Mikrotik VPN for windows domain Remote users

MUM 2016 LEBANON-BEIRUT

By: Eng. Afif Darwich

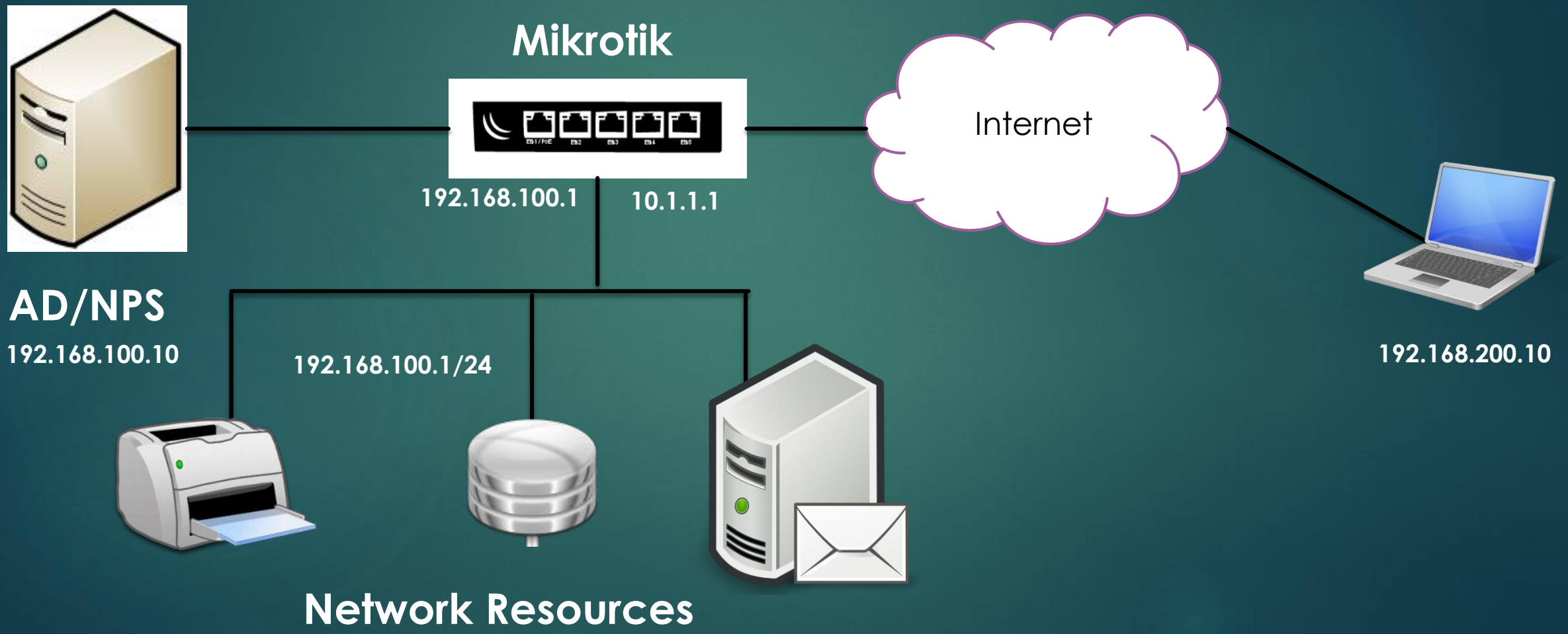
About Me

- Afif Ahmad Darwich
- MTCNA, MTCRE, MTCWE, MTCTCE, MTCINE
- Mikrotik Academy Trainer
- Cisco, Microsoft, Linux
- Ehorizon Cofounder 2014
- Tamkeen Vocational Institute Executive Manager 2016

Contents

- Introduction
- Windows Network Policy Server setup
- Mikrotik VPN server configuration
- Windows VPN client Configuration

Network Diagram



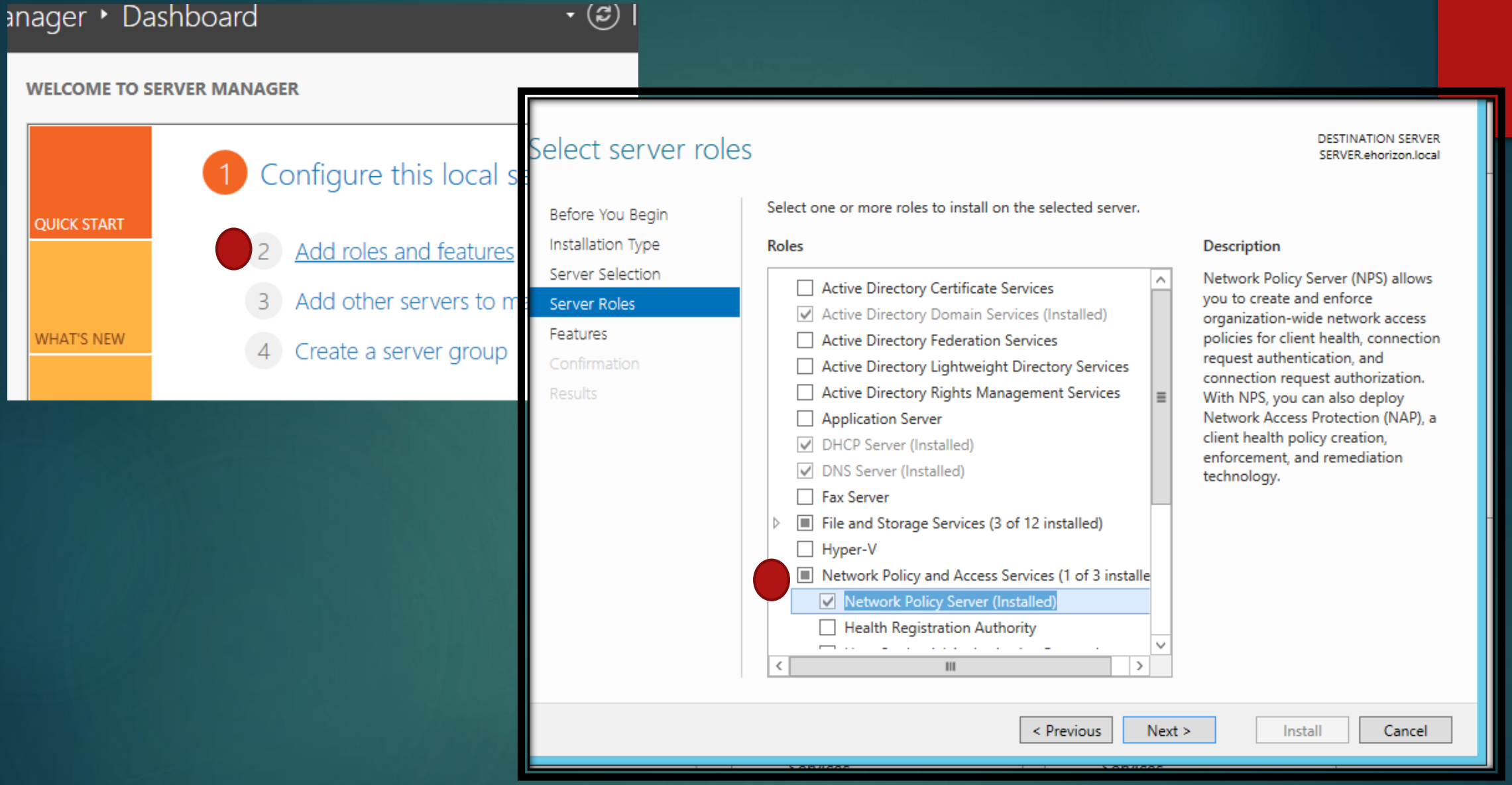
Setup and roles

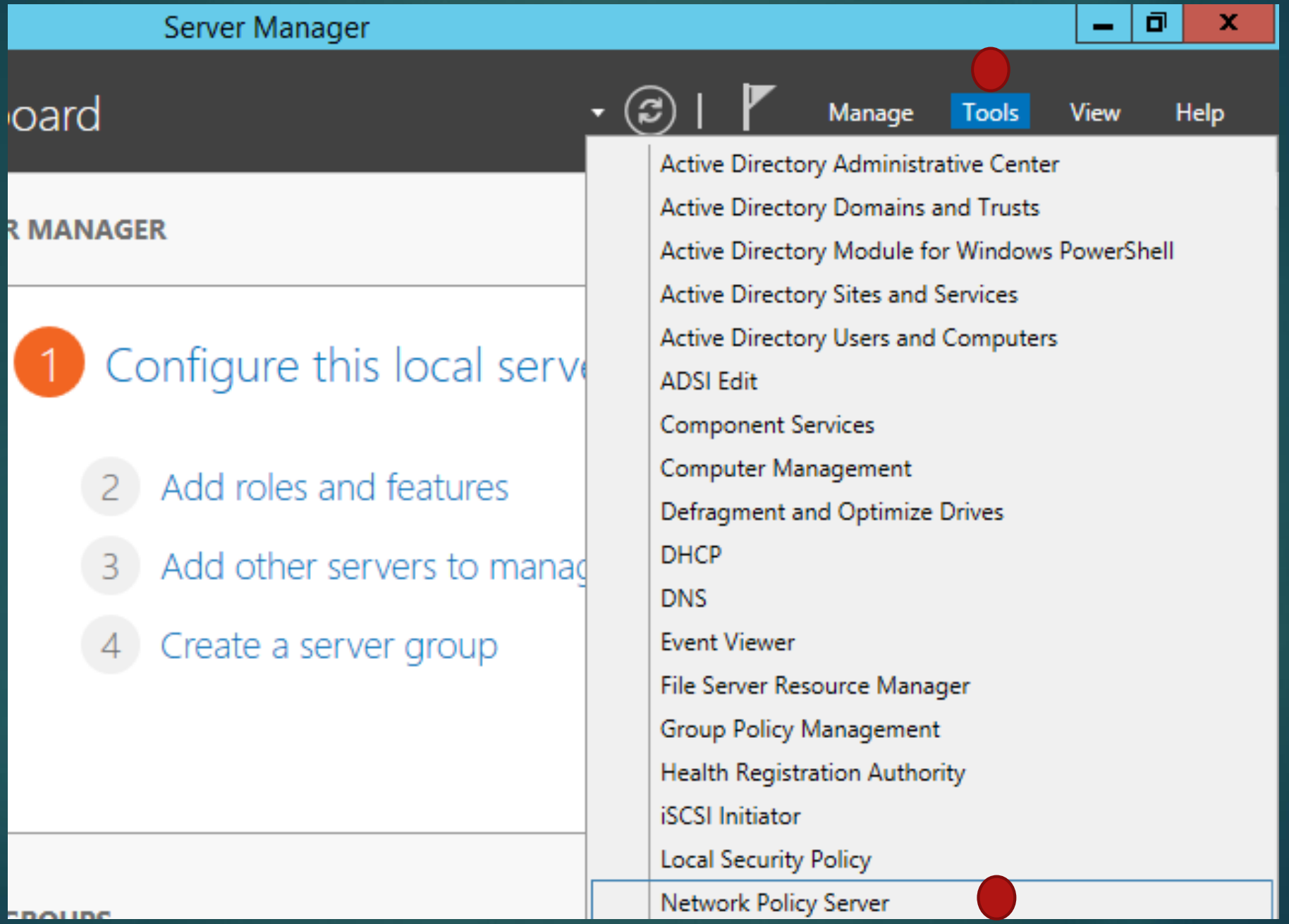
- Windows server 2012:
  - Active directory
  - DNS
  - NPS
- Mikrotik Router
  - L2TP/IPSEC VPN Edge
  - RADIUS client
- Windows Client
  - L2TP/IPSEC VPN client
  - Windows domain user

Benefits

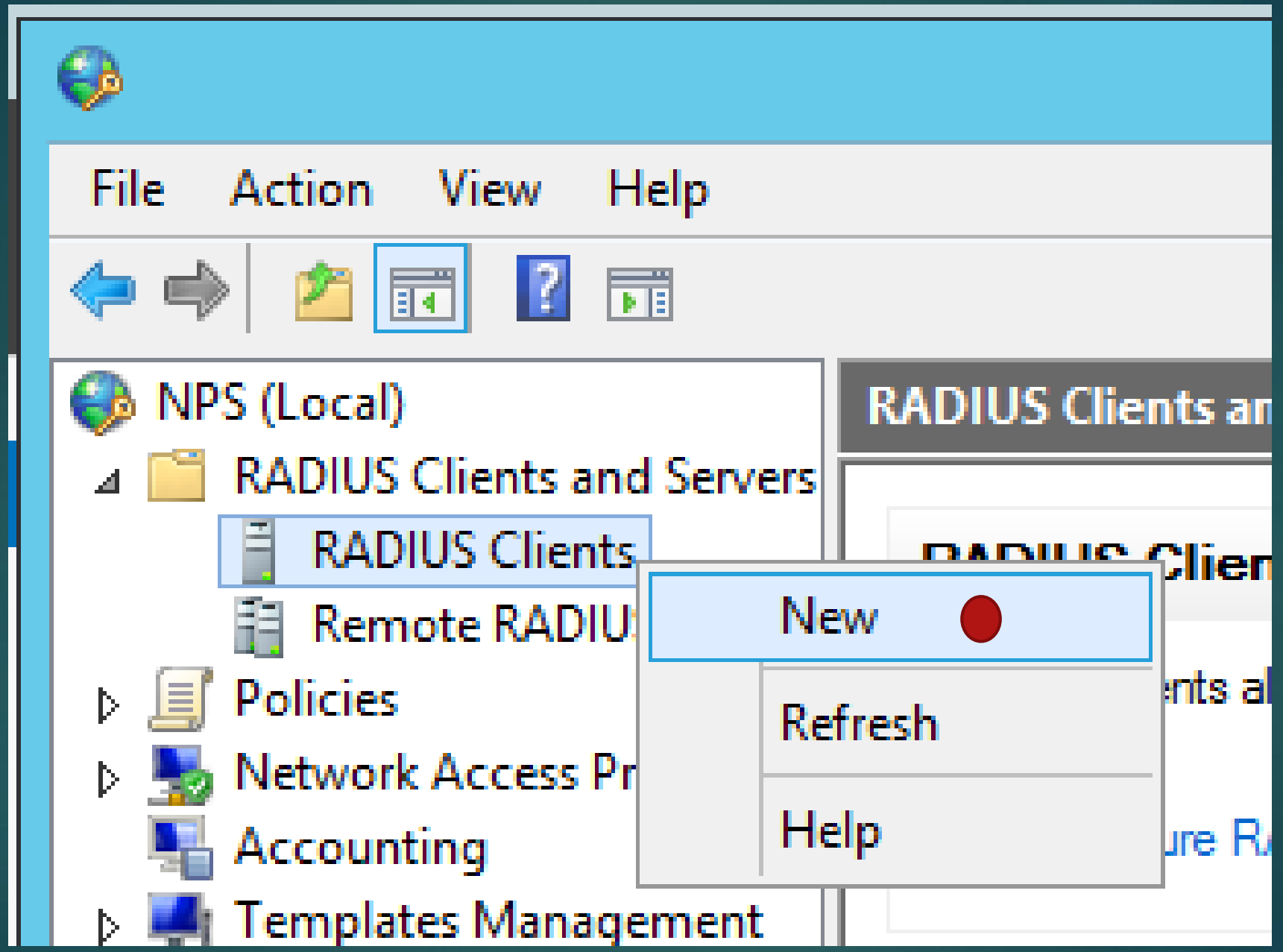
- One centralized User Authentication database.
- No need to create PPP secrets on Mikrotik
- Users will use their windows credentials to connect to VPN and Active directory
- Group policy will be applied to connected users
- Remote users will get benefit of all network resources
- Securing remote user connection using good security standards

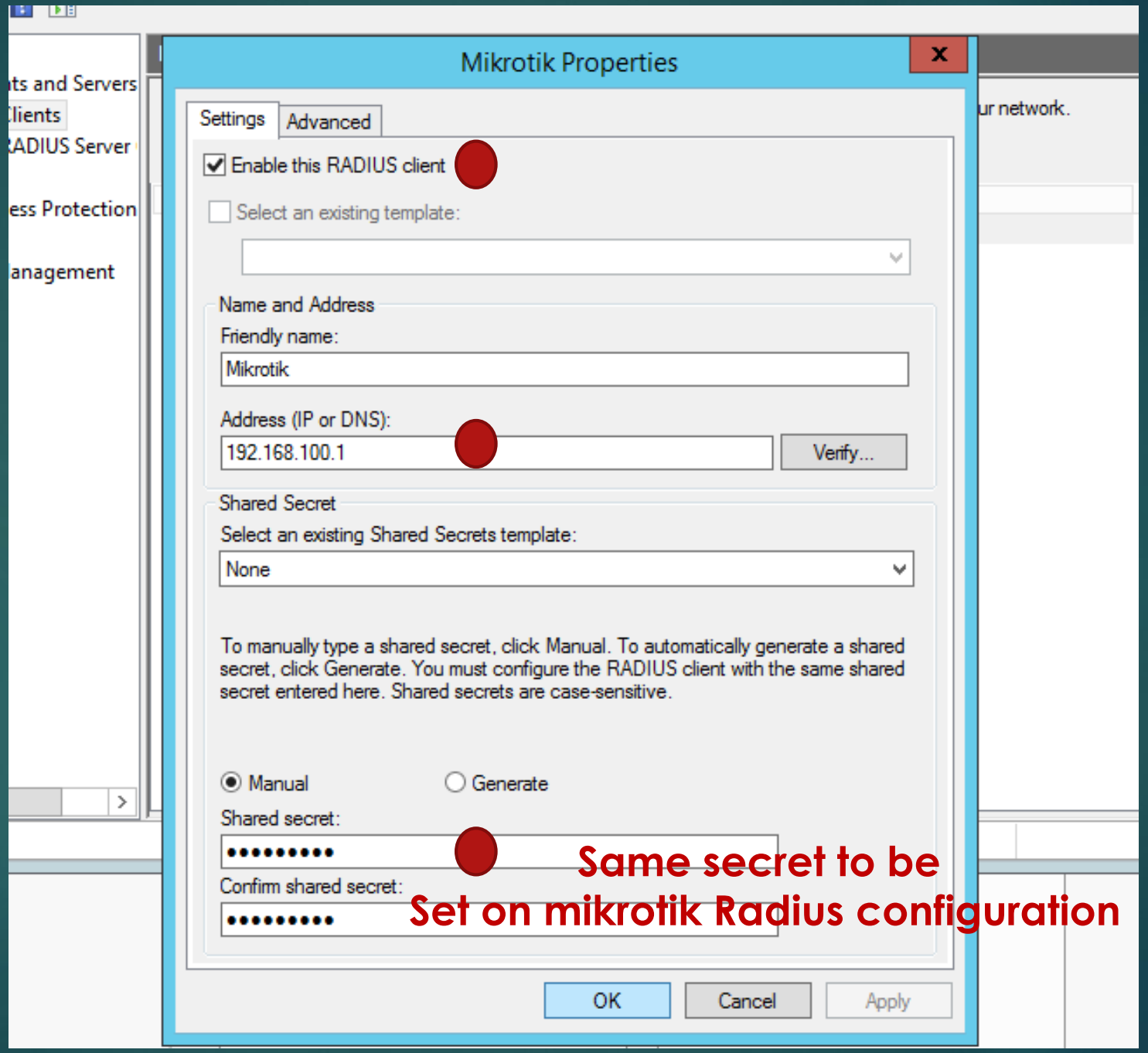
Windows server 2012 Configuration

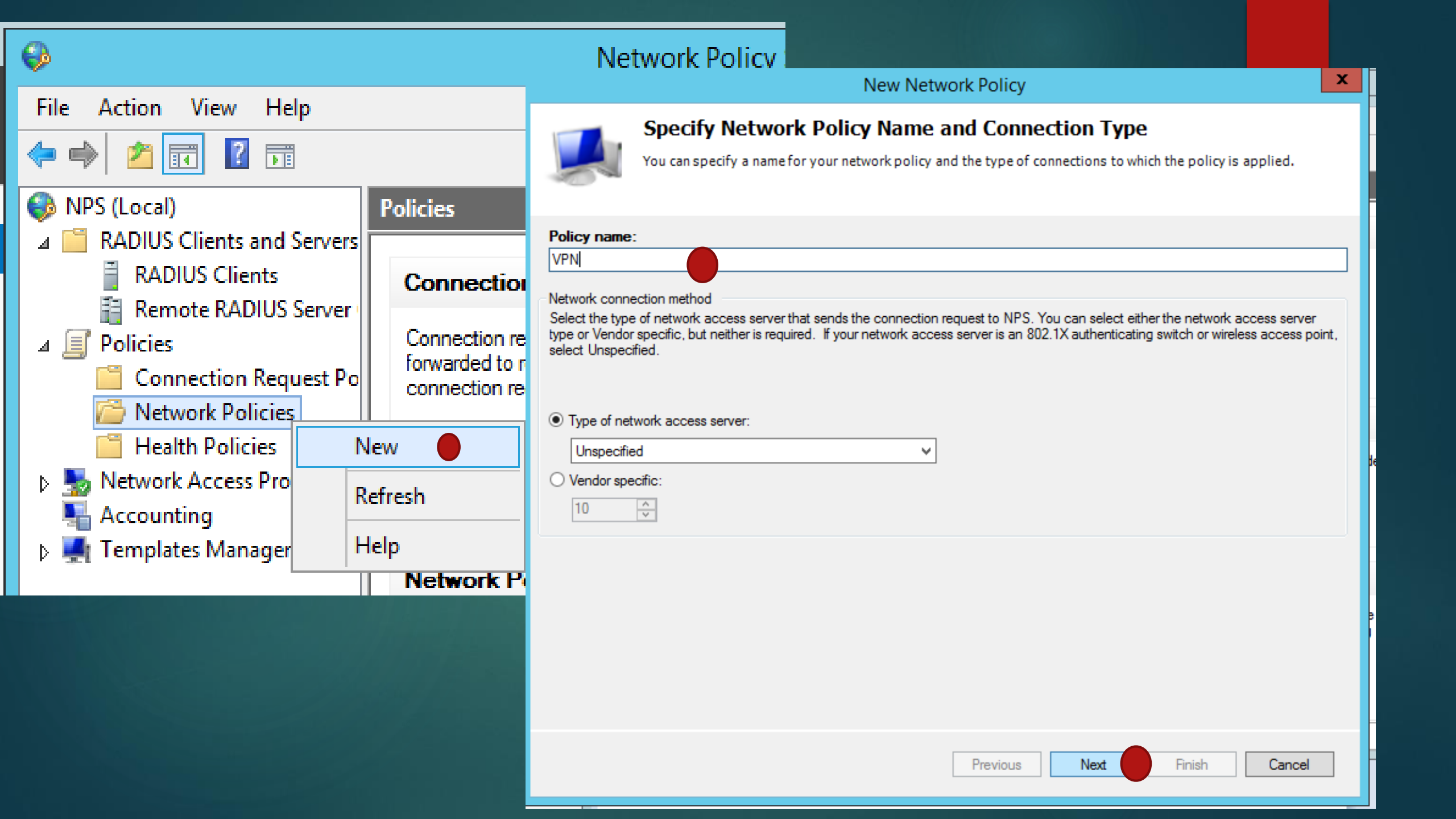

anager ▸ Dashboard
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local s
2 Add roles and features
3 Add other servers to m
4 Create a server group
Select server roles
DESTINATION SERVER
SERVER.ehorizon.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server (Installed)
DNS Server (Installed)
Fax Server
File and Storage Services (3 of 12 installed)
Hyper-V
Network Policy and Access Services (1 of 3 installe
Network Policy Server (Installed)
Health Registration Authority
Description
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.
< Previous
Next >
Install
Cancel

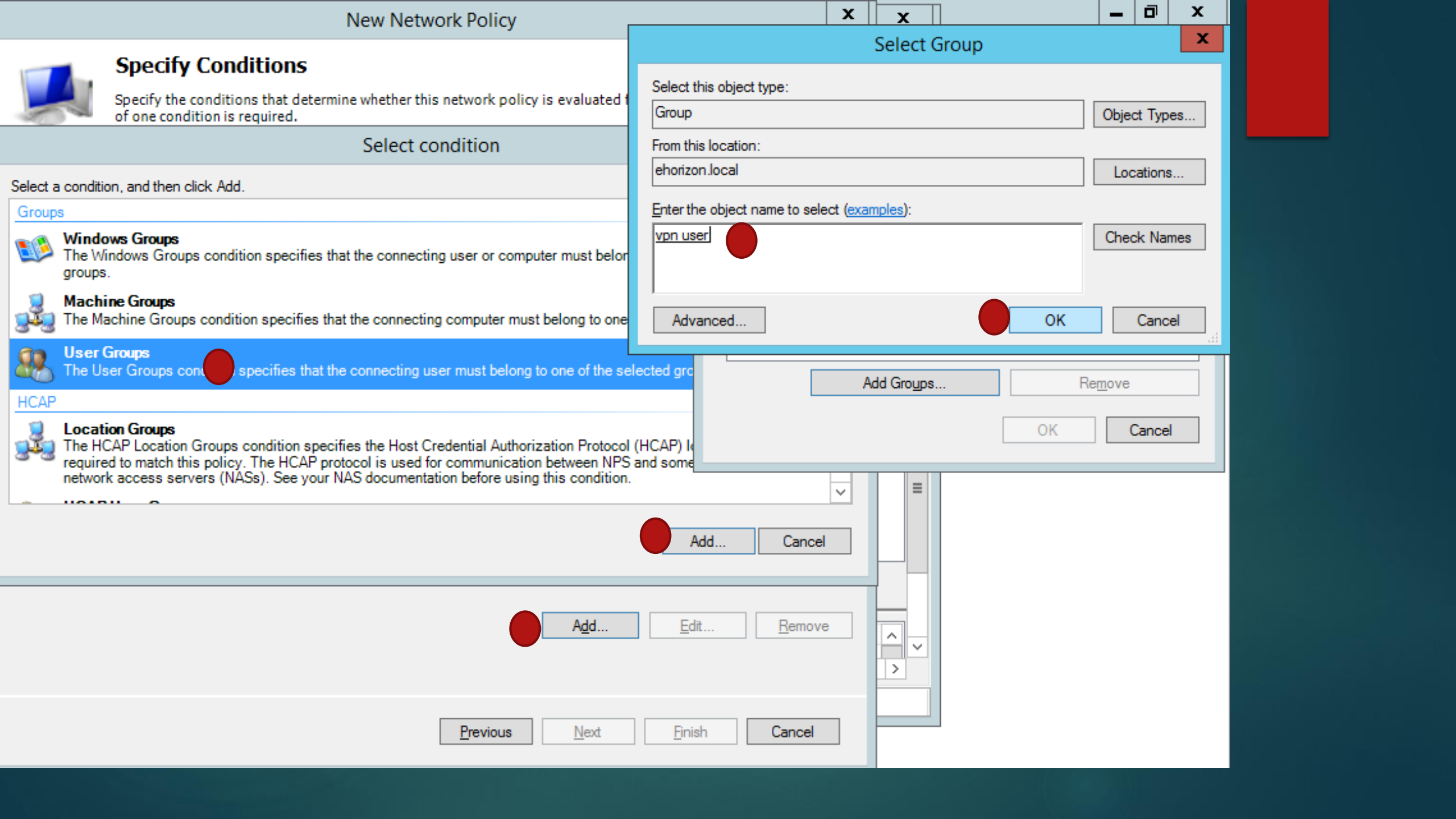

Server Manager
oard
Manage
Tools
View
Help
R MANAGER
1 Configure this local serv
2 Add roles and features
3 Add other servers to manag
4 Create a server group
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
File Server Resource Manager
Group Policy Management
Health Registration Authority
iSCSI Initiator
Local Security Policy
Network Policy Server

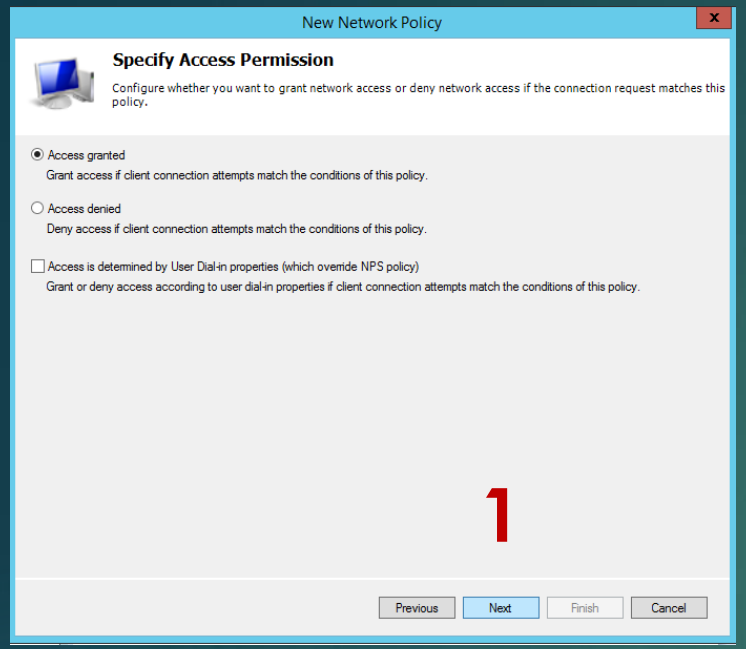

File
Action
View
Help
NPS
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory
Properties
Help
olicies
twork policies allow you to designate
n or cannot connect.
cess Server Policy
ions to Microsoft Routing and Remote
ions to other access servers
Windows Security Hea

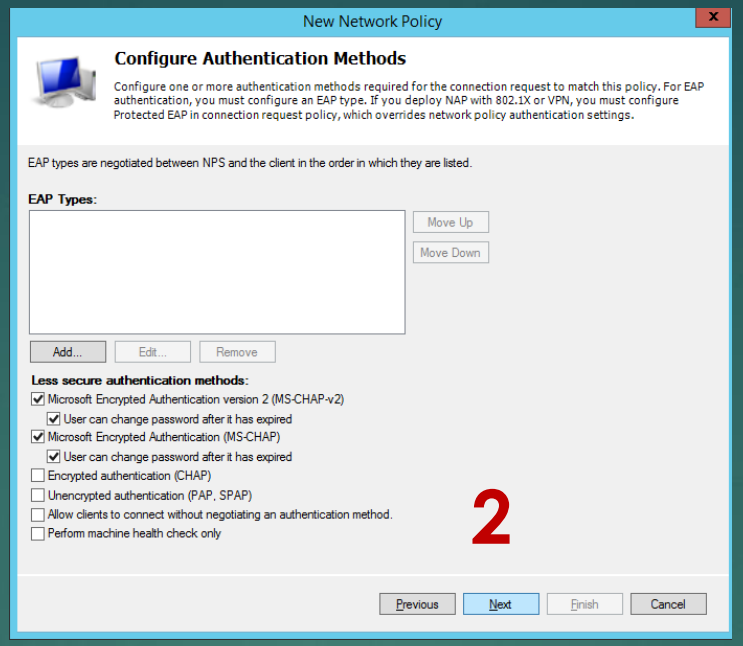

File
Action
View
Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIU
Policies
Network Access Pr
Accounting
Templates Management
RADIUS Clients an
New
Refresh
Help

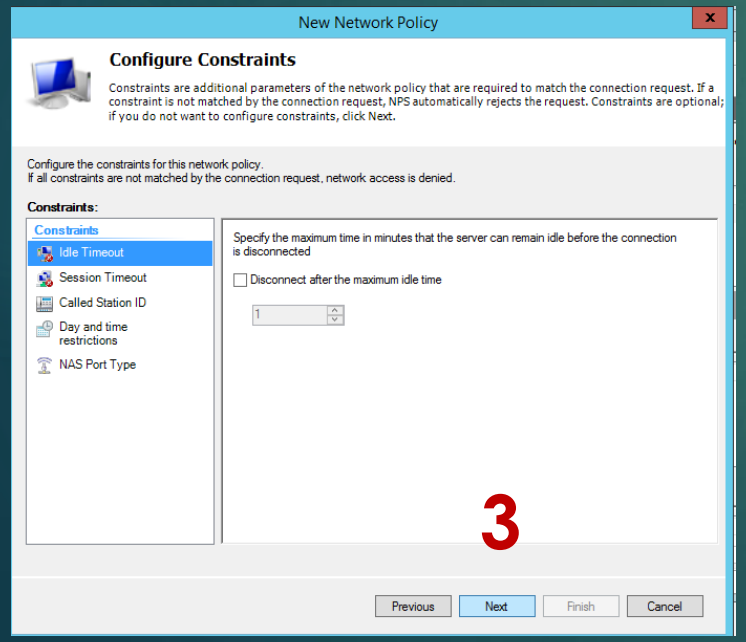

Mikrotik Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Mikrotik
Address (IP or DNS):
192.168.100.1
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply
Same secret to be
Set on mikrotik Radius configuration

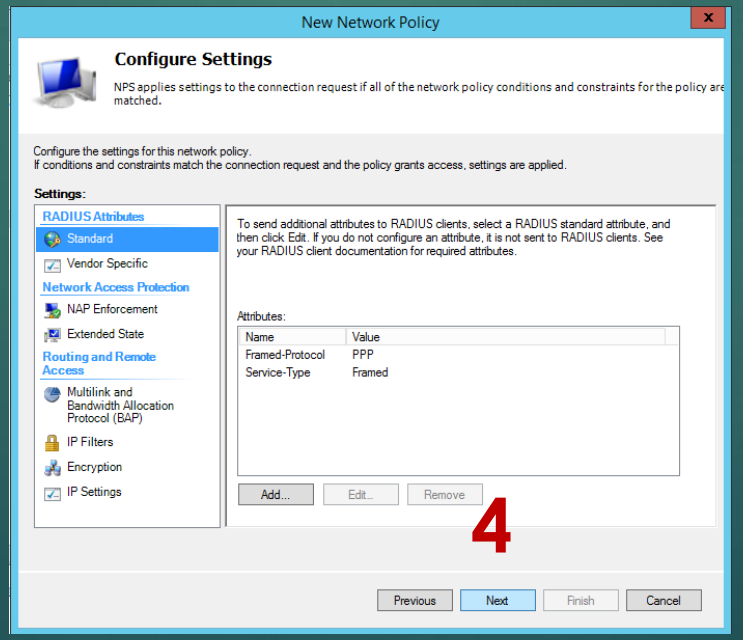

Network Policy
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Health Policies
Network Access Pro
Accounting
Templates Manager
Policies
Connection
Connection re
forwarded to r
connection re
Network P
New
Refresh
Help
New Network Policy
Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name:
VPN
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
Previous
Next
Finish
Cancel

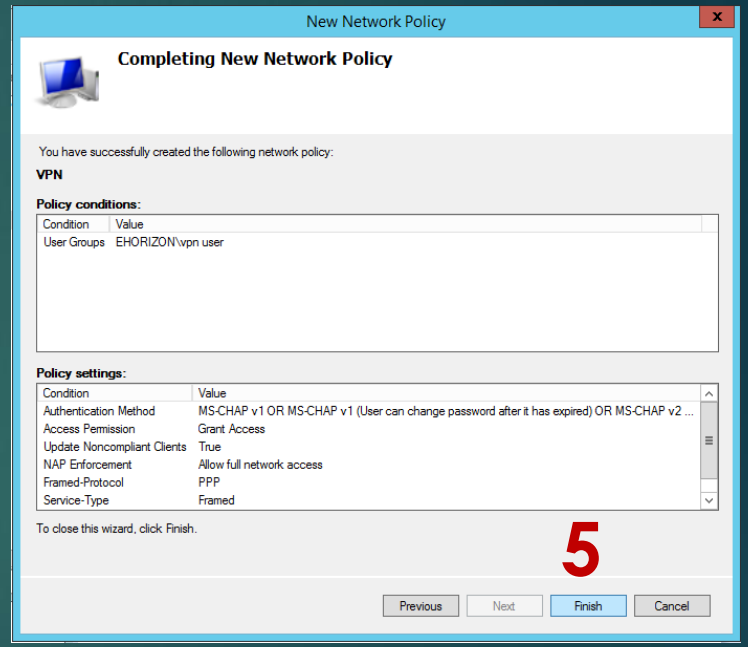

New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated f
of one condition is required.
Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belor
groups.
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one
User Groups
The User Groups con specifies that the connecting user must belong to one of the selected gro
HCAP
Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) l
required to match this policy. The HCAP protocol is used for communication between NPS and some
network access servers (NASs). See your NAS documentation before using this condition.
Add...
Cancel
Add...
Edit...
Remove
Previous
Next
Finish
Cancel
Select Group
Select this object type:
Group
Object Types...
From this location:
ehorizon.local
Locations...
Enter the object name to select (examples):
vpn user
Check Names
Advanced...
OK
Cancel
Add Groups...
Remove
OK
Cancel

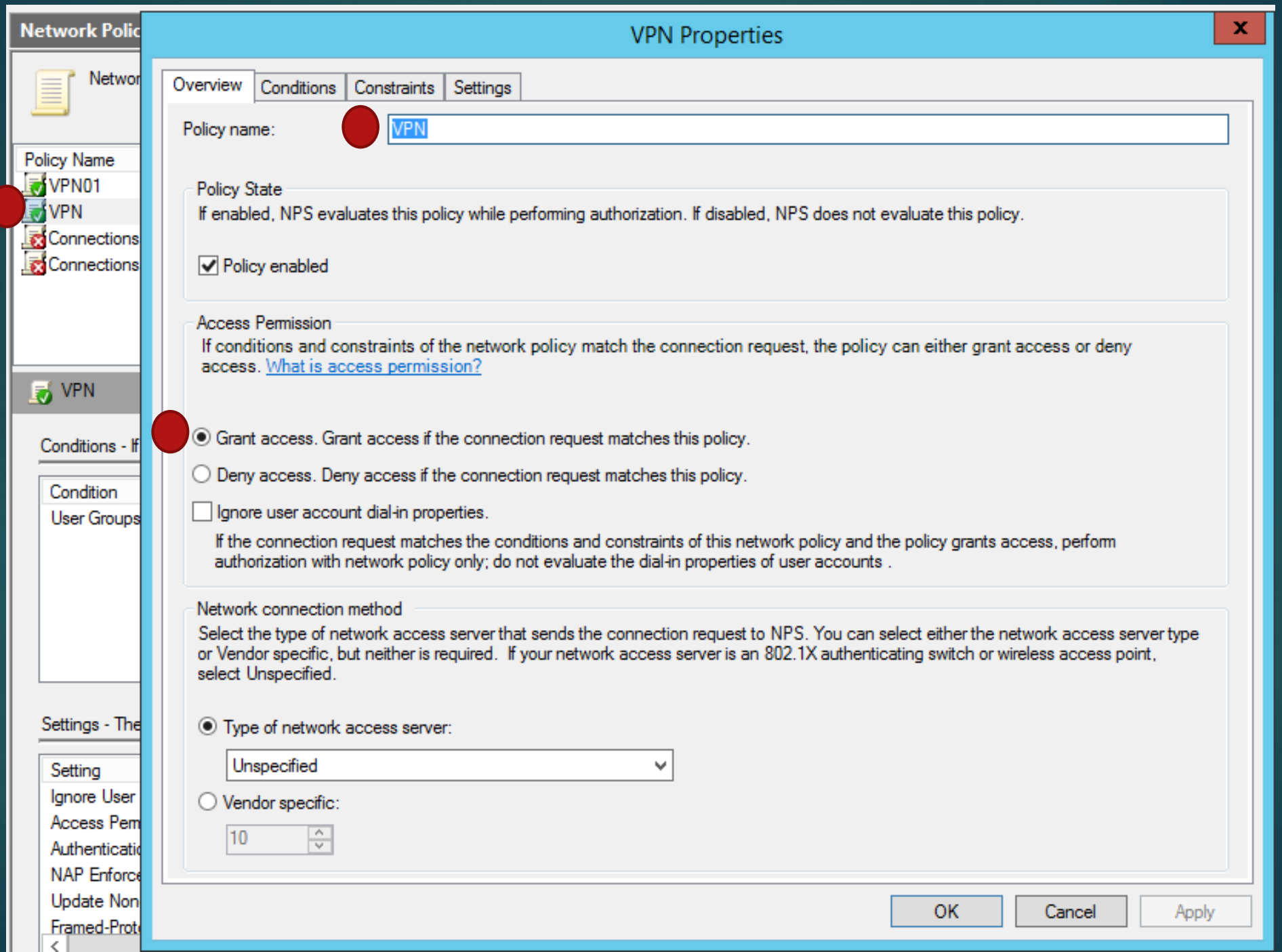

New Network Policy
Specify Access Permission
Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access granted
Grant access if client connection attempts match the conditions of this policy.
Access denied
Deny access if client connection attempts match the conditions of this policy.
Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.
1
Previous
Next
Finish
Cancel


New Network Policy
Configure Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Perform machine health check only
2
Previous
Next
Finish
Cancel


New Network Policy
Configure Constraints
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected
Disconnect after the maximum idle time
1
3
Previous
Next
Finish
Cancel

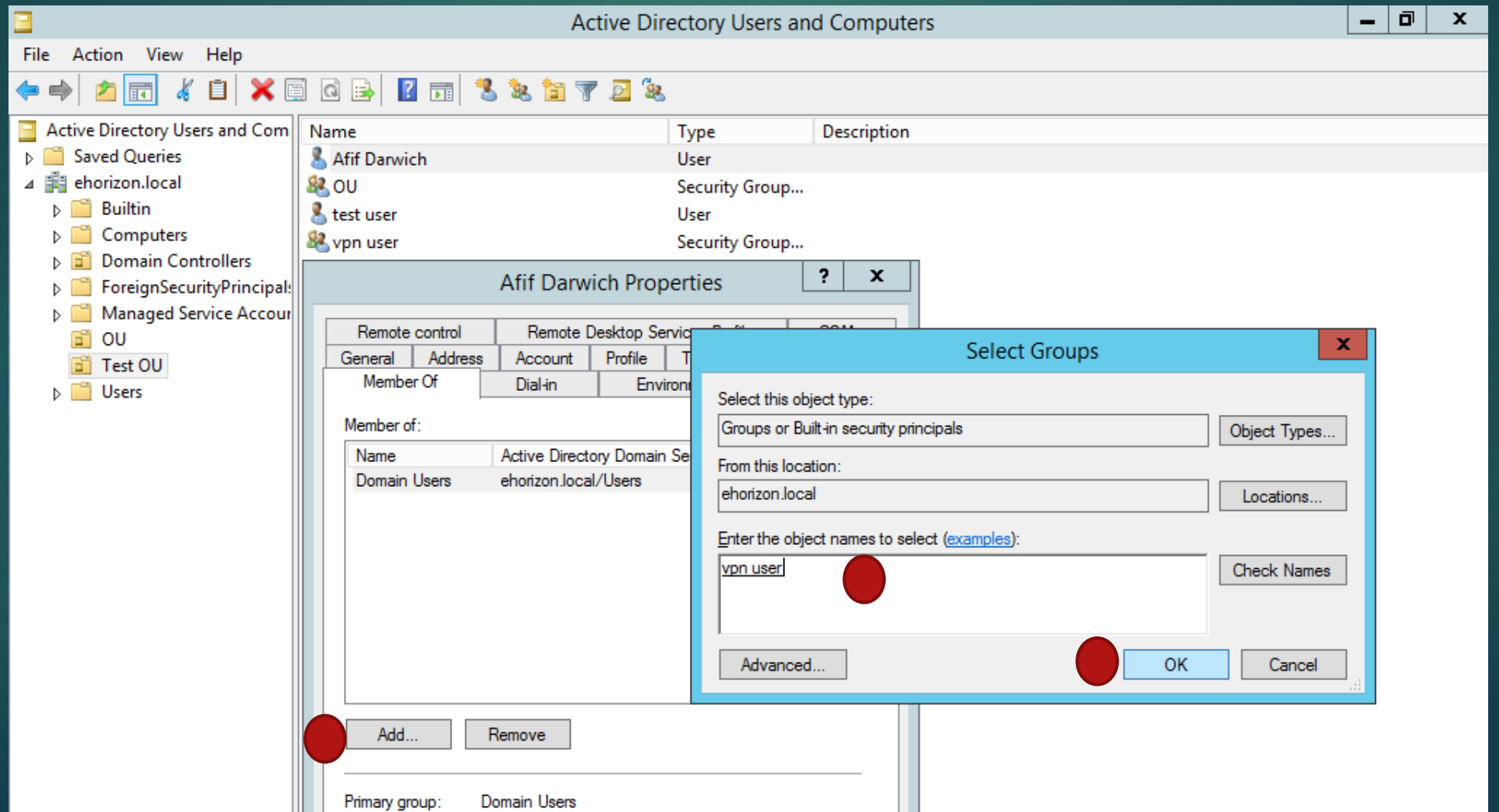

New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
4
Previous
Next
Finish
Cancel


New Network Policy
Completing New Network Policy
You have successfully created the following network policy:
VPN
Policy conditions:
Condition
Value
User Groups
EHORIZON\vpn user
Policy settings:
Condition
Value
Authentication Method
MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission
Grant Access
Update Noncompliant Clients
True
NAP Enforcement
Allow full network access
Framed-Protocol
PPP
Service-Type
Framed
To close this wizard, click Finish.
5
Previous
Next
Finish
Cancel

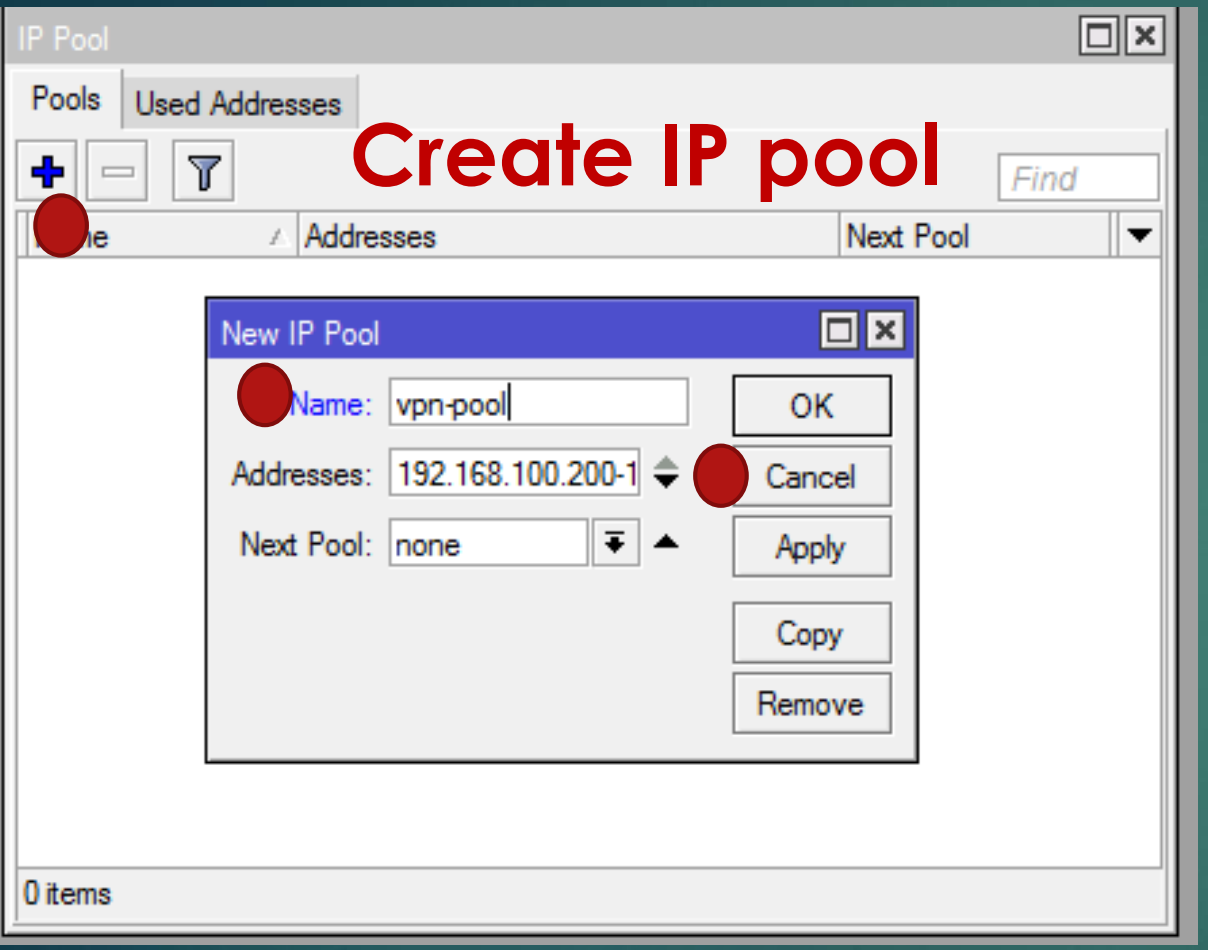

Network Polic
Networ
Policy Name
VPN01
VPN
Connections
Connections
VPN
Conditions - If
Condition
User Groups
Settings - The
Setting
Ignore User
Access Perm
Authenticatio
NAP Enforce
Update Non
Framed-Prot
VPN Properties
Overview
Conditions
Constraints
Settings
Policy name:
VPN
Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.
Policy enabled
Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?
Grant access. Grant access if the connection request matches this policy.
Deny access. Deny access if the connection request matches this policy.
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
OK
Cancel
Apply

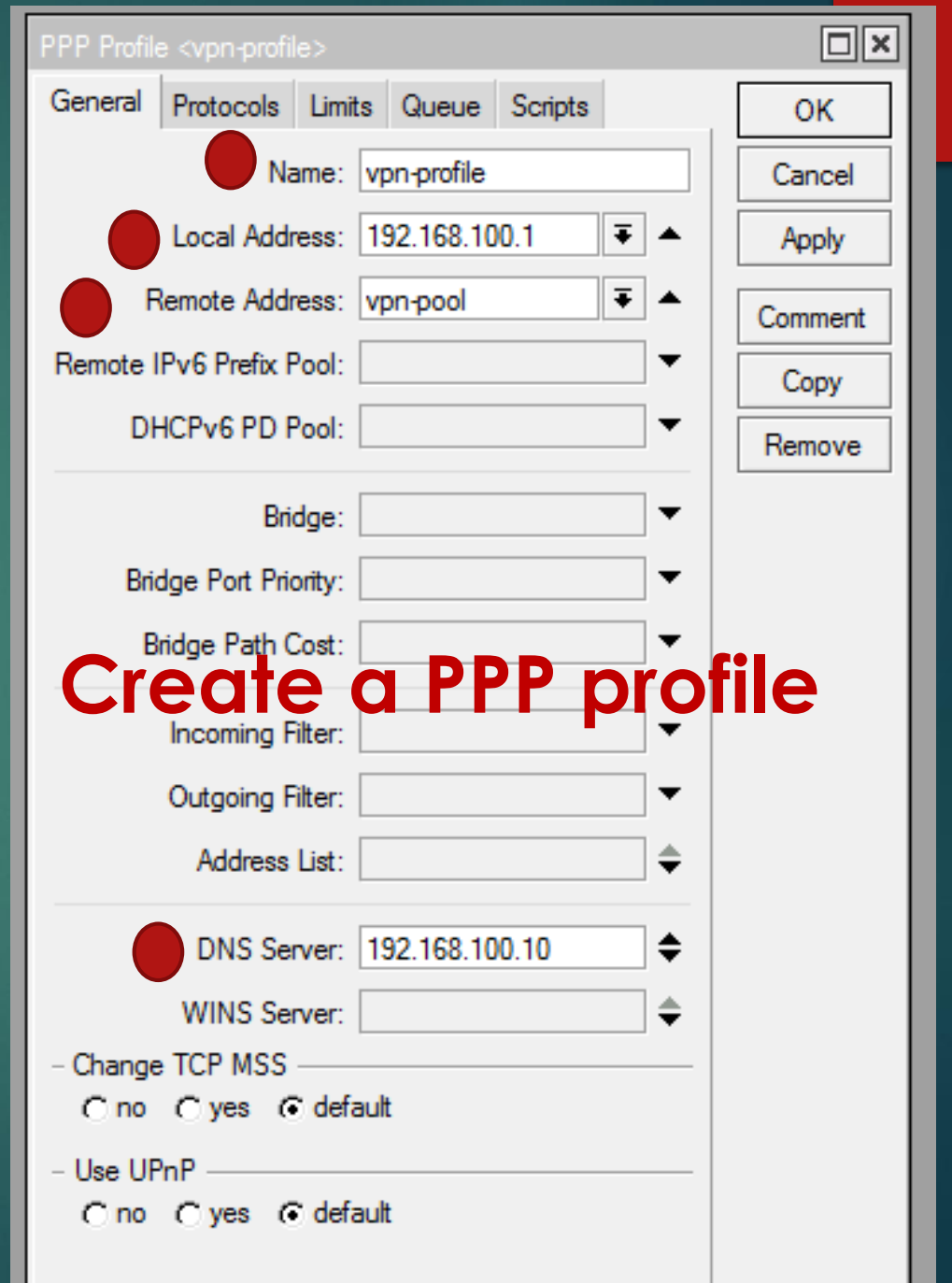
Make sure the user is member of the groups allowed to connect

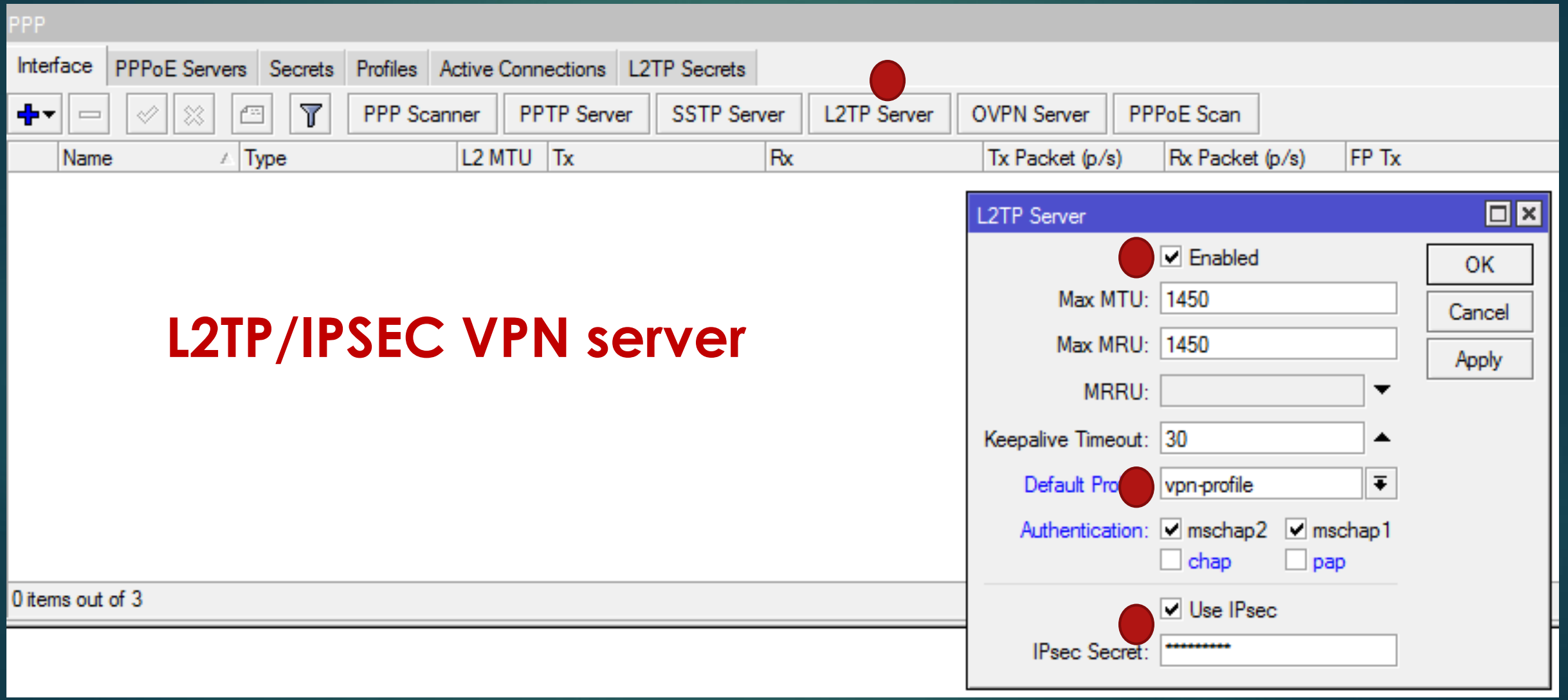
-



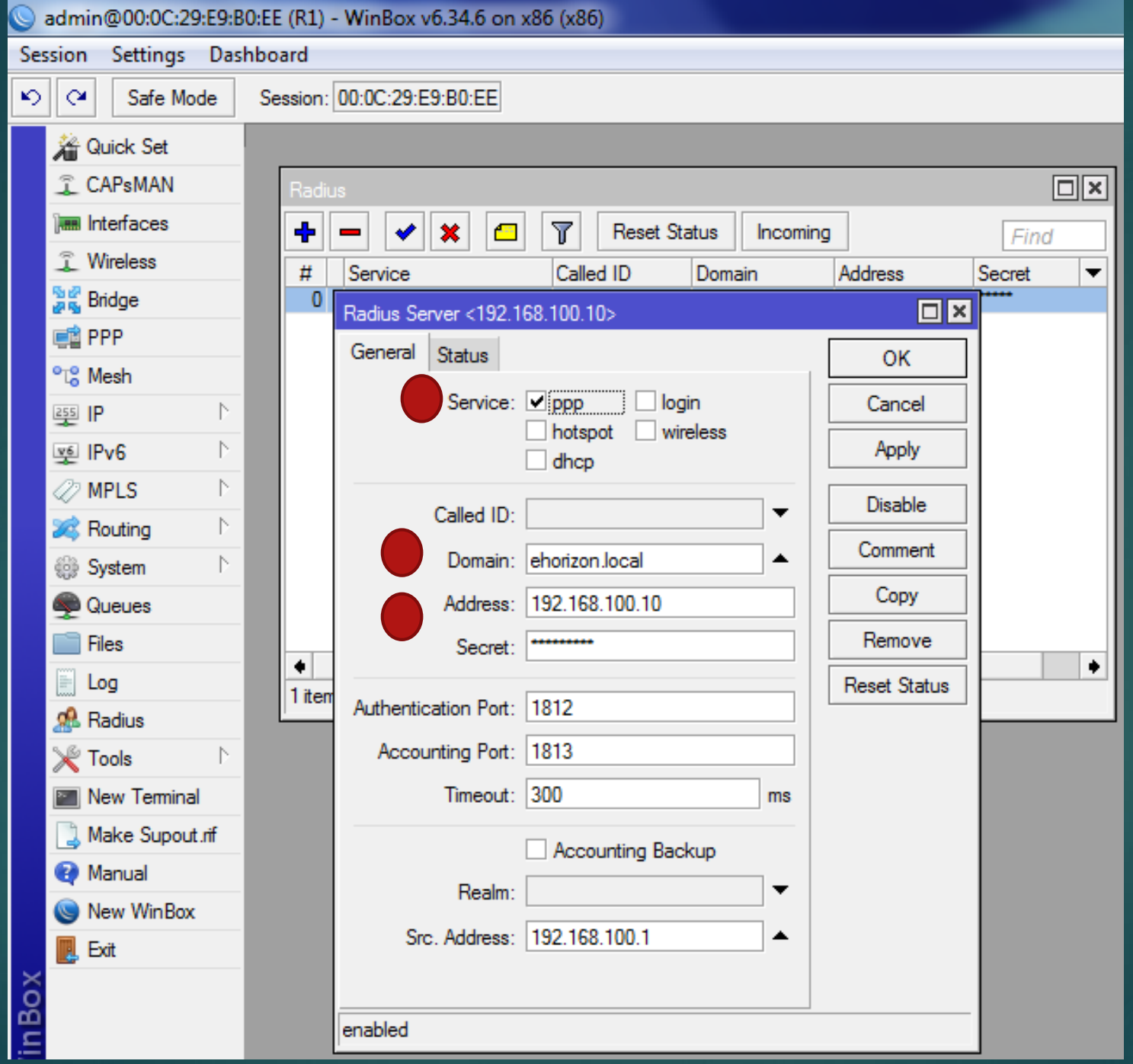
Mikrotik Router Configuration

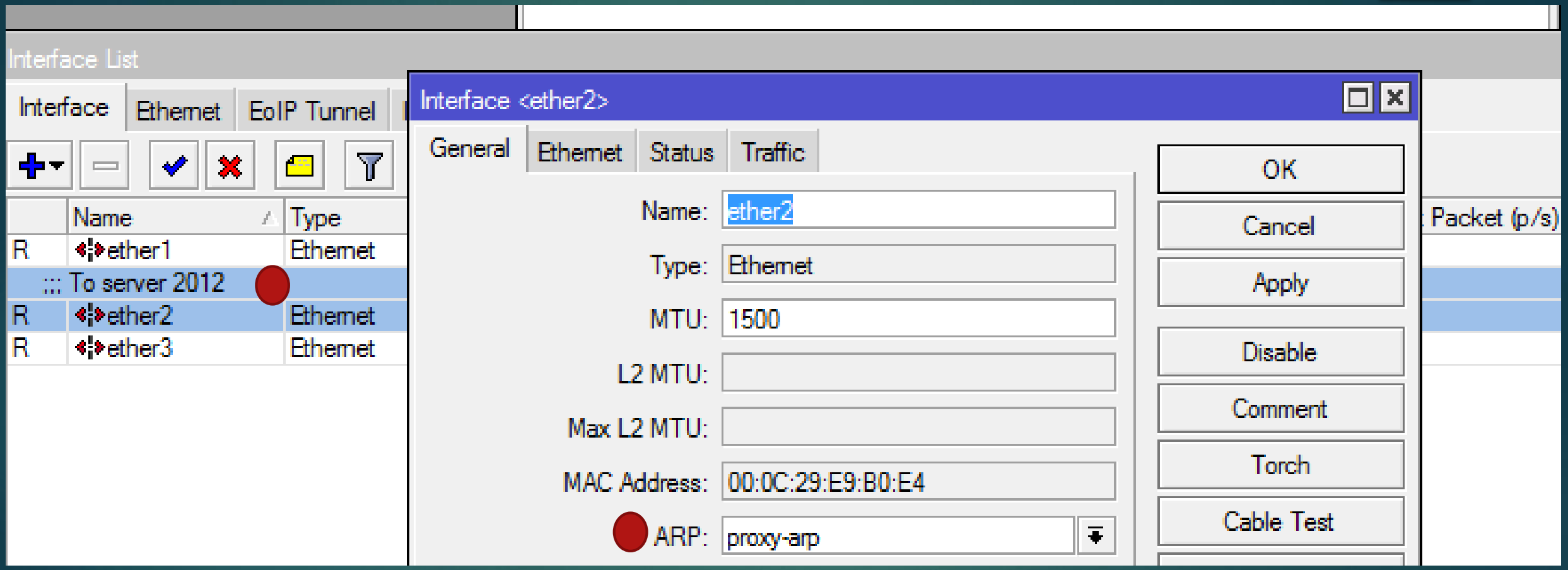

IP Pool
Pools
Used Addresses
Create IP pool
Find
Addresses
Next Pool
New IP Pool
Name: vpn-pool
Addresses: 192.168.100.200-1
Next Pool: none
OK
Cancel
Apply
Copy
Remove
0 items


PPP Profile <vpn-profile>
General
Protocols
Limits
Queue
Scripts
Name: vpn-profile
Local Address: 192.168.100.1
Remote Address: vpn-pool
Remote IPv6 Prefix Pool:
DHCPv6 PD Pool:
Bridge:
Bridge Port Priority:
Bridge Path Cost:
Incoming Filter:
Outgoing Filter:
Address List:
DNS Server: 192.168.100.10
WINS Server:
Change TCP MSS
no
yes
default
Use UPnP
no
yes
default
OK
Cancel
Apply
Comment
Copy
Remove
Create a PPP profile



L2TP/IPSEC VPN server


admin@00:0C:29:E9:B0:EE (R1) - WinBox v6.34.6 on x86 (x86)
Session
Settings
Dashboard
Safe Mode
Session: 00:0C:29:E9:B0:EE
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
New WinBox
Exit
Radius
Reset Status
Incoming
Find
Service Called ID Domain Address Secret
0
Radius Server <192.168.100.10>
General
Status
Service: ppp login hotspot wireless dhcp
Called ID:
Domain: ehorizon.local
Address: 192.168.100.10
Secret: ••••••••
Authentication Port: 1812
Accounting Port: 1813
Timeout: 300 ms
Accounting Backup
Realm:
Src. Address: 192.168.100.1
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status
enabled


Interface List
Interface
Ethernet
EoIP Tunnel
Name
Type
R
ether1
Ethernet
::: To server 2012
R
ether2
Ethernet
R
ether3
Ethernet
Packet (p/s)
Interface <ether2>
General
Ethernet
Status
Traffic
Name:
ether2
Type:
Ethernet
MTU:
1500
L2 MTU:
Max L2 MTU:
MAC Address:
00:0C:29:E9:B0:E4
ARP:
proxy-arp
OK
Cancel
Apply
Disable
Comment
Torch
Cable Test

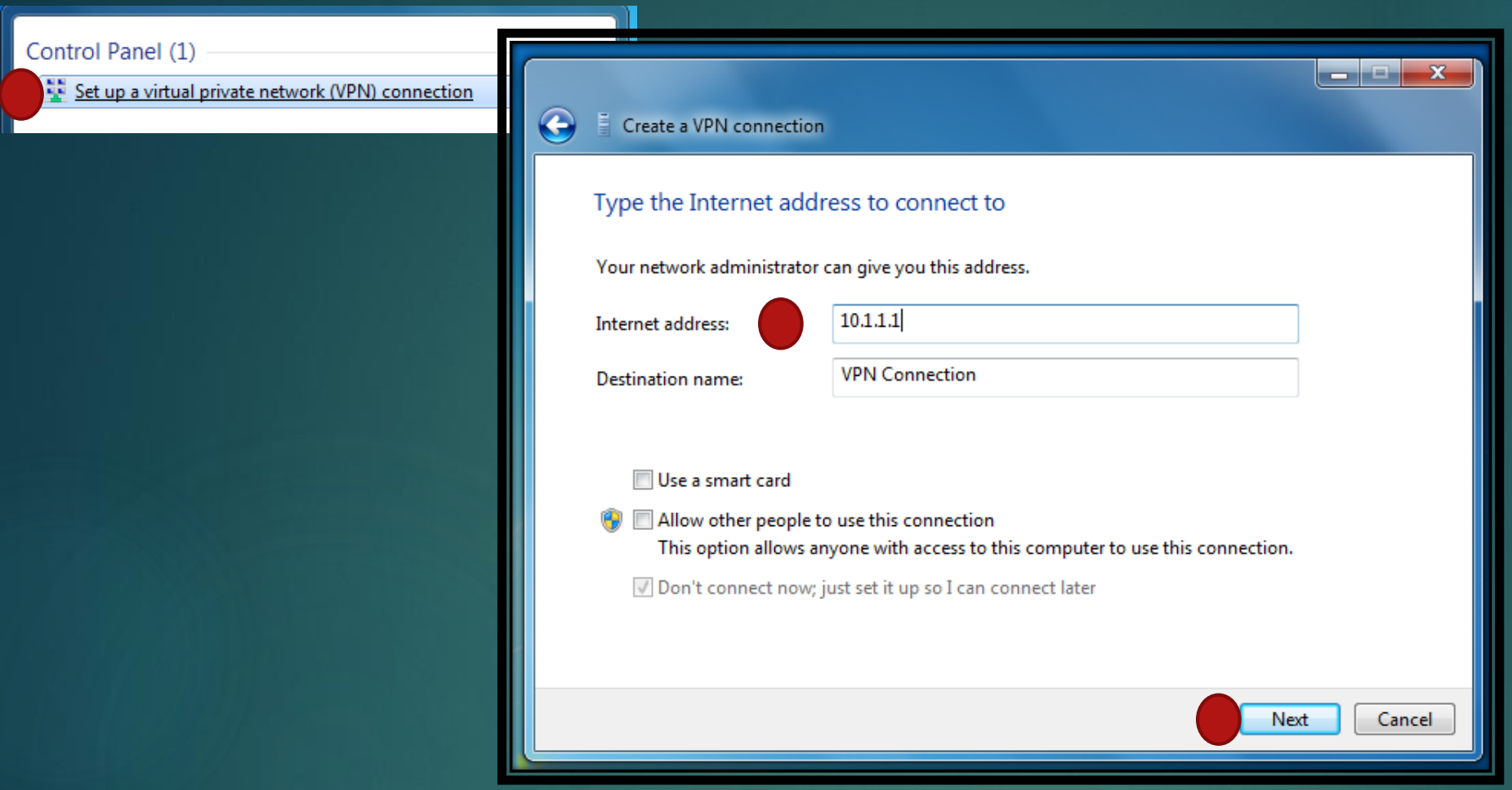
Firewall Configuration

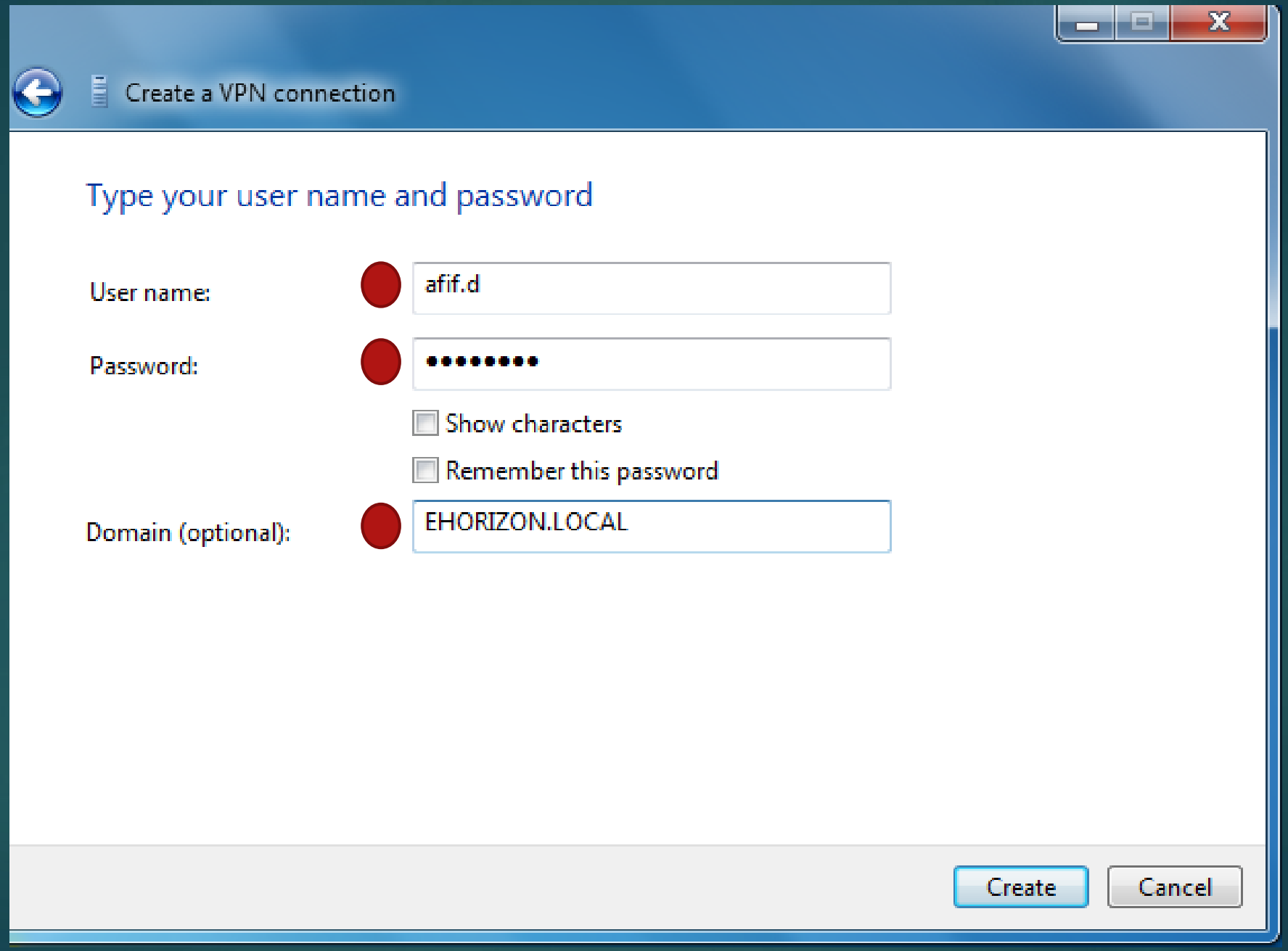
/ip firewall filter

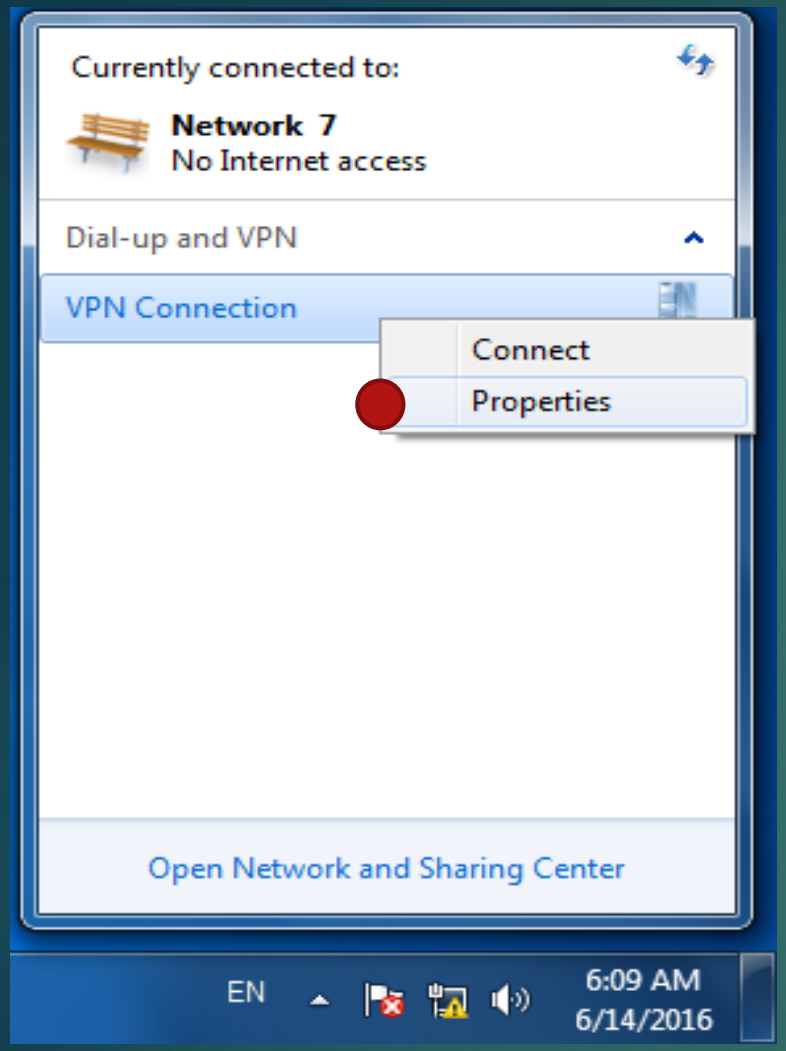
add chain=input protocol=udp port=1701,500,4500

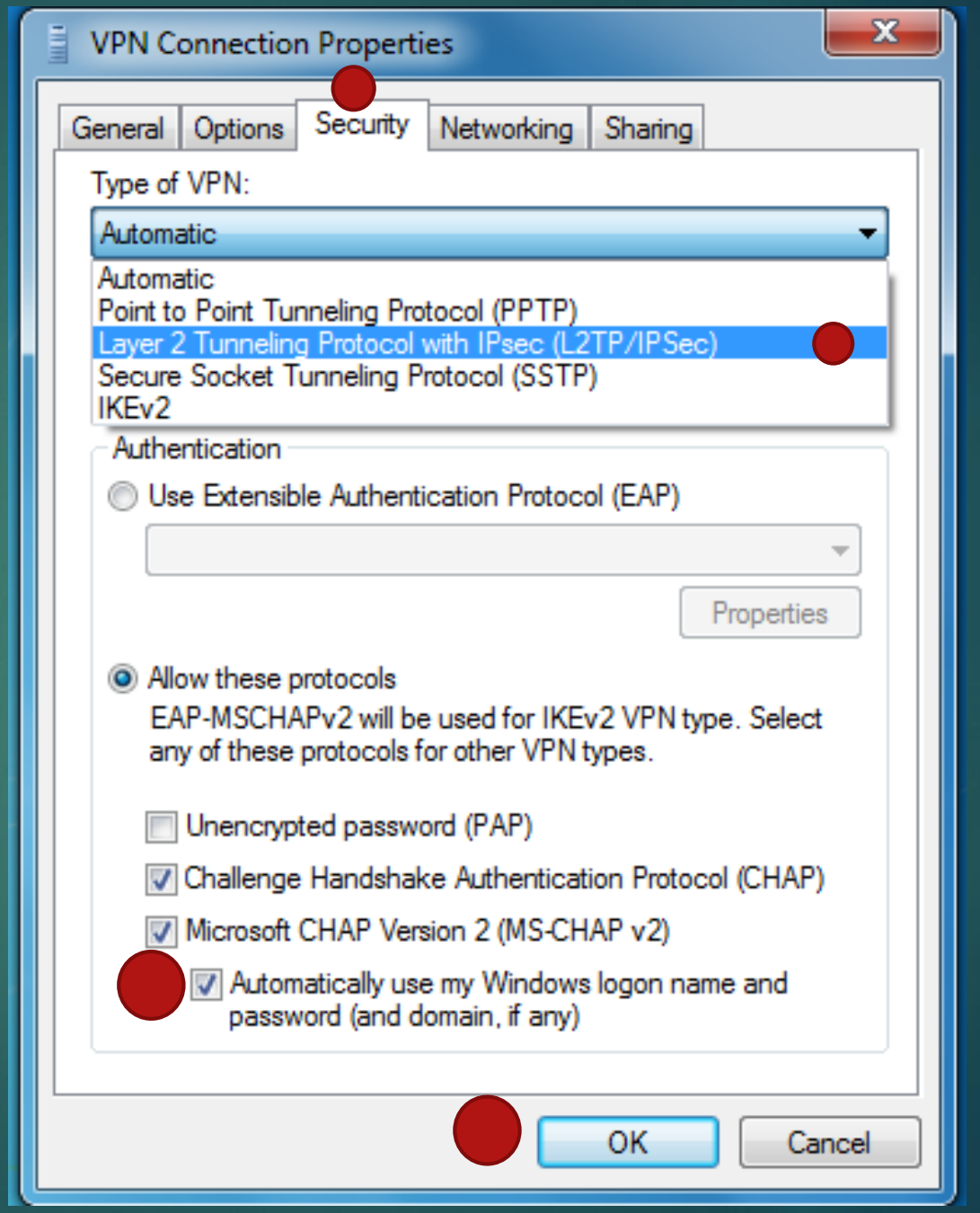
add chain=input protocol=ipsec-esp

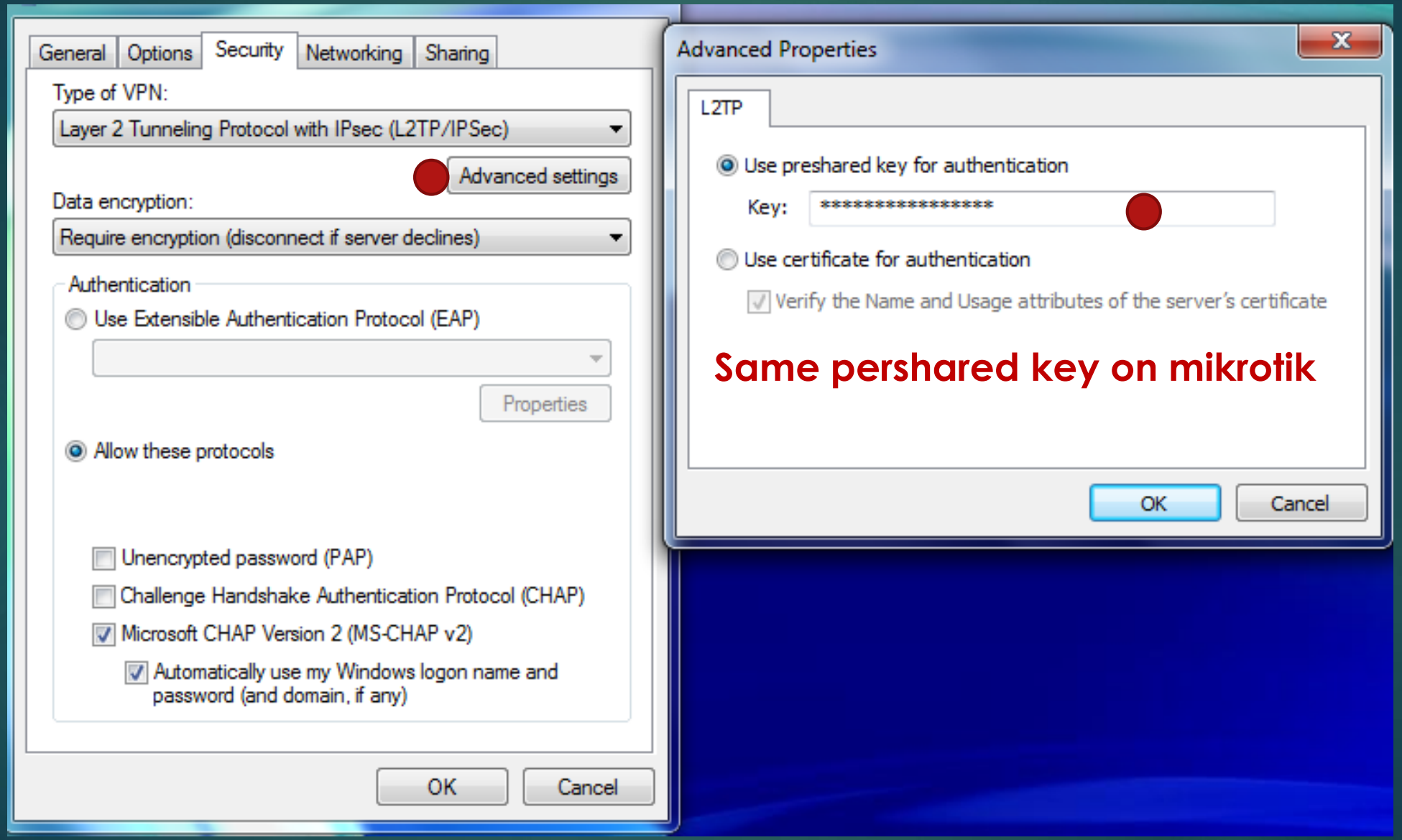
Windows VPN client configuration


Control Panel (1)
Set up a virtual private network (VPN) connection
Create a VPN connection
Type the Internet address to connect to
Your network administrator can give you this address.
Internet address:
10.1.1.1
Destination name:
VPN Connection
Use a smart card
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
Don't connect now; just set it up so I can connect later
Next
Cancel

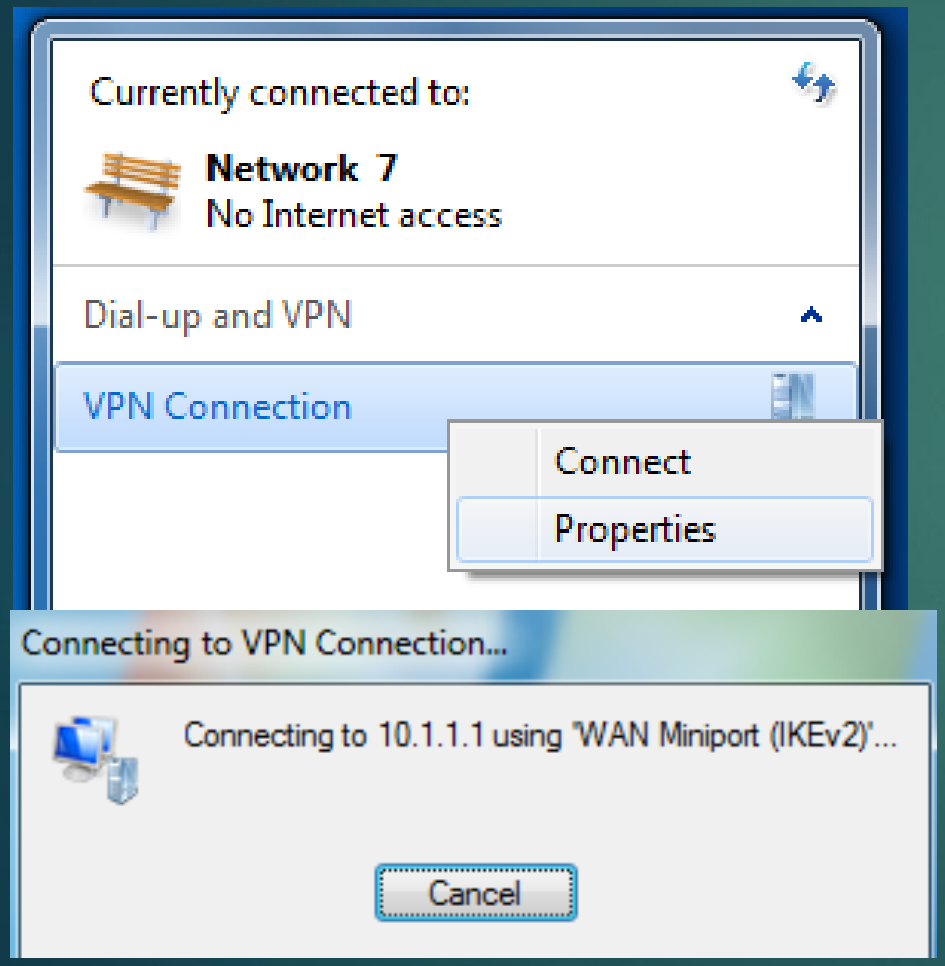

Create a VPN connection
Type your user name and password
User name:
afif.d
Password:
Show characters
Remember this password
Domain (optional):
EHORIZON.LOCAL
Create
Cancel


Currently connected to:
Network 7
No Internet access
Dial-up and VPN
VPN Connection
Connect
Properties
Open Network and Sharing Center
EN
6:09 AM
6/14/2016


VPN Connection Properties
General
Options
Security
Networking
Sharing
Type of VPN:
Automatic
Automatic
Point to Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)
Secure Socket Tunneling Protocol (SSTP)
IKEv2
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK
Cancel


General
Options
Security
Networking
Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)
Advanced settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK
Cancel
Advanced Properties
L2TP
Use preshared key for authentication
Key:
****
Use certificate for authentication
Verify the Name and Usage attributes of the server's certificate
Same pershared key on mikrotik
OK
Cancel

Verify / test

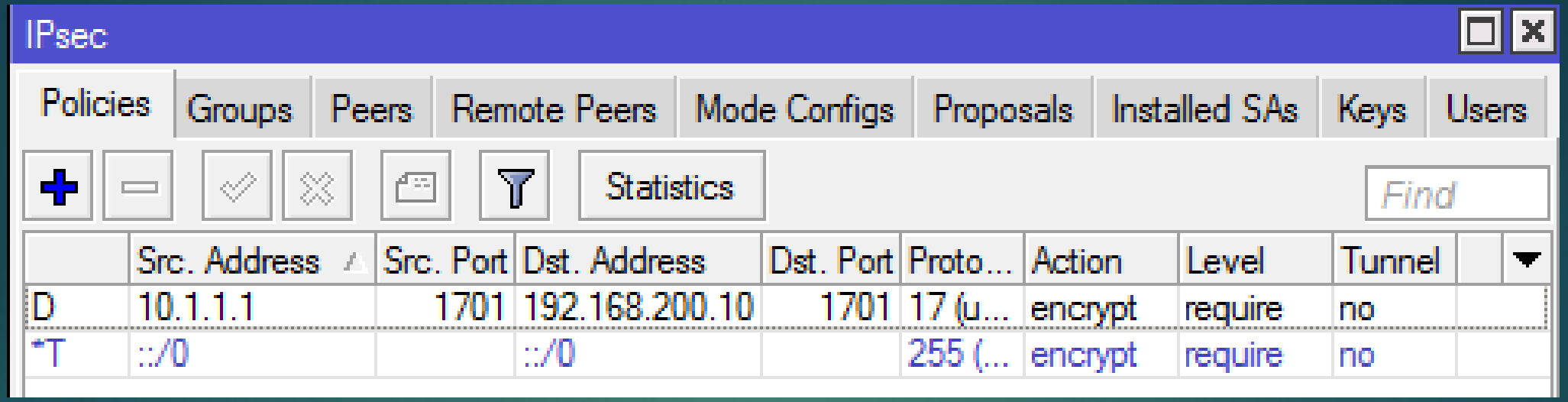


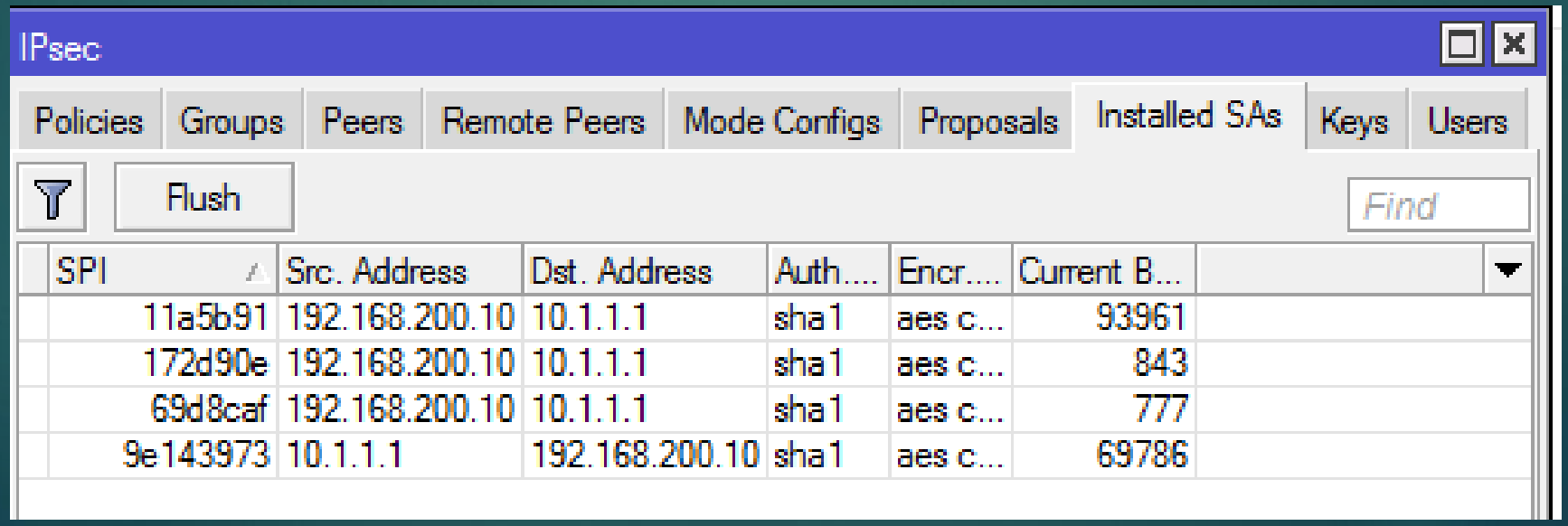
PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2TP Secrets

	Name	Service	Caller ID	Encoding	Address	Uptime
R	affif.d	l2tp	192.168.200...	cbc(aes)...	192.168.100.220	00:03:11

Verify / test


IPsec
Policies
Groups
Peers
Remote Peers
Mode Configs
Proposals
Installed SAs
Keys
Users
Statistics
Find
Src. Address
Src. Port
Dst. Address
Dst. Port
Proto...
Action
Level
Tunnel
D 10.1.1.1 1701 192.168.200.10 1701 17 (u... encrypt require no
*T ::/0 ::/0 255 (... encrypt require no


IPsec
Policies
Groups
Peers
Remote Peers
Mode Configs
Proposals
Installed SAs
Keys
Users
Flush
Find
SPI
Src. Address
Dst. Address
Auth....
Encr....
Current B...
11a5b91 192.168.200.10 10.1.1.1 sha1 aes c... 93961
172d90e 192.168.200.10 10.1.1.1 sha1 aes c... 843
69d8caf 192.168.200.10 10.1.1.1 sha1 aes c... 777
9e143973 10.1.1.1 192.168.200.10 sha1 aes c... 69786

Thank you