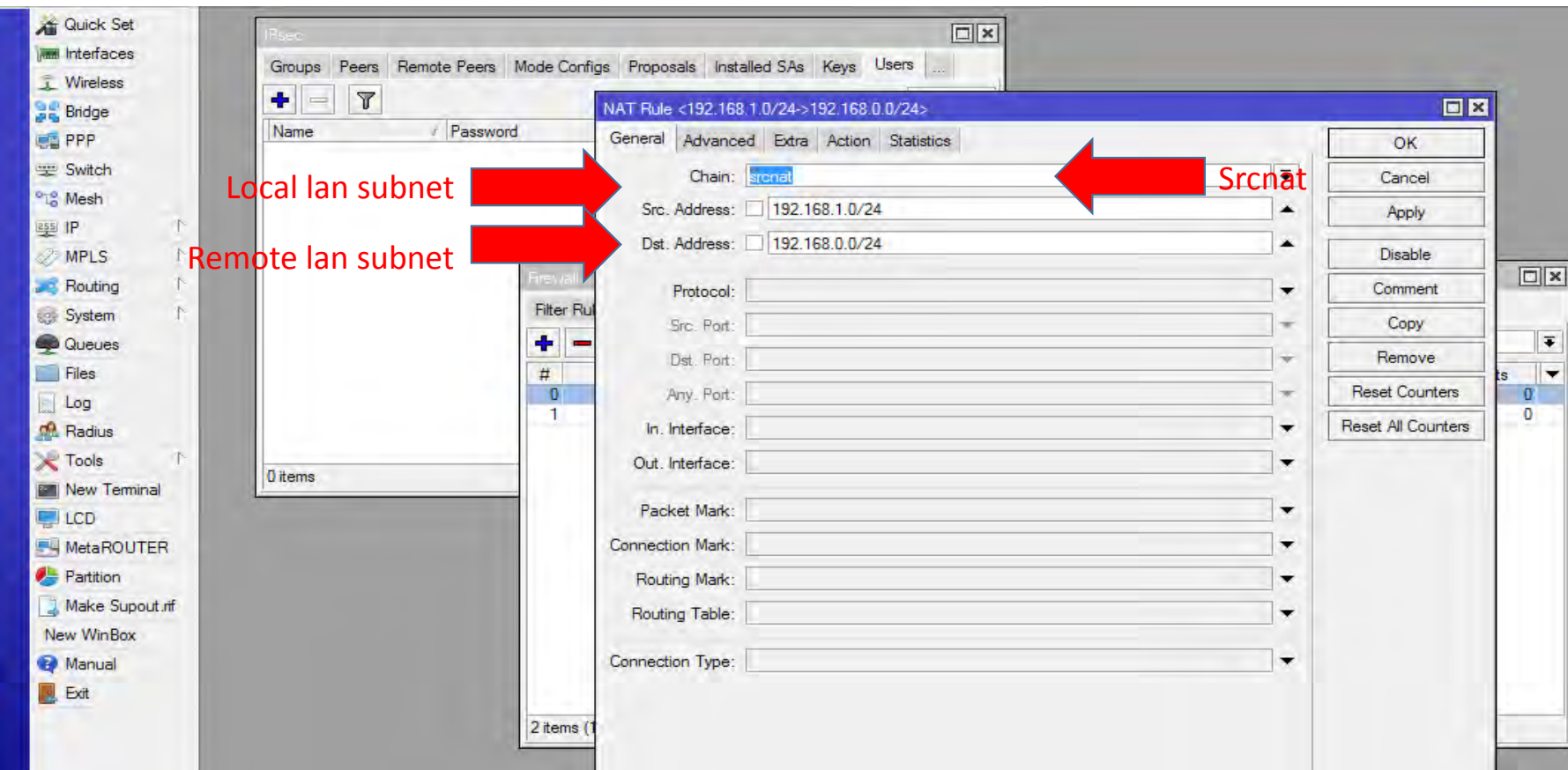
IPSEC Cisco ASA To Mikrotik



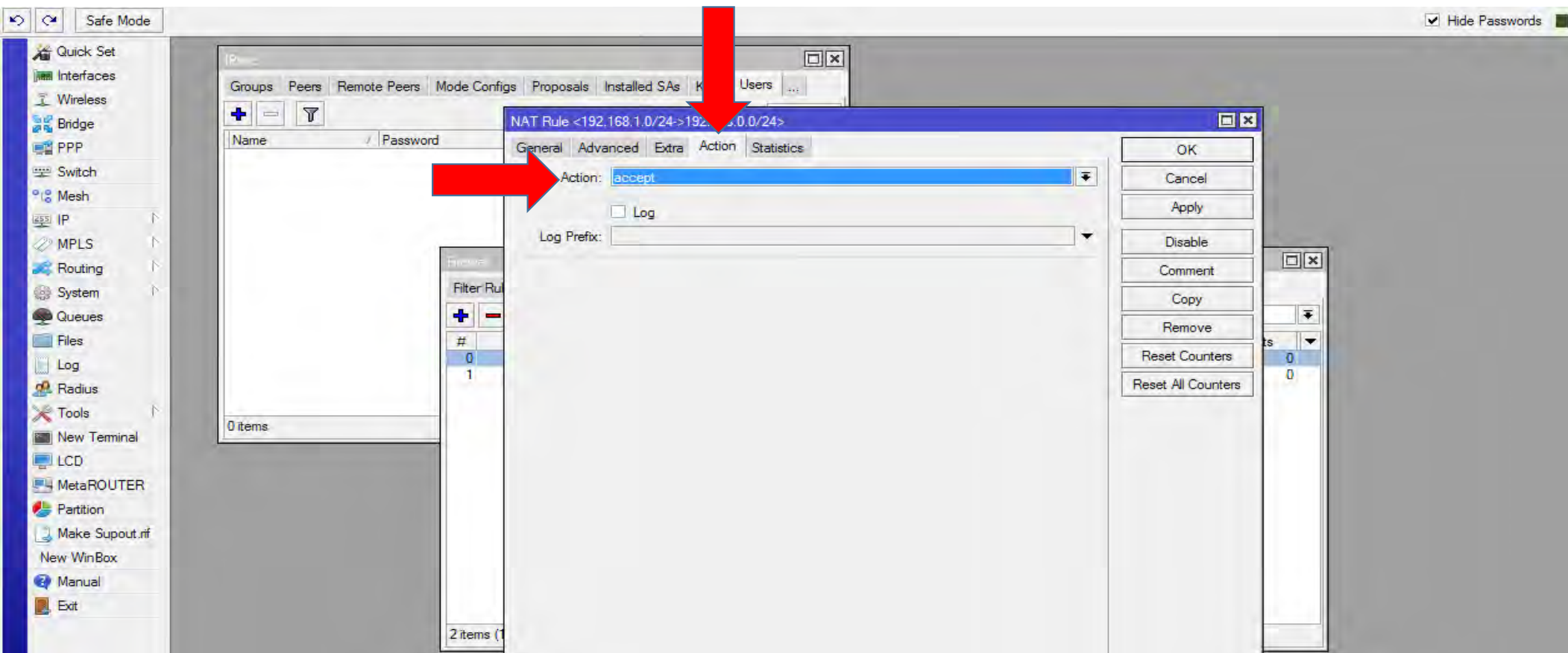
IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik

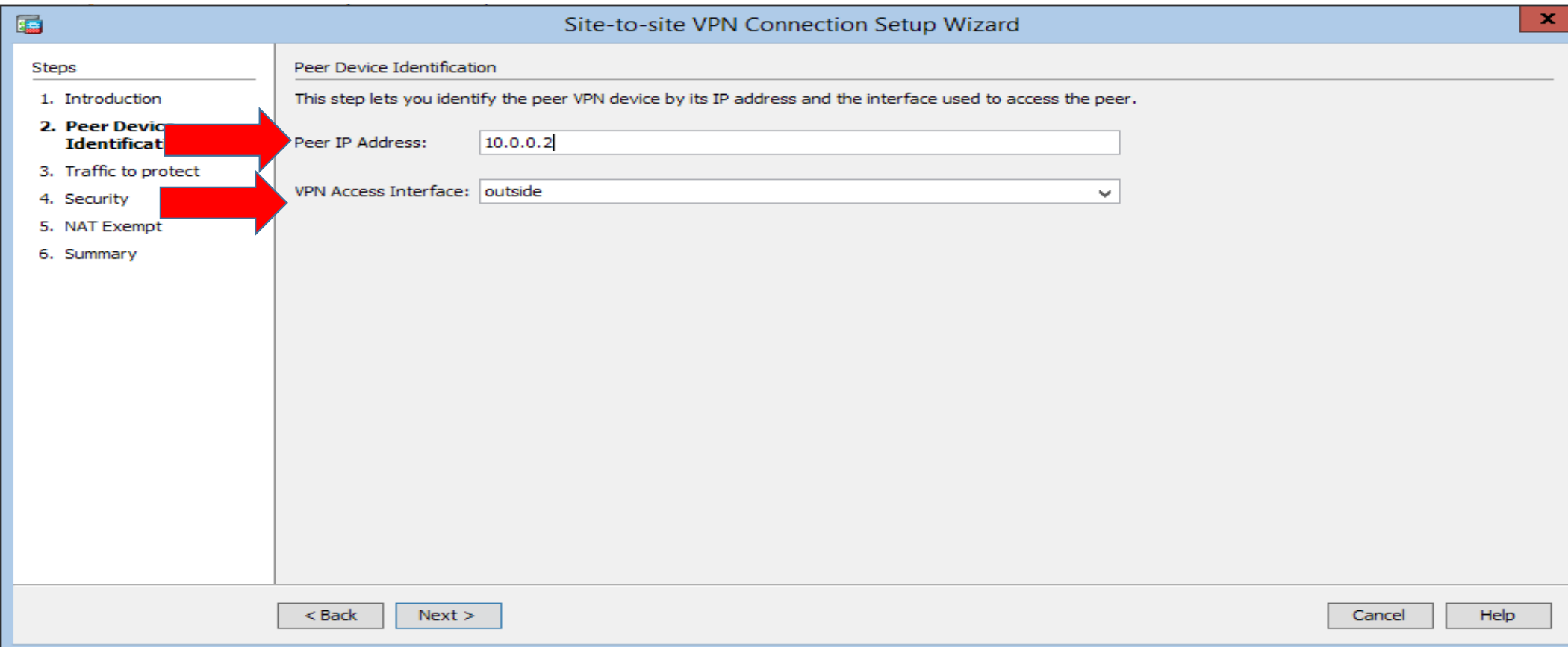
The screenshot shows the Cisco ASDM 7.1 interface for ASA - 192.168.1.1. The 'Wizards' menu is open, and the 'VPN Wizards' sub-menu is selected. The 'Site-to-site VPN Wizard...' option is highlighted. The background shows the 'Site-to-Site VPN' configuration page with a table of policies.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
GroupPolicy_10.0.0.2	Internal	ikev2;ikev1	10.0.0.2
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup

IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik



The image shows a screenshot of the 'Site-to-site VPN Connection Setup Wizard' window. The window has a title bar with a close button (X) in the top right corner. On the left side, there is a 'Steps' list with six items: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. Security, 5. NAT Exempt, and 6. Summary. Item 2 is highlighted in bold, and two red arrows point from it to the main content area. The main content area is titled 'Peer Device Identification' and contains the text: 'This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.' Below this text are two input fields: 'Peer IP Address:' with the value '10.0.0.2' and 'VPN Access Interface:' with the value 'outside' (selected from a dropdown menu). At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
- 2. Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

Peer Device Identification

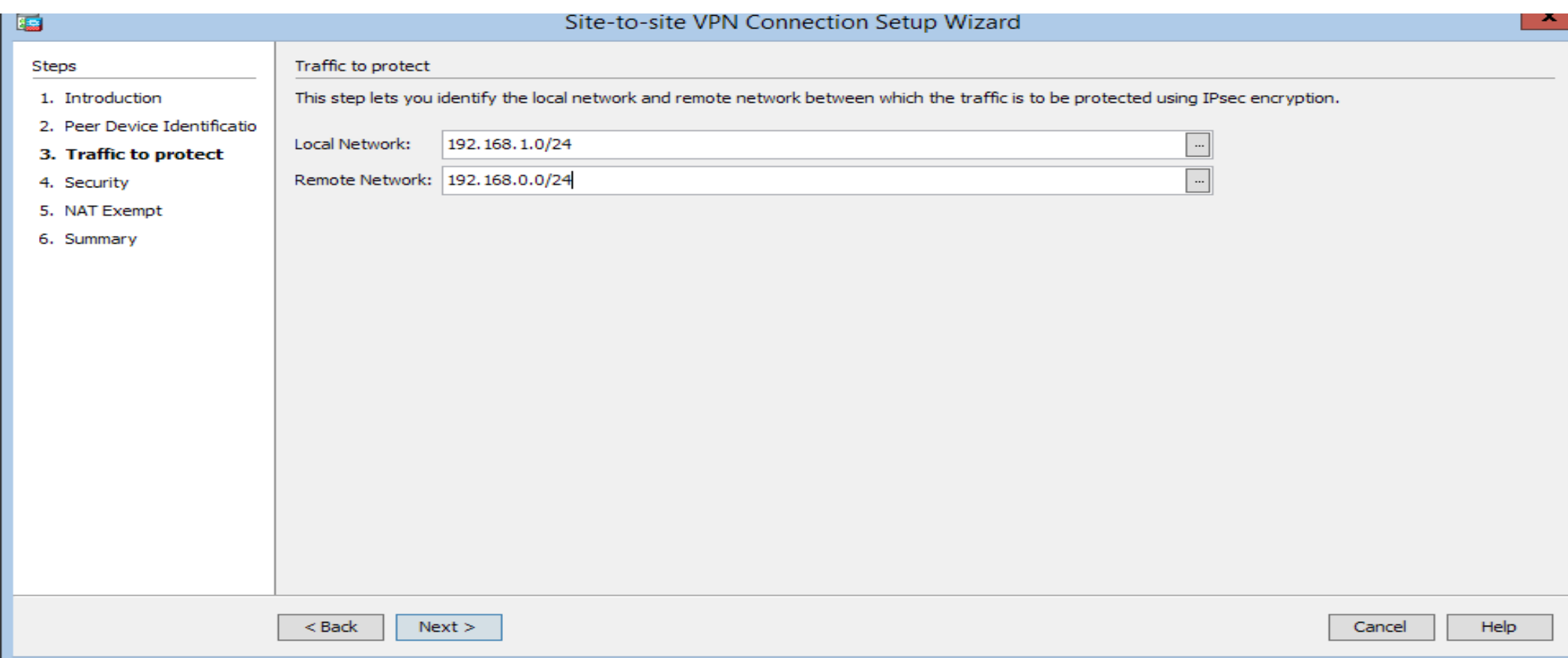
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 10.0.0.2

VPN Access Interface: outside

< Back Next > Cancel Help

IPSEC Cisco ASA To Mikrotik



The image shows a screenshot of a 'Site-to-site VPN Connection Setup Wizard' window. The window has a title bar with a standard Windows icon on the left and a close button on the right. On the left side, there is a 'Steps' pane with a list of six steps: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect (which is bolded and has a dark background), 4. Security, 5. NAT Exempt, and 6. Summary. The main area of the window is titled 'Traffic to protect' and contains a descriptive text: 'This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.' Below this text are two input fields. The first is labeled 'Local Network:' and contains the text '192.168.1.0/24' with a small '...' button to its right. The second is labeled 'Remote Network:' and contains the text '192.168.0.0/24' with a small '...' button to its right. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
- 3. Traffic to protect**
4. Security
5. NAT Exempt
6. Summary

Traffic to protect

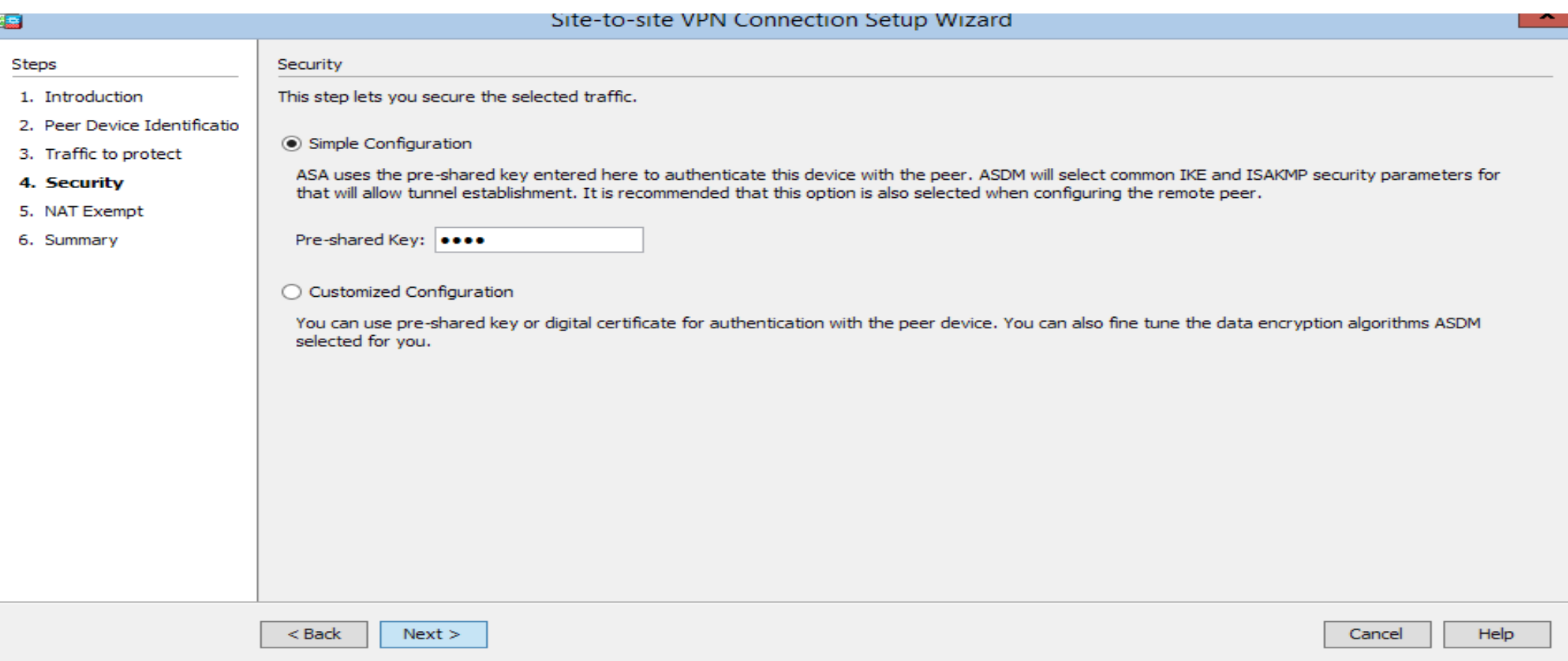
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network: 192.168.1.0/24 ...

Remote Network: 192.168.0.0/24 ...

< Back Next > Cancel Help

IPSEC Cisco ASA To Mikrotik



The image shows a screenshot of the 'Site-to-site VPN Connection Setup Wizard' window. The window has a blue title bar and a light gray background. On the left side, there is a 'Steps' panel with a list of steps: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. **Security**, 5. NAT Exempt, and 6. Summary. Step 4 is highlighted. The main area of the wizard is titled 'Security' and contains the following text: 'This step lets you secure the selected traffic.' Below this, there are two radio button options. The first option, 'Simple Configuration', is selected and has a description: 'ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.' Below the description is a text field labeled 'Pre-shared Key:' with four black dots inside. The second option, 'Customized Configuration', is unselected and has a description: 'You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.' At the bottom of the window, there are three buttons: '< Back' (disabled), 'Next >' (active), 'Cancel' (disabled), and 'Help' (disabled).

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
- 4. Security**
5. NAT Exempt
6. Summary

Security

This step lets you secure the selected traffic.

☒ Simple Configuration

ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

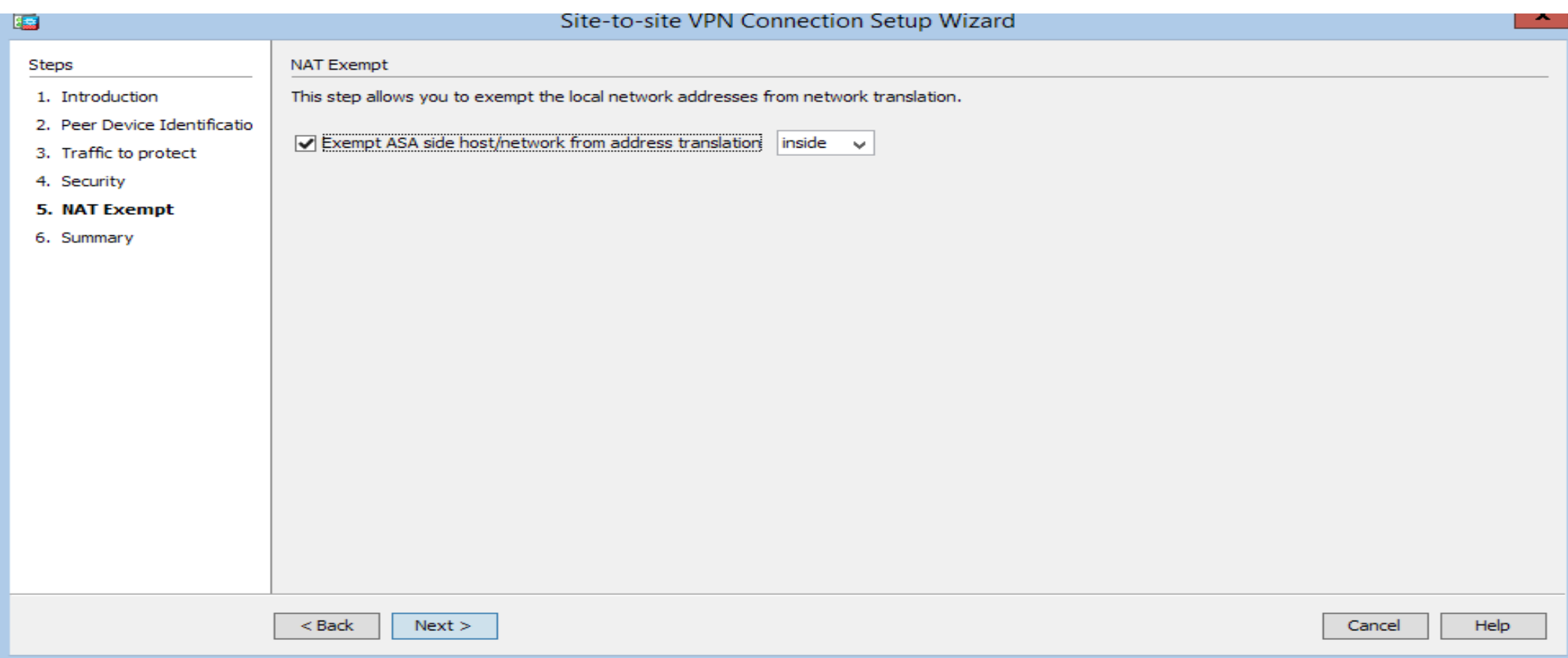
Pre-shared Key:

☐ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

< Back Next > Cancel Help

IPSEC Cisco ASA To Mikrotik



The image shows a screenshot of the 'Site-to-site VPN Connection Setup Wizard' window. The window has a blue title bar and a light gray background. On the left side, there is a 'Steps' panel with a list of steps: 1. Introduction, 2. Peer Device Identification, 3. Traffic to protect, 4. Security, 5. NAT Exempt (highlighted in bold), and 6. Summary. The main area of the wizard is titled 'NAT Exempt' and contains the text: 'This step allows you to exempt the local network addresses from network translation.' Below this text, there is a checkbox labeled 'Exempt ASA side host/network from address translation' which is checked. To the right of the checkbox is a dropdown menu showing 'inside'. At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. Security
- 5. NAT Exempt**
6. Summary

NAT Exempt

This step allows you to exempt the local network addresses from network translation.


☒ Exempt ASA side host/network from address translation inside

< Back Next > Cancel Help

IPSEC Cisco ASA To Mikrotik

Site-to-site VPN Connection Setup Wizard

VPN Wizard



Summary

Here is the summary of the configuration.

Name	Value
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> IKE v2	

< Back

Finish

Cancel

Help

IPSEC Cisco ASA To Mikrotik

Edit IPsec Site-to-Site Connection Profile: 10.0.0.2

Protected Networks

Local Network: inside-network/24

Remote Network: 192.168.0.0/24

IPsec Enabling

Group Policy Name: GroupPolicy_10.0.0.2

(Following two fields are attributes of the group policy selected above.)

☒ Enable IKE v1 ☒ Enable IKE v2

Settings

IKE v1 Settings | IKE v2 Settings

Authentication

Pre-shared Key:

Device Certificate: -- None --

Encryption Algorithms

IKE Policy: crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha,

IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-SHA,

NAT Exempt

This allows you to exempt the local network addresses from network translation.

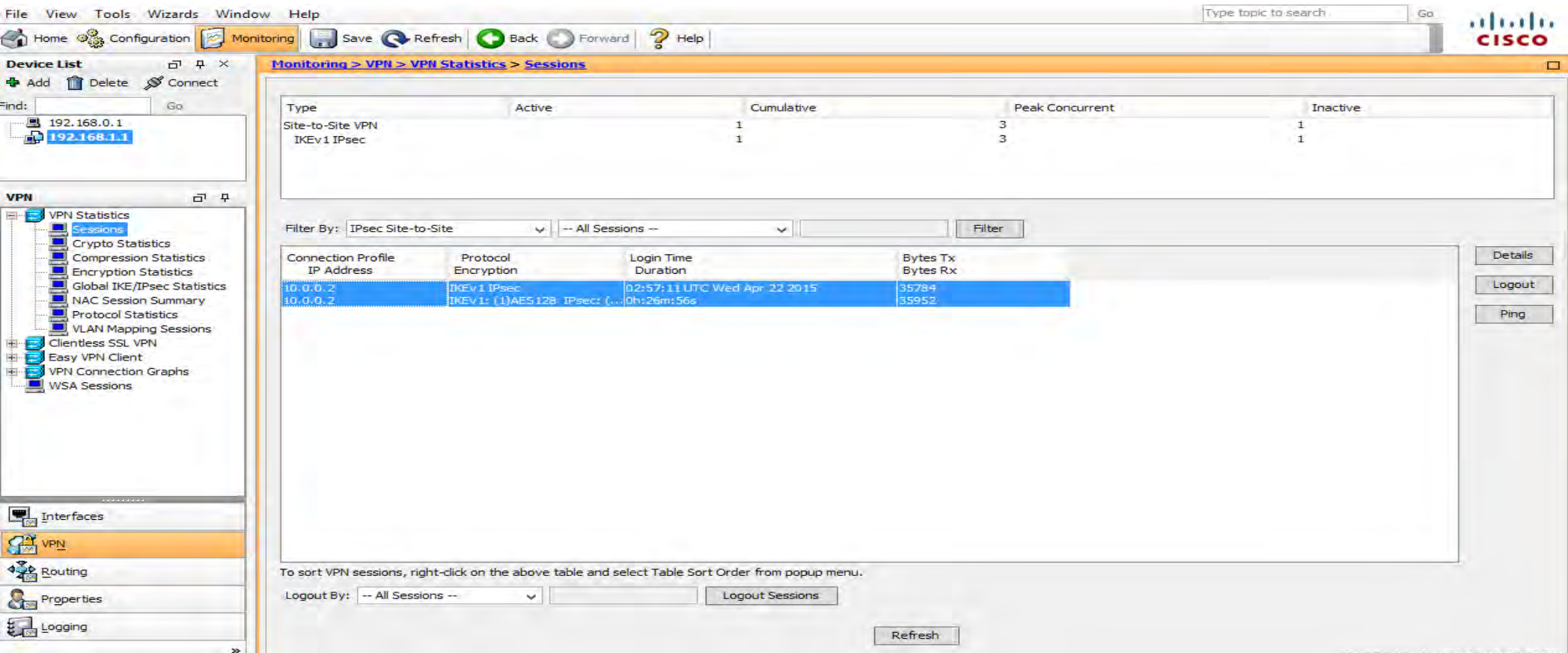
☒ Exempt ASA side host/network from address translation inside

Find:

Next Previous

OK Cancel Help

IPSEC Cisco ASA To Mikrotik



The screenshot displays the Cisco ASA Monitoring interface, specifically the 'VPN > VPN Statistics > Sessions' page. The interface includes a top navigation bar with 'File', 'View', 'Tools', 'Wizards', 'Window', and 'Help' menus. Below this is a 'Device List' sidebar on the left, showing a search for '192.168.0.1' and '192.168.1.1'. The main content area shows a summary table of VPN sessions and a detailed table of active sessions.

VPN Sessions Summary Table:

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	1	3	1
IKEv1 IPsec	1	1	3	1

Filter By: IPsec Site-to-Site -- All Sessions --

VPN Sessions Detailed Table:

Connection Profile	Protocol	Login Time	Bytes Tx	Bytes Rx
IP Address	Encryption	Duration		
10.0.0.2	IKEv1 IPsec	02:57:11 UTC Wed Apr 22 2015	35784	
10.0.0.2	IKEv1: (1)AES 128 IPsec: (...)	0h:26m:56s	35952	

Logout By: -- All Sessions -- Logout Sessions

Refresh

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

IPSEC Cisco ASA To Mikrotik

Session Details

Session Details

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
10.0.0.2	IKEv1 IPsec	02:57:11 UTC Wed Apr 22 2015	35784
10.0.0.2	IKEv1: (1)AES128 IPsec: (...)	0h:19m:32s	35952

Details

ACL

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	IKEv1		AES-128	Tunnel ID: 4.1 Authentication Mode: preSharedKeys UDP Source Port 500 UDP Destination Port 500 Authentication Mode: preSharedKeys UDP Source Port 500 UDP Destination Port 500 IKE Negotiation Mode: Main Hashing: SHA1 Authentication Mode: preSharedKeys UDP Source Port 500 UDP Destination Port 500 IKE Negotiation Mode: Main Hashing: SHA1 Diffie-Hellman Group: 2 Rekey Time Interval: 86400 Seconds Rekey Left(T): 85227 Seconds	
	IPsec	192.168.1.0/255.255.255.0/0/0 192.168.0.0/255.255.255.0/0/0	AES-128	Tunnel ID: 4.2 Hashing: SHA1 Encapsulation: Tunnel Rekey Time Interval: 28800 Seconds Rekey Left(T): 27633 Seconds Rekey Data Interval: 4608000 K-Bytes	35784 35952

Refresh

Close

Help

Tunnel ID: 4.2

Hashing: SHA1

Encapsulation: Tunnel

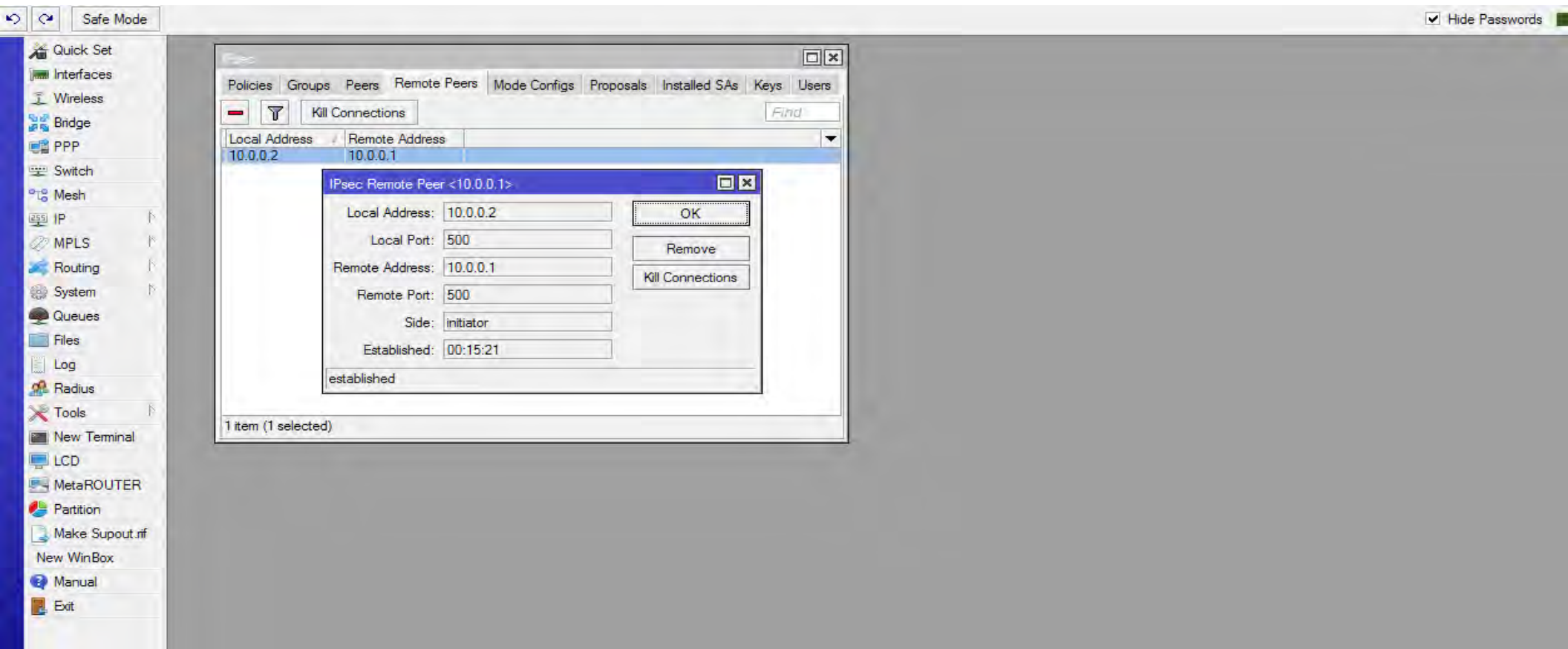
Rekey Time Interval: 28800 Seconds

Rekey Left(T): 27633 Seconds

Rekey Data Interval: 4608000 K-Bytes

Updated: 4/21/15 10:39:02 PM

IPSEC Cisco ASA To Mikrotik



IPSEC Cisco ASA To Mikrotik

Safe Mode

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.tif
New WinBox
Manual
Exit

Ring (Running)

General Advanced

Src. Address: 192.168.0.1

Packet Size: 50

TTL:

DSCP:

Routing Table:

☐ Dont Fragment

Start
Stop
Close
New Window

Seq #	Host	Time	Reply Size	TTL	Status
699	192.168.1.79	1ms	50	128	
700	192.168.1.79	1ms	50	128	
701	192.168.1.79	1ms	50	128	
702	192.168.1.79	1ms	50	128	
703	192.168.1.79	1ms	50	128	
704	192.168.1.79	1ms	50	128	
705	192.168.1.79	1ms	50	128	
706	192.168.1.79	2ms	50	128	
707	192.168.1.79	2ms	50	128	
708	192.168.1.79	1ms	50	128	
709	192.168.1.79	1ms	50	128	
710	192.168.1.79	1ms	50	128	
711	192.168.1.79	1ms	50	128	
712	192.168.1.79	1ms	50	128	
713	192.168.1.79	1ms	50	128	

714 items 672 of 714 packets... 5% packet loss Min: 0 ms Avg: 1 ms Max: 46 ms

IPsec

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users

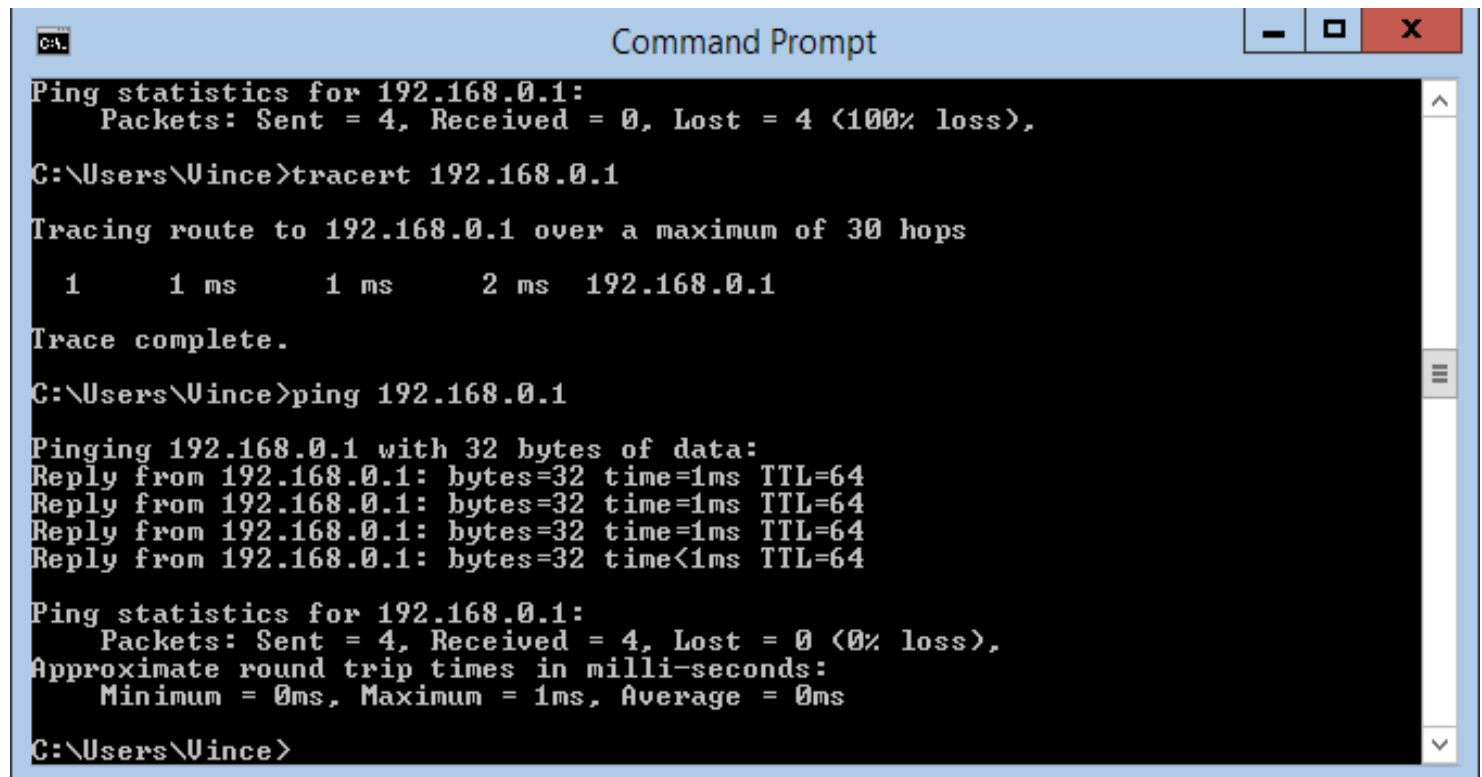
Flush Find

SPI	Src. Address	Dst. Address	Auth...	Encr...	Current B...
8a936c	10.0.0.1	10.0.0.2	sha1	aes c...	34534
fa710a2f	10.0.0.2	10.0.0.1	sha1	aes c...	34702

2 items

Hide Passwords

IPSEC Cisco ASA To Mikrotik



```
Command Prompt

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Vince>tracert 192.168.0.1

Tracing route to 192.168.0.1 over a maximum of 30 hops
    0      1 ms      1 ms      2 ms   192.168.0.1
Trace complete.

C:\Users\Vince>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Vince>
```

IPSEC Cisco ASA To Mikrotik