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
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
Select server roles

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 installed)
- 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.
1. Configure this local server
2. Add roles and features
3. Add other servers to manage
4. Create a server group

Tools:
- 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
Same secret to be set on Mikrotik Radius configuration.
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: [VN]

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]
Specify Conditions

Specify the conditions that determine whether this network policy is evaluated. At least one condition is required.

Select a condition, and then click Add.

**Groups**
- Windows Groups: The Windows Groups condition specifies that the connecting user or computer must belong to one or more groups.
- Machine Groups: The Machine Groups condition specifies that the connecting computer must belong to one or more machine groups.

**User Groups**
- User Groups condition specifies that the connecting user must belong to one of the selected groups.

**Location Groups**
- Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) Location Groups condition, which requires the Host Credential Authorization Protocol (HCAP) to match this policy. The HCAP protocol is used for communication between NPS and some network access servers (NASes). See your NAS documentation before using this condition.

Select Group

Select this object type:
- Group

From this location:
- Horizon local

Enter the object name to select (examples):
- vpn user

Advanced... OK Cancel

Add Groups... OK Cancel
VPN Properties

Overview

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
- 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
Make sure the user is member of the groups allowed to connect.
Mikrotik Router Configuration
Create IP pool

Create a PPP profile
L2TP/IPSEC VPN server
Firewall Configuration

/ip firewall filter
add chain=input protocol=udp port=1701,500,4500
add chain=input protocol=ipsec-esp
Windows VPN client configuration
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
- Don’t connect now, just set it up so I can connect later

Next  Cancel
Type your user name and password

User name:  afif.d

Password:  

- Show characters
- Remember this password

Domain (optional):  EHorizon.Local
Same pershared key on mikrotik
Verify / test
Verify / test
Thank you