



<https://www.mikrotraining.ro>

MikroTik RouterOS IPsec VPN with RADIUS client & Windows 2016 Server NPS backend

MIKROTIK USER MEETING
BUCHAREST – ROMANIA, OCTOBER 29, 2018

PRESENTED BY:
DANIEL TUREAN - MIKRO TRAINING SRL

About me - Daniel Turean

- Over 18 years experience in Information Technology of which 10 years in Computer Networks
- 2007 –2010 Nortel Networks beta tester
- Cisco CCNA certified since 2013
- 2012 – Started working with MikroTik RouterOS and becoming MTCNA in 2015
- Currently Certified for MTCRE, MTCWE, MTCTCE and IPv6E
- 2016 – Founded Mikro Training SRL and become MikroTik Certified Trainer no:364
- MikroTik Certified Consultant on a variety of topics based on MikroTik RouterOS.

<https://www.mikrotraining.ro>

Agenda, technical details and implementation steps

- General information about IPsec implementation in MikroTik RouterOS
- General information regarding RADIUS Client implementation in MikroTik RouterOS
- RouterOS IPsec related option settings
- RouterOS typical IP firewall settings for IPsec tunnels
- Preparing and configuring Microsoft Windows Server 2016 NPS role to provide RADIUS Server services to MikroTik RouterOS road warriors VPN Clients.
 - Configuring the ShrewSoft VPN software client for roadwarriors.
 - Configuring the Android mobile phone for using IPsec Xauth PSK

Why IPsec?

- Provides US DoD (Department of Defense) encryption strength
- Ability to mitigate many network threats like:
 - Data theft in transit
 - Credentials sniffing in transit
 - Network based attacks
- Provides Confidentiality, Integrity and Authentication
- Cross Vendor support, IETF standard
- GDPR? ... Privacy by design!!!

General information about IPsec implementation in MikroTik RouterOS

- IPsec represents the set of protocols defined by IETF to provide secure transport means of sensitive data over untrusted networks.
 - Can be divided in 3 categories
 - IKE (Internet Key Exchange) Provides authenticated keying material for ISAKMP framework. Uses port UDP 500
 - AH (Authentication Header) RFC 4302 Provides authentication and integrity (no encryption) by hashing entire packet (header + payload). Uses AH IP protocol 51 and it is incompatible with NAT!
 - ESP (Encapsulating Security Payload) RFC 4303 Provides confidentiality, authentication and integrity by encrypting the payload but leaving the IP header intact, thus surviving through NAT*. Uses ESP IP protocol 50 or UDP 4500 for NAT-T.

* NAT-T is required to pass portless IP protocol 50 through NAT

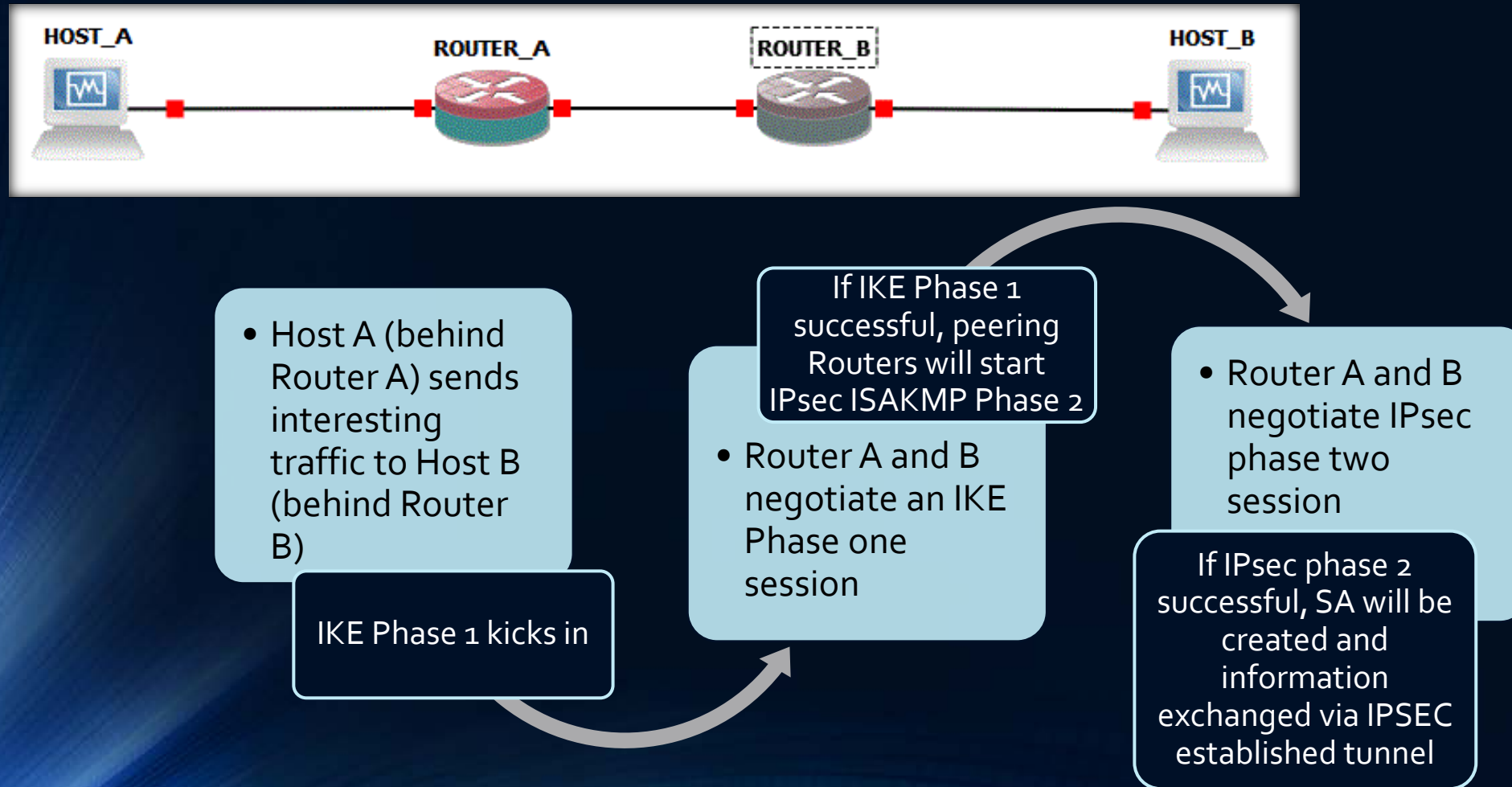
Internet Key Exchange

- Has two phases
 - **Phase 1 – IKE** Peers agree and settles for the keying material used to derive the keys for all SAs
 - **Phase 2 – IPsec (ISAKMP)** Peers establish one or more SA (depending on the unique or required option) that will be used to actually encrypt data

Note: RouterOS also supports IKEv2

Phase 1 IKE	Phase 2 IPsec
Auth Method	Ipsec Protocol
DH Group	Mode (Tun or Tap)
Encryption algorithm	Auth Method
Exchange mode	PFS (DH group)
Hash algorithm	Lifetime
NAT-T	
DPD and Lifetime	

IPsec IKE Security Association establish



Encapsulating Security Payload

USES SHARED KEYS FOR PROVIDING ENCRYPTION

ESP Header/TRANSPORT Mode – existing between Original IP header and Payload data.



ESP Header/TUNNEL Mode – Changes the position compared to TRANSPORT Mode, providing confidentiality to Original IP header as well.



Encryption algorithms available in RouterOS

AUTHENTICATION

- MD5 - **Obsolete**
- SHA1 - somewhat obsolete
- SHA2 (256, 512) - Recommended

ENCRYPTION

- DES/3DES - **Obsolete**
- AES - 128, 256 bit keys CBC/GCM
- Blowfish
- Twofish
- Camellia - 128, 192 and 256 bit key

IKEv1 & IKEv2 comparison

IKE VERSION 1

How many Exchange messages

- 9 messages in Main Mode
- 6 messages in Aggressive Mode

PEER enforcement on Lifetime

Remote Access VPN NOT defined, implementation is by vendor specific,

- ModeConf
- XAUTH

IKE VERSION 2

How many Exchange messages

- Only 4 messages
- No Exchange modes (only 1 mode)

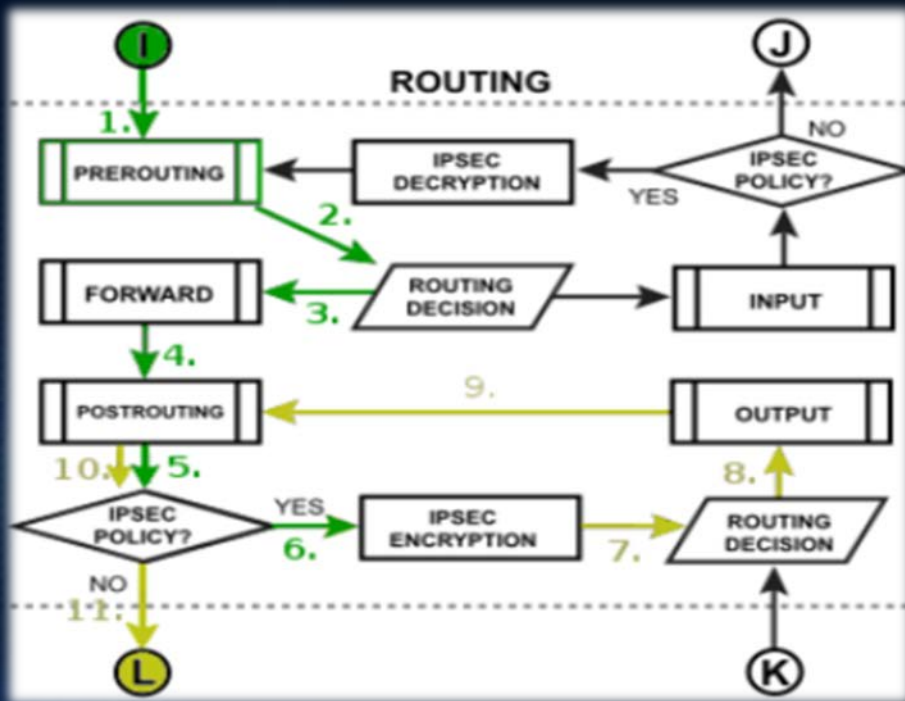
Lifetime NOT negotiated, each peer can delete SAs anytime by exchanging DELETE payloads

Remote Access VPN by default

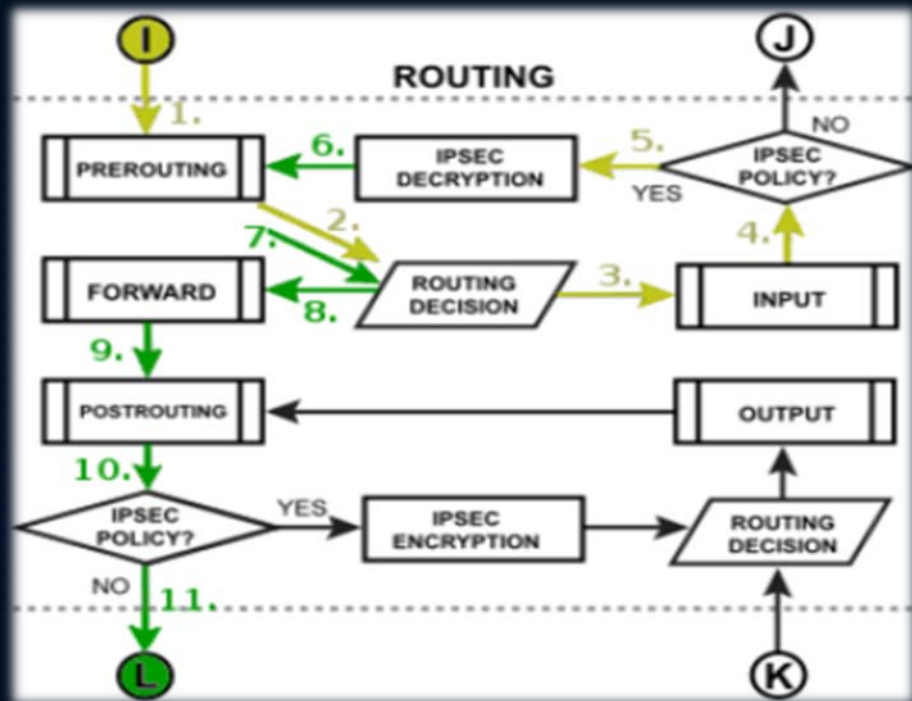
- EAP
- User authentication over EAP

Packet flow - IPsec

ENCRYPTION



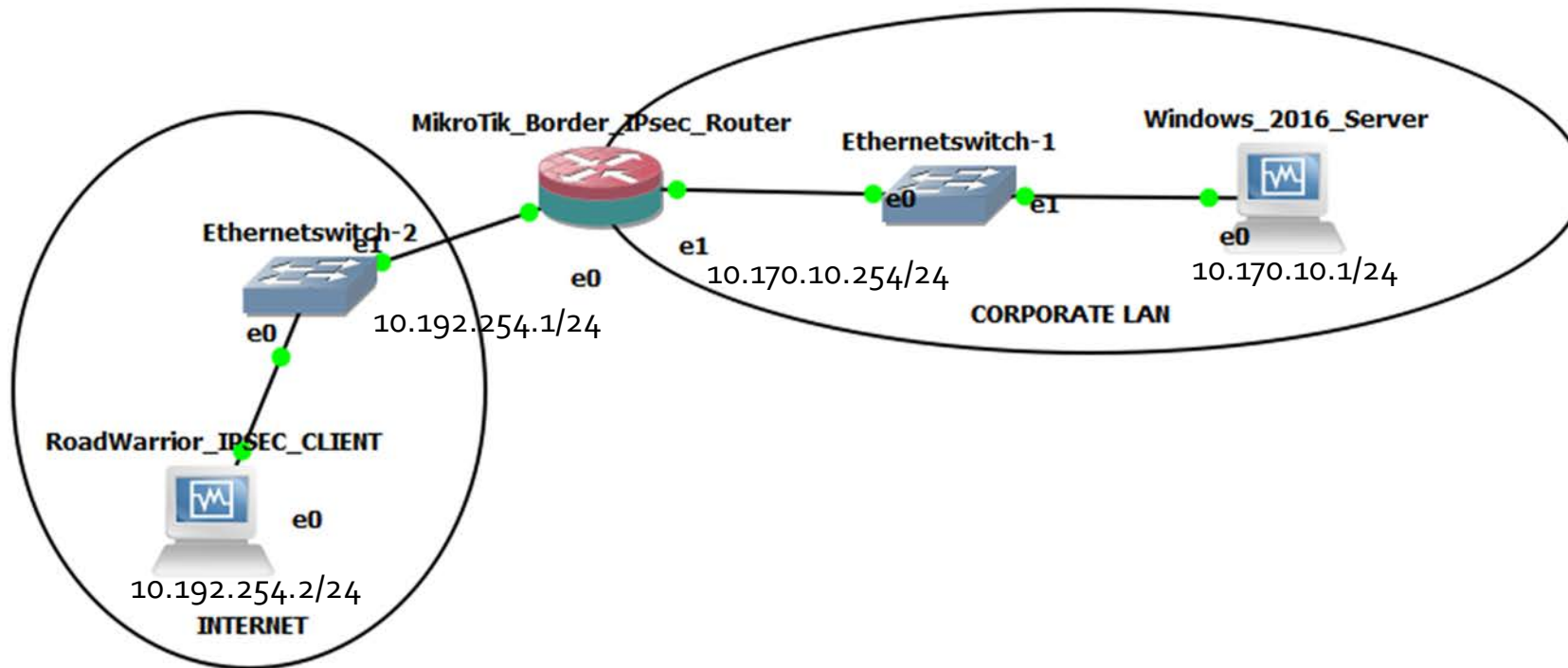
DECRYPTION



MikroTik RouterOS RADIUS Client

- Supports IPsec authentication along with other options like PPP, hotspot, wireless etc.
- Implements standard RADIUS RFC 2865 and it is compatible with FreeRADIUS, XTRadius or similar servers.
- **Current limitation:** only PAP is supported for RouterOS RADIUS Ipsec
- Windows 2016 Server must have the NPS role configured in PAP mode

LAB topology and presentation scenario

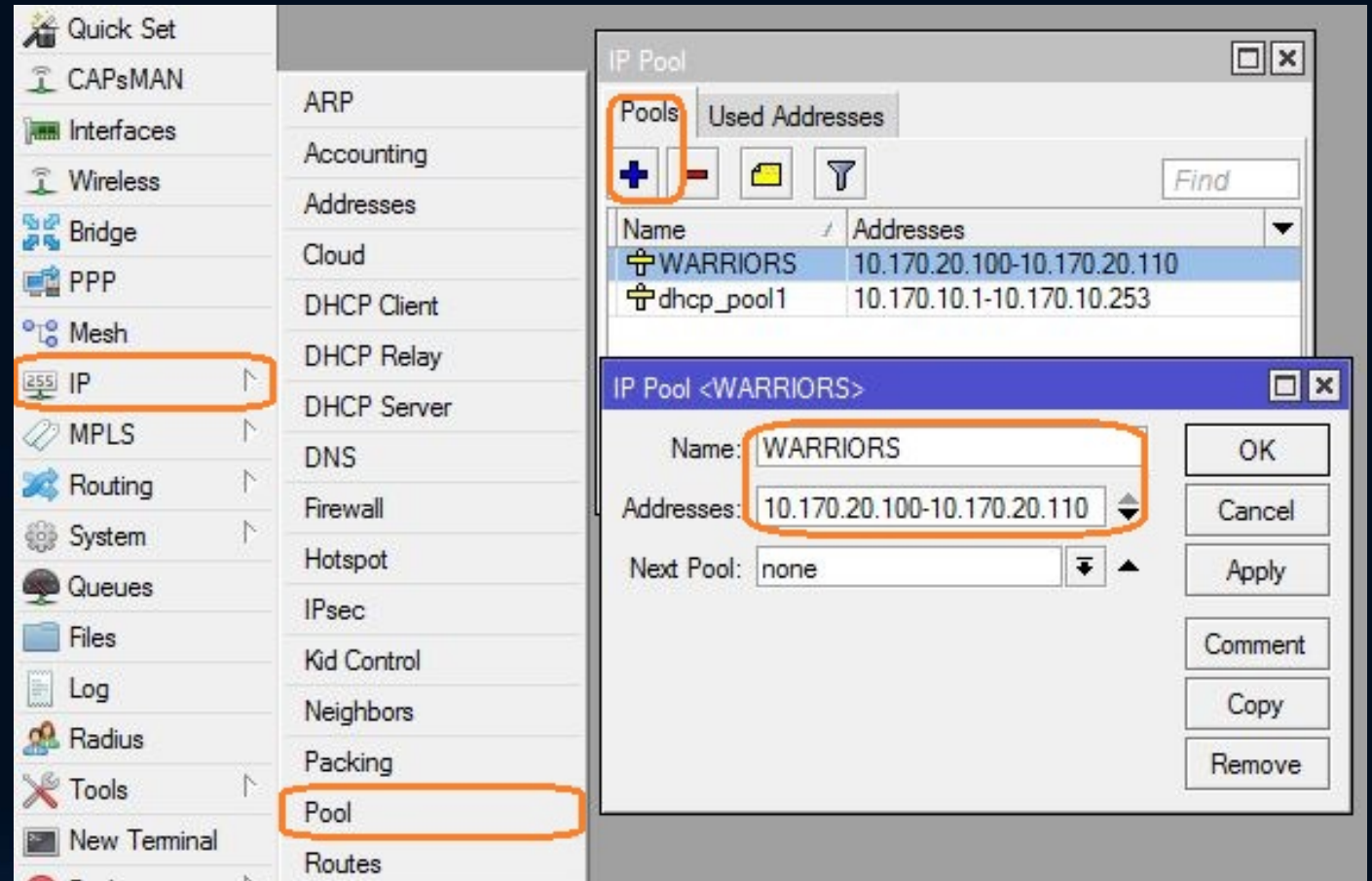


RouterOS IPsec related option settings

Pool

- Step 1 – Create an IP Pool for later use in IPsec Policy in order to assign IP addresses to IPsec VPN road warriors

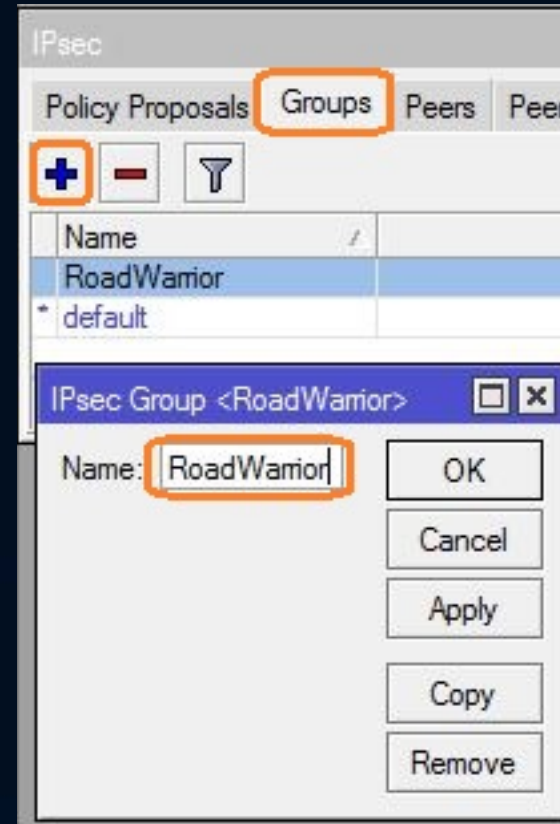
Note: RouterOS already has the standard required configuration



RouterOS IP IPsec menu option settings

Groups

- Step 2 – Configure RoadWarrior Group that will later be invoked in the Policy template
- Starting with this slide, all remaining settings are done in IP > IPsec menu



RouterOS IP IPsec menu related option settings

Policies General

- Step 3 – Policies configuration in Template mode, Src Address representing the local subnet and Dst. Address, the remote roadwarrior subnet
- We need Template option enabled because we do not know the public IP that the client will use to initiate the IKE session

IPsec

Policies Policy Proposals Groups Peers Peer Profiles Remote Peers

+ - ✓ ✗ 📁 🗑️

#		Src. Address	Src. Port	Dst. Address
0	X*T	::/0		::/0
1	T	10.170.10.0/24		10.170.20.0/24

IPsec Policy <10.170.10.0/24:0>10.170.20.0/24:0>

General Action Status

Src. Address: 10.170.10.0/24

Src. Port: ▾

Dst. Address: 10.170.20.0/24

Dst. Port: ▾

Protocol: 255 (all) ▾

☒ Template

Group: RoadWarrior ▾

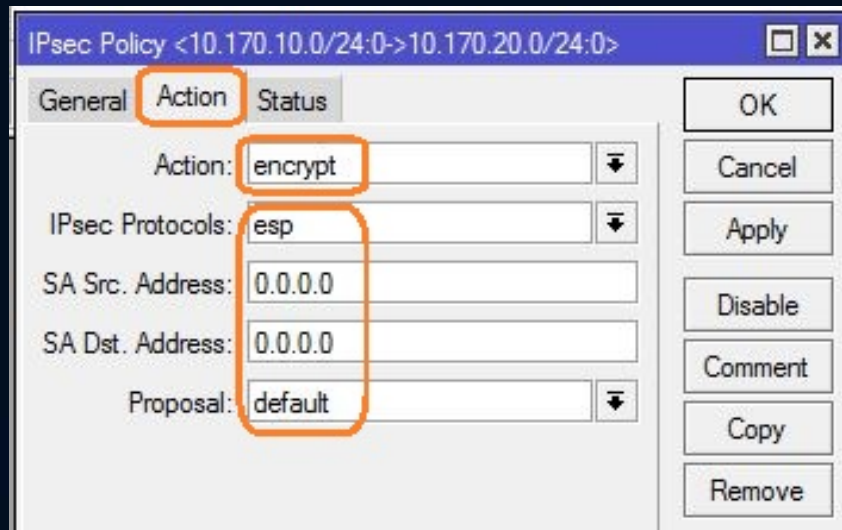
OK Cancel Apply Disable Comment Copy Remove

enabled Template Active

RouterOS IP IPsec menu option settings

Policies Action

- Step 4 – Policy Action tab is where we need to select the Action as encrypt
- IPsec protocol should be set as esp
- SA Src and Dst addresses remain unspecified to match clients connecting from anywhere
- Proposal is the default one following in the next slide



RouterOS IP IPsec menu related option settings

Proposals

- Step 5 – Proposals can be named profiles where we declare Phase2 settings
- In our case we have edited the default policy proposal with following
 - Authentication sha1
 - Encryption aes-128 cbc (cypher block chain)
 - Lifetime of 1 hour

IPsec

Policies **Policy Proposals** Groups Peers Peer Profiles Remote Peers

+ - ✓ ✗ Filter Statistics

Name	Auth. Algorithms	Encr. Algorithms	Lifetime
default	sha1	aes-128 cbc	01:00:00

IPsec Policy Proposal <default>

Name: default

Auth. Algorithms: ☐ md5 ☒ sha1 ☐ sha256 ☐ sha512 ☐ null

Encr. Algorithms: ☐ null ☒ aes-128 cbc ☐ aes-256 cbc ☐ aes-192 cbc ☐ aes-128 ctr ☐ aes-256 ctr ☐ aes-192 ctr ☐ aes-128 gcm ☐ aes-256 gcm ☐ aes-192 gcm ☐ des ☐ twofish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256

Lifetime: 01:00:00

PFS Group: none

enabled default

OK Cancel Apply Disable Copy Remove

RouterOS IP IPsec menu related option settings

Peer profiles

- Step 6 – Peer profiles are used to create Peer Phase1 encryption settings
- In our case we have edited the default peer profile, same as for the policy proposal at step 5 with settings as follow:
 - Sha1, aes-128 , modp 1024
 - Lifetime 1 day
 - NAT-T enabled

The screenshot shows the 'IPsec Peer Profile <default>' configuration window. The 'Peer Profiles' tab is selected in the top menu. The 'default' profile is highlighted in the table below the tabs.

Name	Hash Algorithms	Encryption Algorithm	DH Group
default	sha1	aes-128	modp1024

The configuration details for the 'default' profile are as follows:

- Name: default
- Hash Algorithms: sha1
- Encryption Algorithm: ☒ aes-128, ☐ aes-192, ☐ aes-256, ☐ camellia-128, ☐ camellia-192, ☐ camellia-256, ☐ 3des, ☐ blowfish
- DH Group: ☒ modp1024, ☐ modp768, ☐ ec2n155, ☐ ec2n185, ☐ modp1536, ☐ modp2048, ☐ modp3072, ☐ modp4096, ☐ modp6144, ☐ modp8192, ☐ ecp256, ☐ ecp384, ☐ ecp521
- Proposal Check: obey
- Lifetime: 1d 00:00:00
- Lifeyes: (empty)
- ☒ NAT Traversal
- DPD Interval: disable DPD
- DPD Maximum Failures: 5

RouterOS IP IPsec menu related option settings

Peers

- Step 7 – Peers General tab provides settings for IPsec Peer, leaving the Address field as 0.0.0.0/0
- Profile is the default one configured at step6
- Authentication method is pre shared key Xauth
- Exchange mode main with passive mode

IPsec

Groups Peers Peer Profiles Remote Peers Mode Configs Installed SAs

+ - ✓ ✗ 📁 🔍

#	Address	Port	Auth. Method	Exchange ...
0 R	0.0.0.0/0		pre shared key xauth	main

IPsec Peer <0.0.0.0/0>

General Advanced

Address: 0.0.0.0/0

Port: 0

Local Address:

Profile: default

Auth. Method: pre shared key xauth

Exchange Mode: main

☒ Passive

Secret: *****

XAuth Login:

XAuth Password:

OK Cancel Apply Disable Comment Copy Remove

enabled responder

RouterOS IP IPsec menu related option settings

Peers

- Step 8 – Peers Advanced tab configures Policy Template Group created at step2
- Mode Config is the one we will create in the next slide
- Generate Policy should have port strict option selected

The screenshot shows the 'IPsec' configuration window with the 'Peers' tab selected. A table lists peers, with the first entry '0 R 0.0.0.0/0' selected. Below the table, the 'IPsec Peer <0.0.0.0/0>' configuration window is open, showing the 'Advanced' tab. The following settings are highlighted with orange boxes:

- Policy Template Group: RoadWarrior
- Mode Configuration: IPSEC-RW
- Generate Policy: port strict

Other visible settings include:

- Notrack Chain: (empty)
- ☐ Send Initial Contact
- My ID Type: auto
- Compatibility Options: ☐ skip peer id validation

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom, the status is 'enabled' and 'responder'.

RouterOS IP IPsec menu related option settings

Mode Configs

- Step 9 – Mode Configs tab configures ModeCfg options to be used at previous step8
- Responder must be enabled
- Must point to Address Pool created in IP Pool at 1st step
- Address prefix length represents the subnet size to be allocated to VPN clients
- Split Include represents the destinations reachable through the IPsec tunnel

IPsec

Groups Peers Peer Profiles Remote Peers **Mode Configs**

+ - Y

Name	Respo...	Address Pool	Address Pref
IPSEC-RW	yes	WARRIORS	

IPsec Mode Config <IPSEC-RW>

Name: IPSEC-RW

☒ Responder

Address Pool: WARRIORS

Address Prefix Length: 24

Split Include: 10.170.10.0/24

☐ System DNS

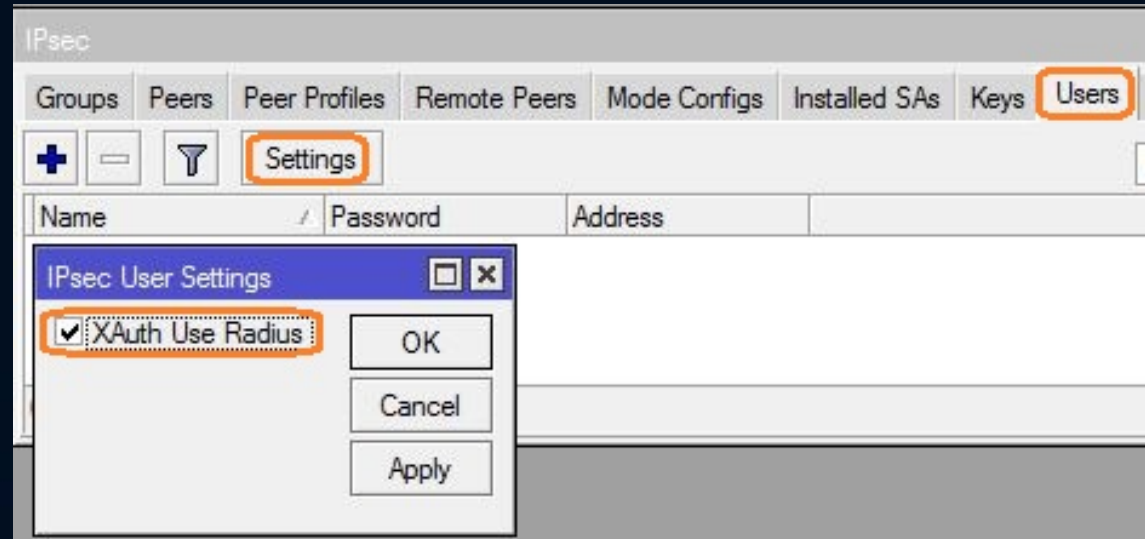
Static DNS:

OK Cancel Apply Copy Remove

RouterOS IP IPsec menu related option settings

Users

- Step 10 – Our last step in IPsec settings is the Users Tab, where we can manually create users for Extended Authentication mode but, we are not going to!
- Instead, we will enable Xauth Use RADIUS option in the Settings button in order to query the Microsoft Active Directory database for username and credentials



RouterOS RADIUS Client related settings

- Step 11 - Last step is to actually configure the RADIUS Client used to query Active Directory for user credentials
- We need to enable the ipsec service for the configured RADIUS client and mention the IP address where RADIUS Server can be reached (Active Directory in our case), and also the shared secret

The screenshot shows the RouterOS WinBox interface. On the left is a sidebar menu with various system settings. The 'Radius' option is highlighted with an orange box. The main window displays the 'Radius' configuration page for a client named 'Radius Server <10.170.10.1>'. The 'General' tab is selected and highlighted with an orange box. Within this tab, the 'Service' section has the 'ipsec' checkbox checked and highlighted with an orange box. The 'Address' field is set to '10.170.10.1' and is also highlighted with an orange box. Other fields include 'Called ID', 'Domain', 'Secret' (masked with asterisks), 'Authentication Port' (1812), 'Accounting Port' (1813), 'Timeout' (300 ms), 'Accounting Backup' (unchecked), 'Realm', and 'Src. Address' (0.0.0.0). Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Reset Status' are visible on the right side of the configuration window.

#	Service	Called ID	Domain	Address
1	ipsec			10.170.10.1

RouterOS typical IP Firewall settings for IPsec tunnels

- IPsec gets more complicated if Fasttrack is used
- We need to make sure to allow ESP IP protocol 50 on the Input chain
- We need to make sure to allow UDP 500
- We need to make sure to allow UDP 4500 for NAT-T
- We also need to prevent IPsec destined traffic from being src-NATed (placed above src-NAT rule)

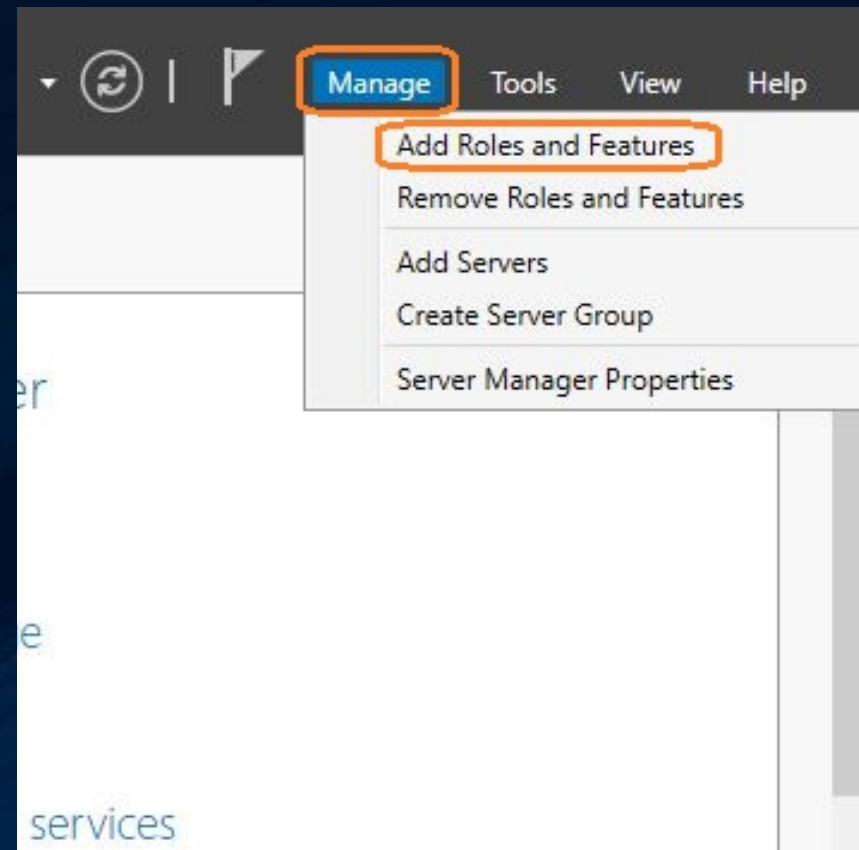
```
/ip firewall filter
add action=drop chain=input comment="DROP INVALID INPUT" connection-state=invalid in-interface=WAN
add action=drop chain=forward comment="DROP INVALID FORWARD" connection-state=invalid in-interface=WAN
add action=accept chain=forward comment="ACCEPT IPSEC ESTABLISHED TRAFFIC" connection-state="" dst-address=\
10.170.20.0/24 src-address=10.170.10.0/24
add action=accept chain=forward comment="ACCEPT IPSEC ESTABLISHED TRAFFIC" connection-state="" dst-address=\
10.170.10.0/24 src-address=10.170.20.0/24
add action=drop chain=forward in-interface=WAN
add action=accept chain=input dst-port=500 in-interface=WAN protocol=udp
add action=accept chain=input dst-port=4500 in-interface=WAN protocol=udp
add action=accept chain=input in-interface=WAN protocol=ipsec-esp
add action=drop chain=input in-interface=WAN
```

```
/ip firewall nat
add action=accept chain=srcnat dst-address=10.170.20.0/24 src-address=10.170.10.0/24
```

Preparing and configuring Microsoft Windows Server 2016 – Network Policy Server role

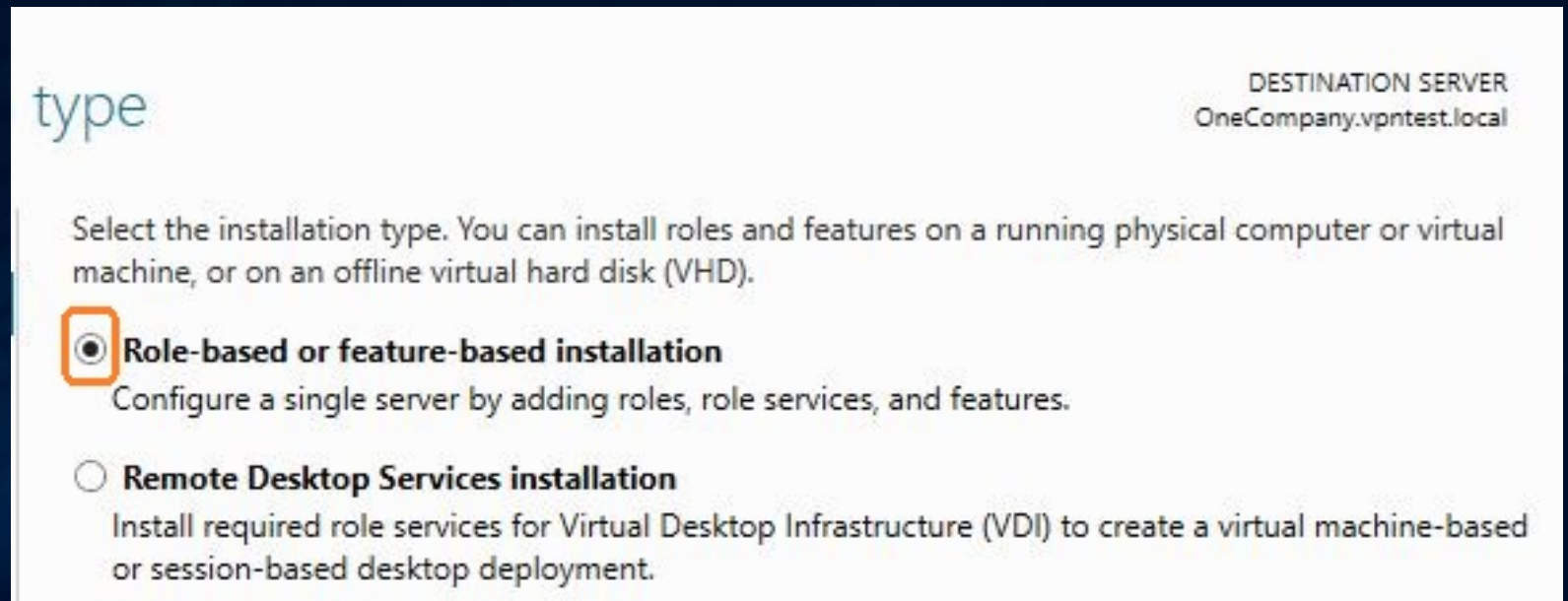
- One easy way to access the Add Roles and Features wizard is using the Server Manager in Windows Server 2016
- We will use it to add the Network Policy Server role detailed in the next slides

Note: Active Directory role is considered as already installed



Preparing and configuring Microsoft Windows Server 2016 – Network Policy Server role

- We should select Role-based or feature-based installation and select Next



type

DESTINATION SERVER
OneCompany.vpntest.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Preparing and configuring Microsoft Windows Server 2016 – Network Policy Server role

- We should leave the selection as default and go to Next menu

server DESTINATION SERVER
OneCompany.vptest.local

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
OneCompany.vptest.lo...	10.170.10.1	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel

Preparing and configuring Microsoft Windows Server 2016 – Network Policy Server role

- We should select Network Policy and Access Services and continue with Next menu

DESTINATION SERVER
OneCompany.vptest.local

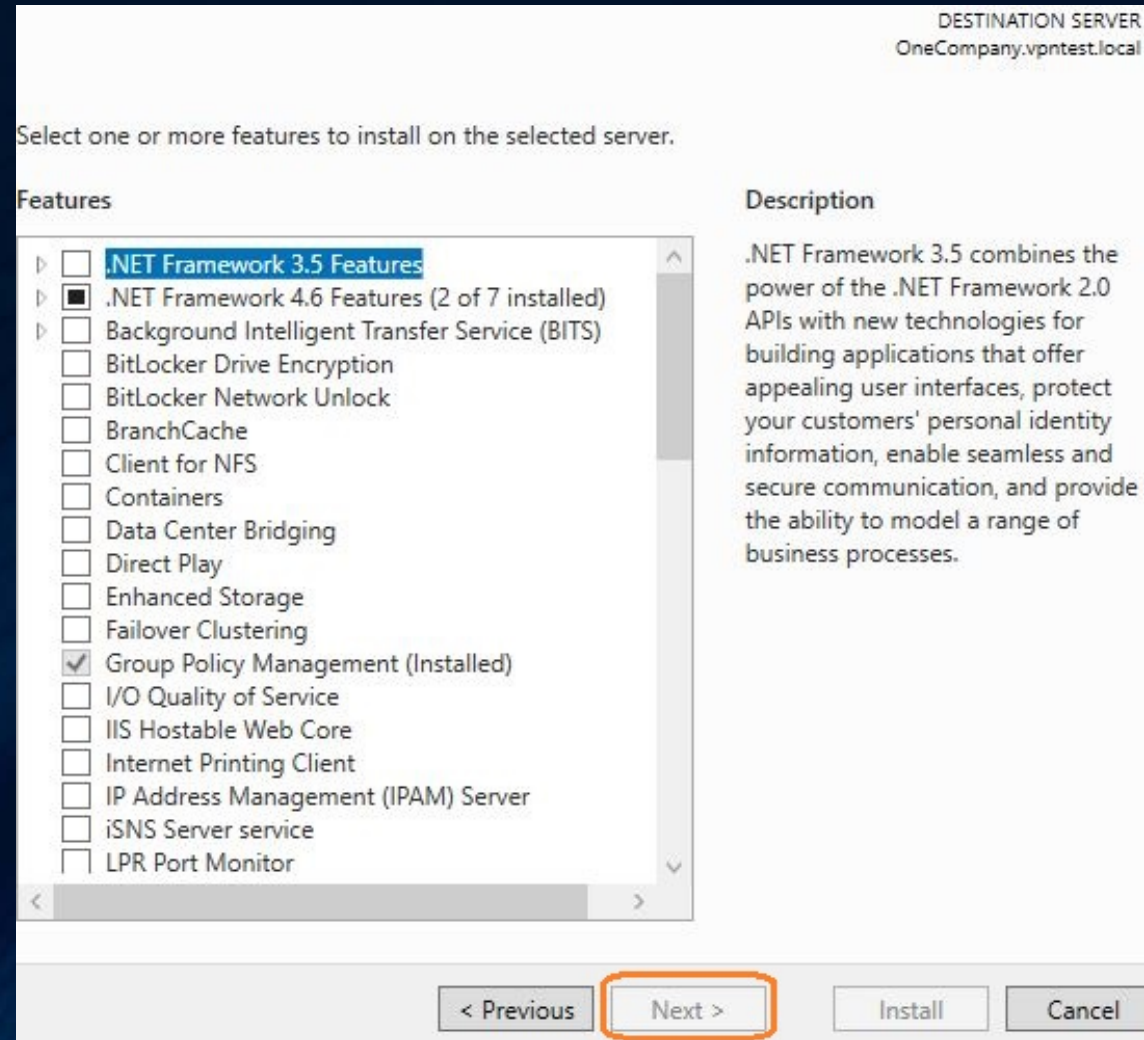
Select one or more roles to install on the selected server.

Roles	Description
☐ Active Directory Certificate Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
☒ Active Directory Domain Services (Installed)	
☐ Active Directory Federation Services	
☐ Active Directory Lightweight Directory Services	
☐ Active Directory Rights Management Services	
☐ Device Health Attestation	
☐ DHCP Server	
☒ DNS Server (Installed)	
☐ Fax Server	
☒ File and Storage Services (2 of 12 installed)	
☐ Host Guardian Service	
☐ Hyper-V	
☐ MultiPoint Services	
☒ Network Policy and Access Services (Installed)	
☐ Print and Document Services	
☐ Remote Access	
☐ Remote Desktop Services	
☐ Volume Activation Services	
☐ Web Server (IIS)	
☐ Windows Deployment Services	

< Previous **Next >** Install Cancel

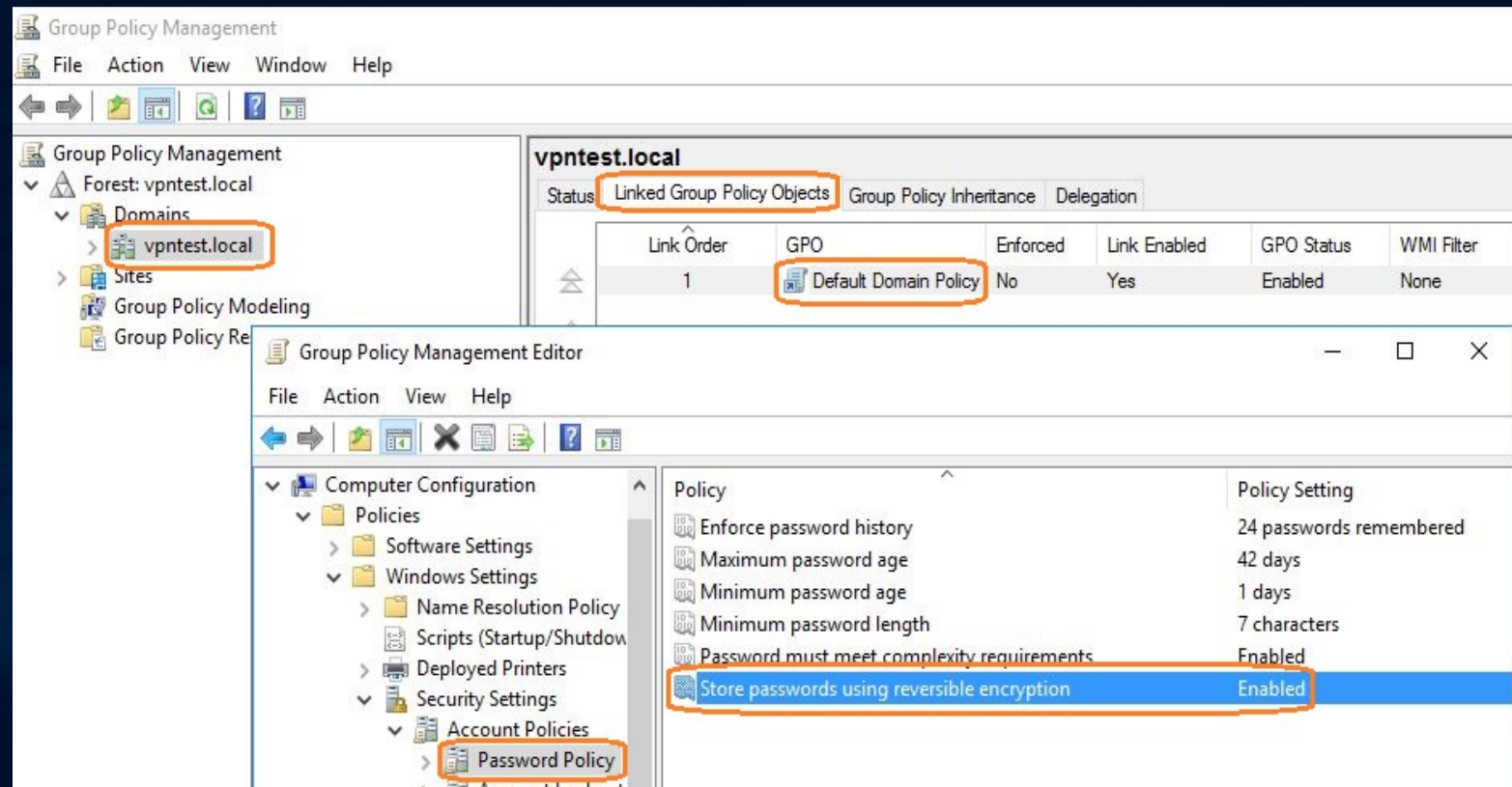
Preparing and configuring Microsoft Windows Server 2016 – Network Policy Server role

- We have no option to select on the Features part of the configuration so we just go with Next on this one
- On the next configuration menu we only need to review and click the Install button to actually start the NPS role installation.



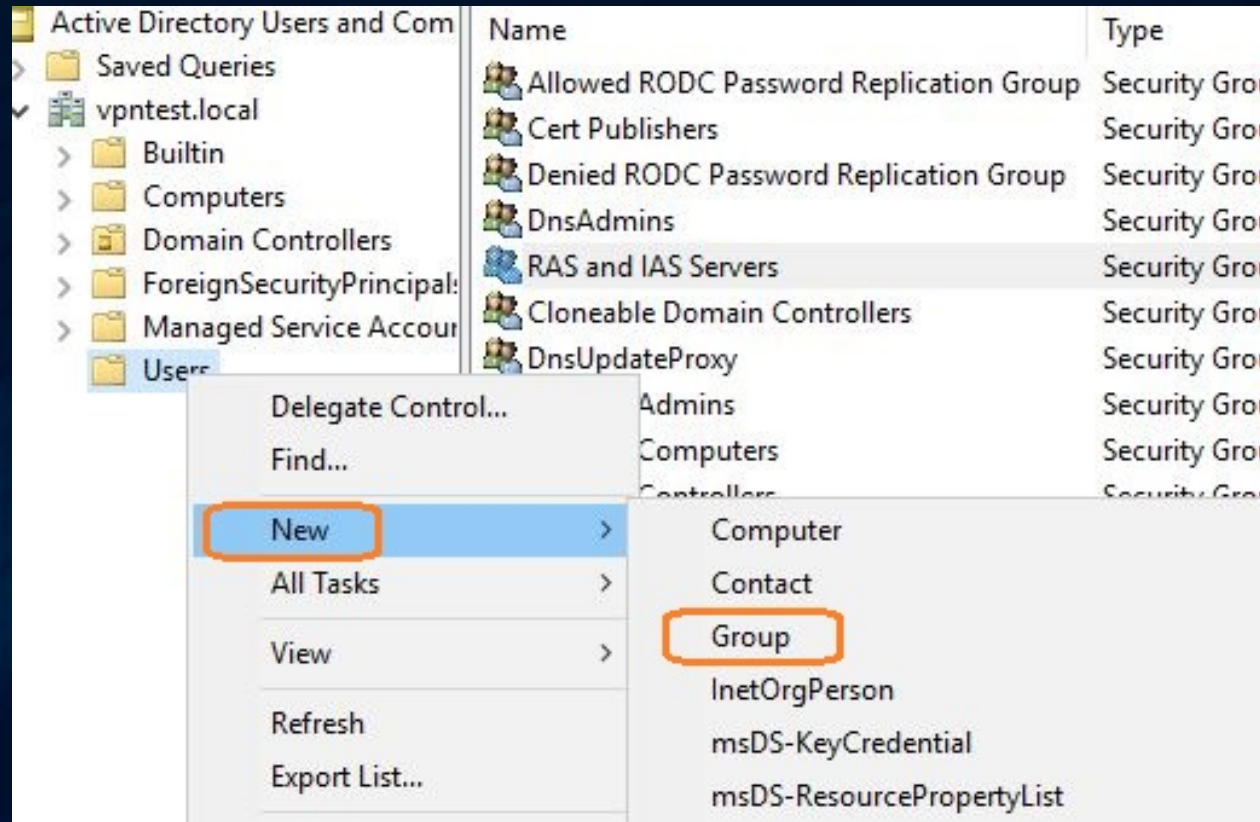
Preparing and configuring Microsoft Windows Server 2016 – Group Policy Management

- Using Group Policy Management from Server Manager, we need to enable Store password using reversible encryption
- On Default Domain Policy we need to right click and select Edit.
- Group Policy Management Editor we need to edit the Password Policy to store in reversible encryption as enabled



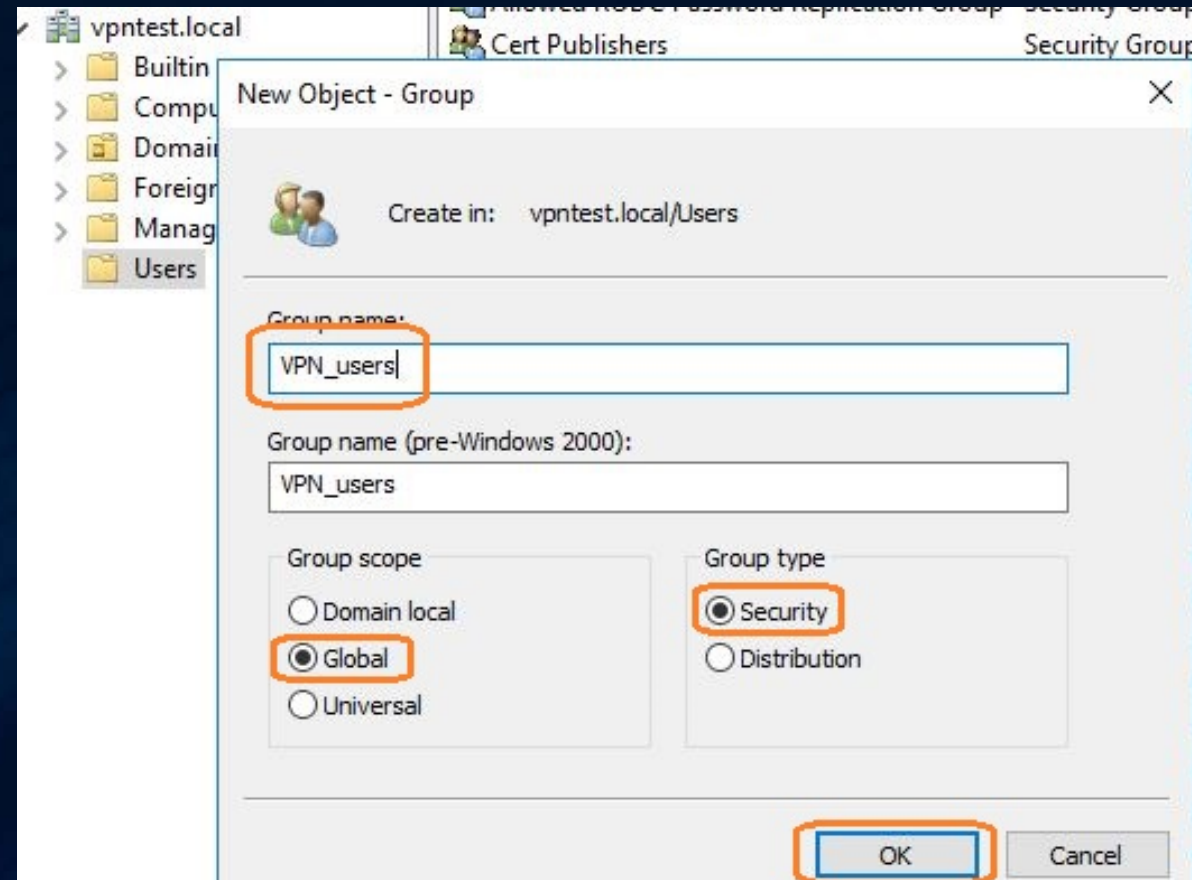
Preparing and configuring Microsoft Windows Server 2016 – Active Directory VPN Group

- In ADUC (Active Directory Users and Computers) console we need to create a Global Security Group
- Right click on the Users container and select New>Group



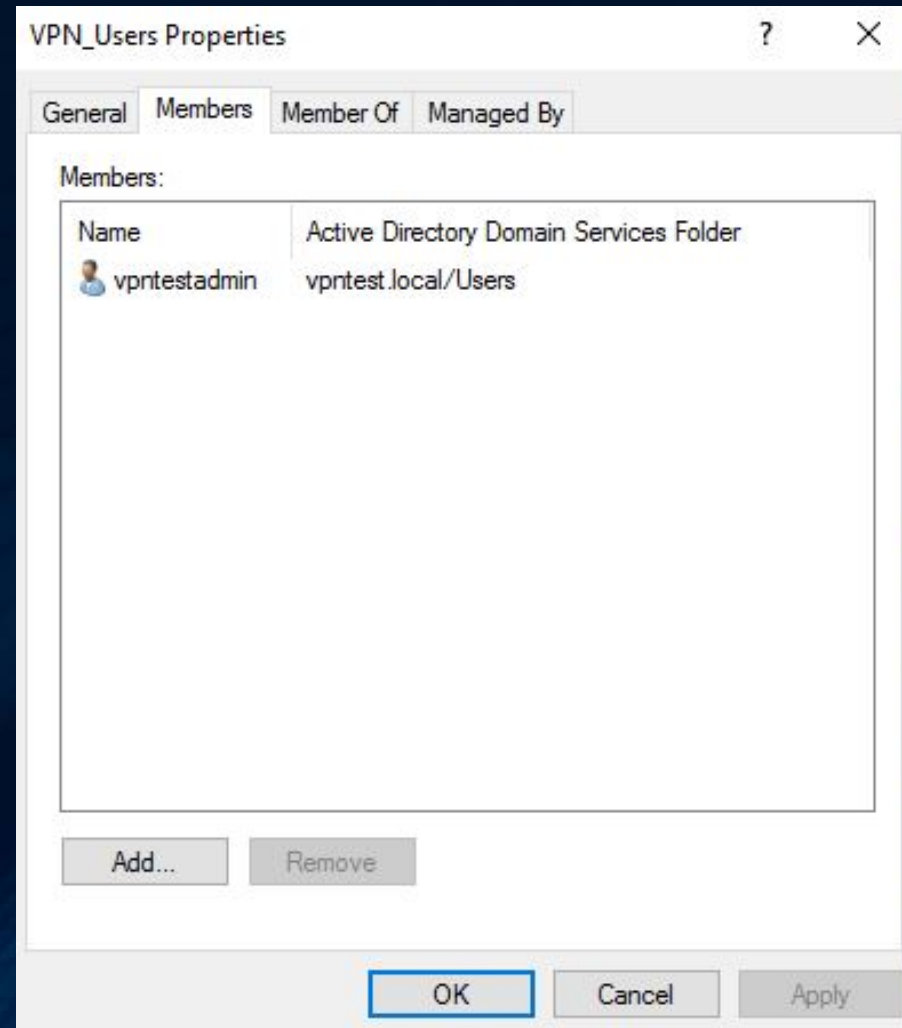
Preparing and configuring Microsoft Windows Server 2016 – Active Directory VPN Group

- In ADUC console new Object Group we should name the group VPN_Users and keep it as Global scope and Security type, then click OK



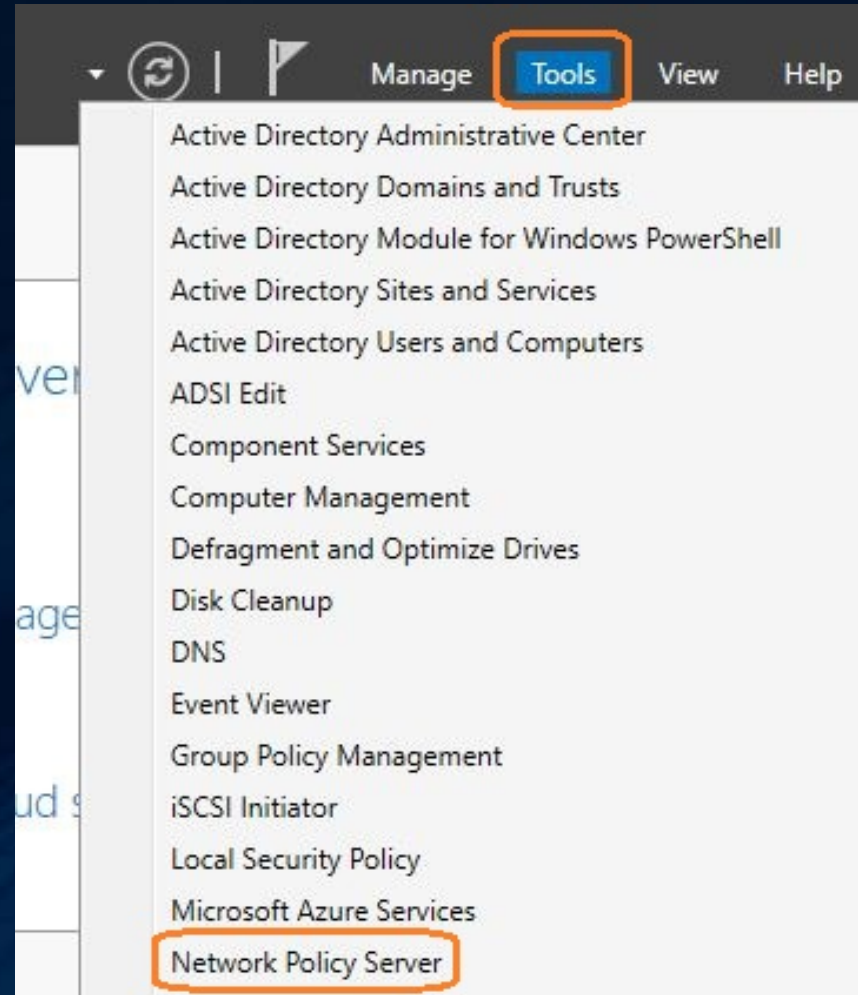
Preparing and configuring Microsoft Windows Server 2016 – Active Directory VPN Group members

- In ADUC console we need to double click the VPN_Users group that we have created in previous step and add the required Active Directory User accounts that are approved to access corporate resources using IPsec tunnel.



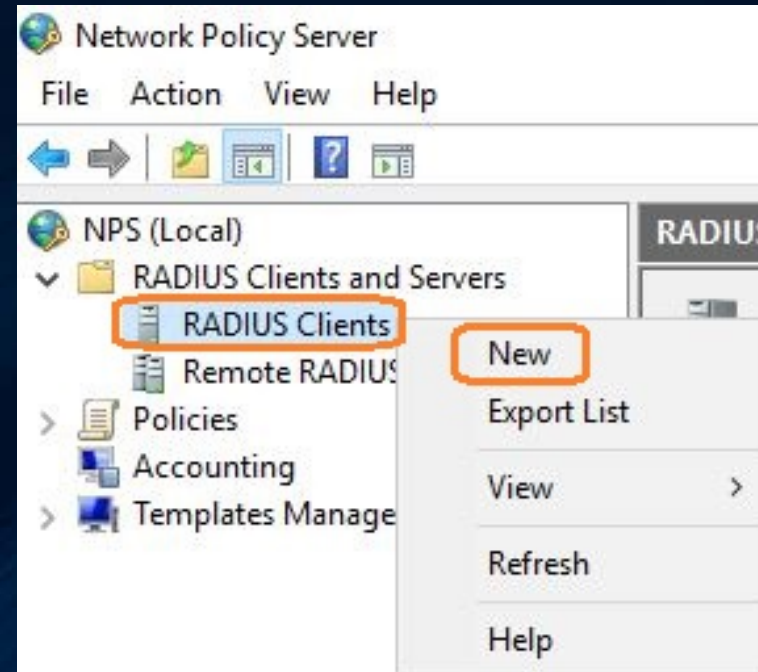
Preparing and configuring Microsoft Windows Server 2016 – Server manager NPS role config

- Using the Server Manager console again we can continue with the Network Policy Server role configuration.



Preparing and configuring Microsoft Windows Server 2016 – Server manager NPS role config

- Using the Server Manager console again we can continue with the Network Policy Server role configuration.
- We need to right click the RADIUS Clients under RADIUS Clients and Servers and Select New



Preparing and configuring Microsoft Windows Server 2016 – Server manager NPS role config

- Using the Network Policy Server cmdlet we have created new RADIUS Client.
- The options were configured as Enable
 - Friendly name
IPSECVPNROUTER
 - IP Address of RADIUS Client
10.170.10.254
 - Manual Shared secret (must match with secret configured at Step 11 from the RouterOS RADIUS Client configuration)

NPS (Local)

- ✓ RADIUS Clients and Policies
- RADIUS Clients
- Remote RADIUS Clients
- > Policies
- > Accounting
- > Templates Management

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
IPSECVPNROUTER

Address (IP or DNS):
10.170.10.254

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 as the one entered here. Shared secrets are case-sensitive.

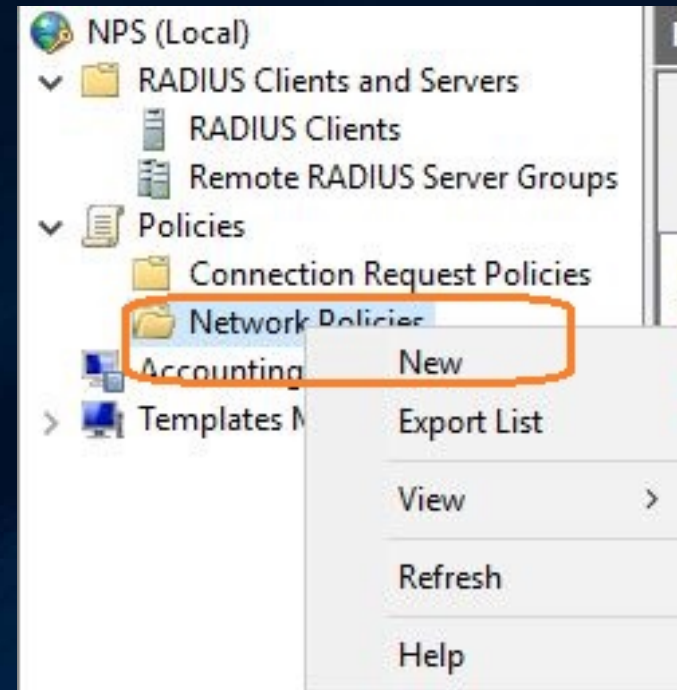
☒ Manual ☐ Generate

Shared secret:
.....

Confirm shared secret:
.....

Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies

- Using the Network Policy Server cmdlet we need to right click Network Policies under Policies menu and select New.



Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies

- Using the New Network Policy setup dialog we should name the policy as IPSEC for future reference and click Next.

Note: New Network Policy dialog has multiple pages so we can use Previous button in case we need to adjust some settings

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:
IPSEC

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.

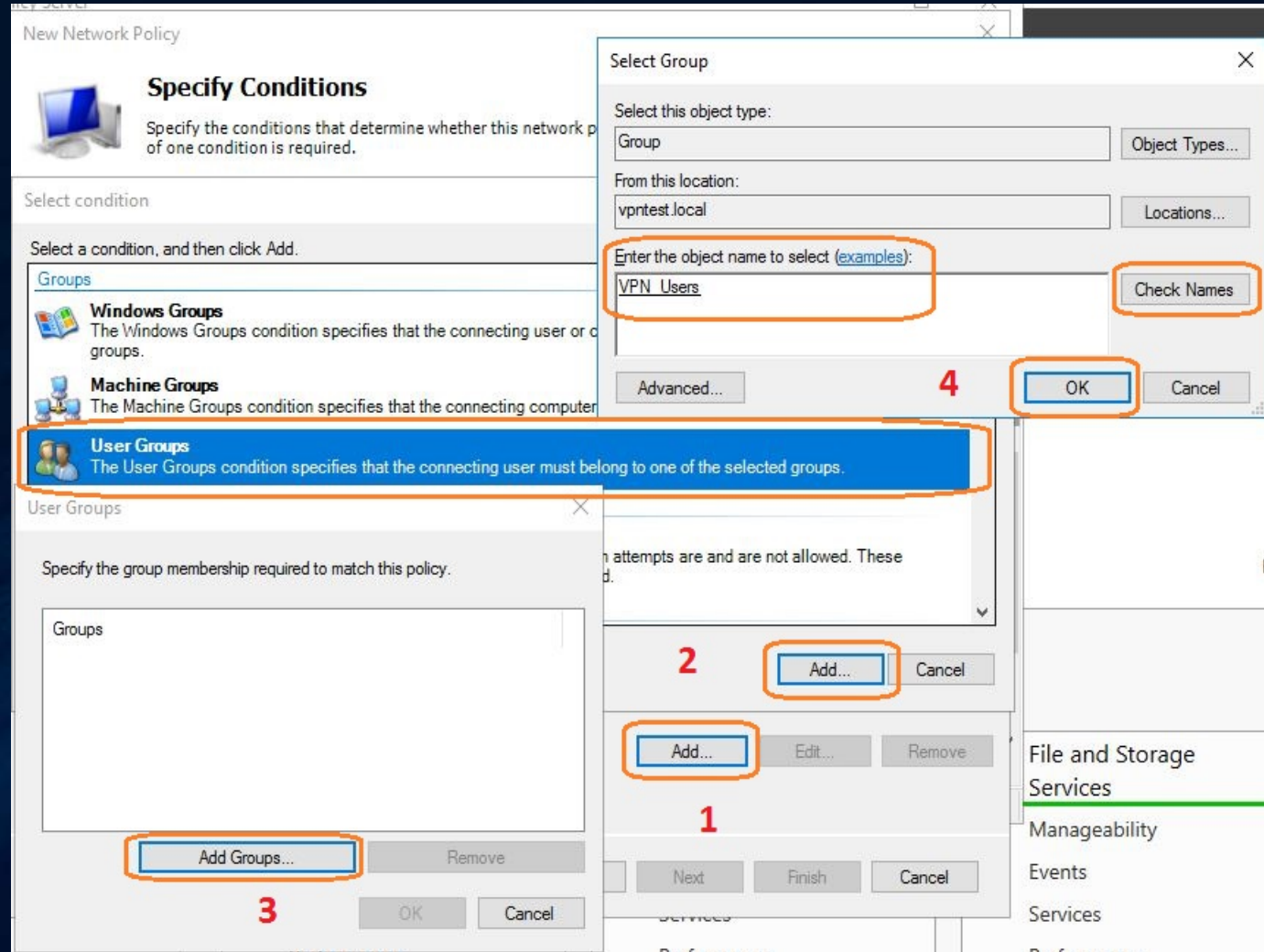
☒ Type of network access server:
Unspecified

☐ Vendor specific:
10

Previous Next Finish Cancel

Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies

- On the Specify Conditions page we should add the VPN_Users Active Directory security group created earlier.
- This will ensure that only VPN_Users group members are allowed to connect through VPN tunnel



Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies

- On Specify Access Permission setup page we should select Access granted option and click Next
- On the Configure Authentication Methods page we should only select Unencrypted authentication (PAP, SPAP) and click Next.
- Next setup page named Constraints is optional so we just continue with setup

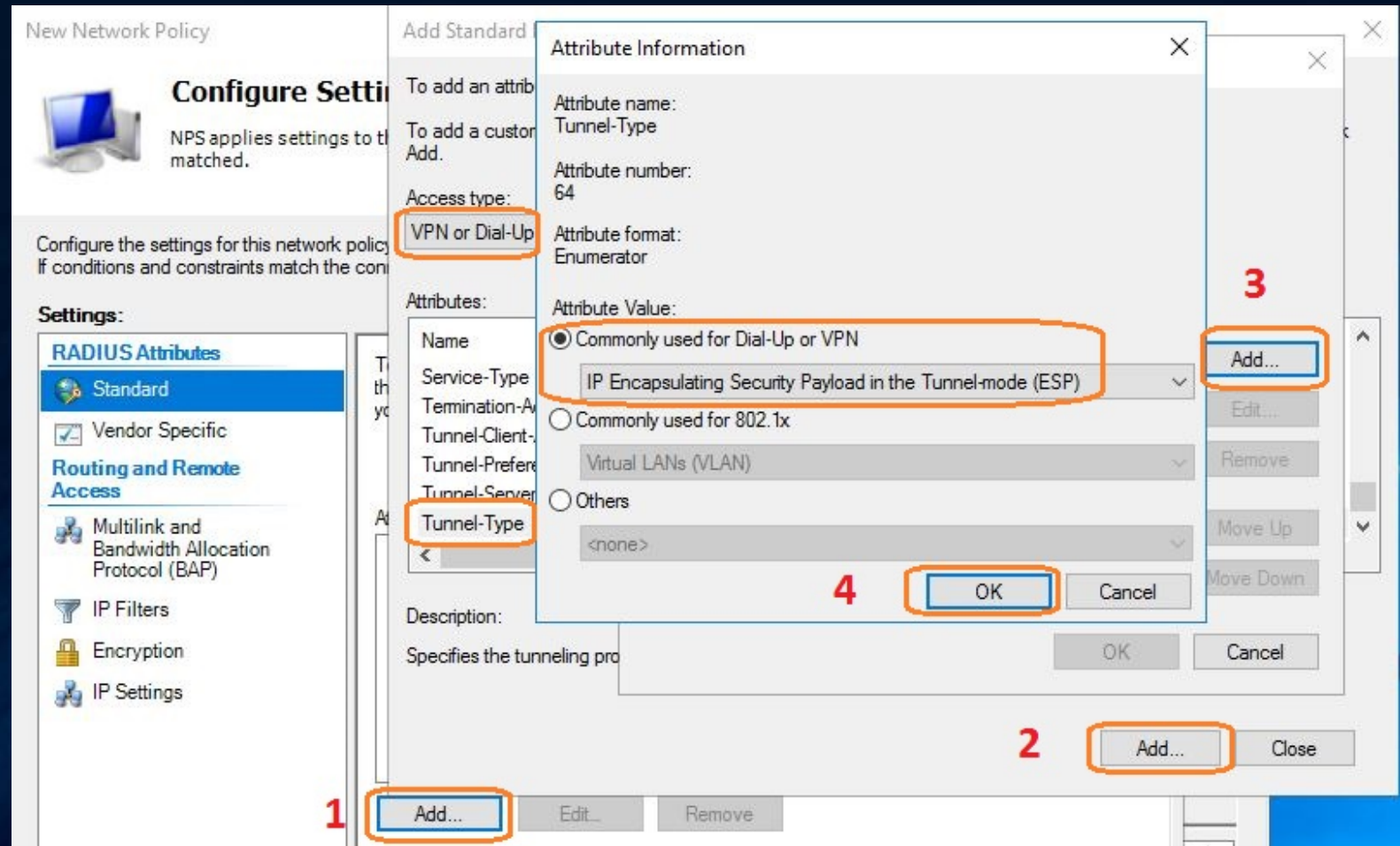
The image displays two screenshots of the Windows Network Policy Server (NPS) configuration wizard.

Left Screenshot: Specify Access Permission
This window is titled "New Network Policy" and "Specify Access Permission". It instructs the user to "Configure whether you want to grant or deny access to the network based on the policy." There are three radio button options: "Access granted" (which is selected and highlighted with an orange box), "Access denied", and "Access is determined by User Dial-in properties".

Right Screenshot: Configure Authentication Methods
This window is also titled "New Network Policy" and "Configure Authentication Methods". It instructs the user to "Configure one or more authentication methods required for the connection authentication, you must configure an EAP type." Below this, it states "EAP types are negotiated between NPS and the client in the order in which they are listed." There is a list box for "EAP Types" with "Move Up" and "Move Down" buttons. Below the list box are "Add...", "Edit...", and "Remove" buttons. Under the heading "Less secure authentication methods:", there are several checkboxes: "Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)", "Microsoft Encrypted Authentication (MS-CHAP)", "Encrypted authentication (CHAP)", "Unencrypted authentication (PAP, SPAP)" (which is selected and highlighted with an orange box), and "Allow clients to connect without negotiating an authentication method."

Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies

- On Configure Settings page we should remove existing PPP and Framed attributes
- Then, using the Add button we add the VPN tunnel type attribute for IPsec-ESP tunnel mode



Preparing and configuring Microsoft Windows Server 2016 – NPS > Network Policies summary

- This is the last setup page which actually summarizes our settings
- In case we are satisfied with the setup we can select Finish

Completing New Network Policy

You have successfully created the following network policy:

IPSEC

Policy conditions:

Condition	Value
User Groups	VPNTEST\VPN_Users

Policy settings:

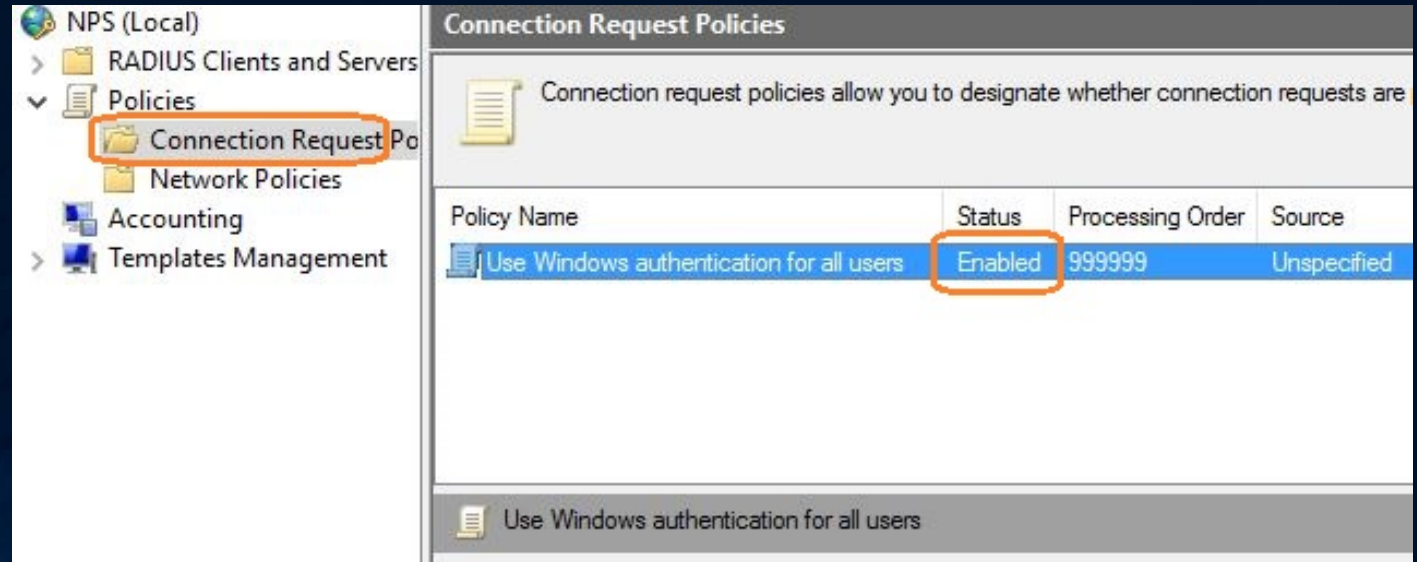
Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP)
Access Permission	Grant Access
Ignore User Dial-In Properties	False
Tunnel-Type	IP Encapsulating Security Payload in the Tunnel-mode (ESP)

To close this wizard, click Finish.

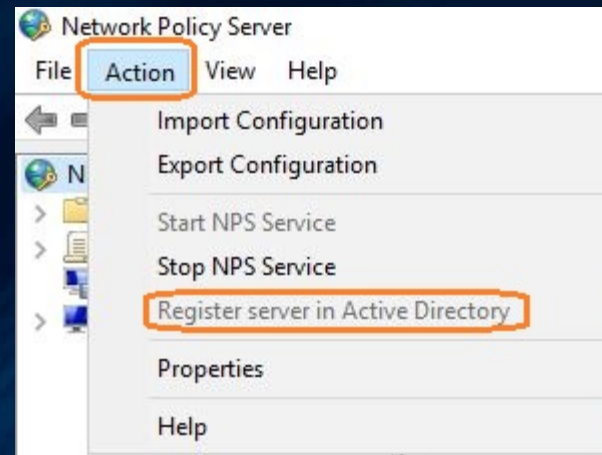
Previous Next **Finish** Cancel

Preparing and configuring Microsoft Windows Server 2016 – NPS > Connection Requests

- On Policies > Connection Request Policies we should make sure that the Authentication process is done locally on the Domain Controller. We need to check if the policy is enabled



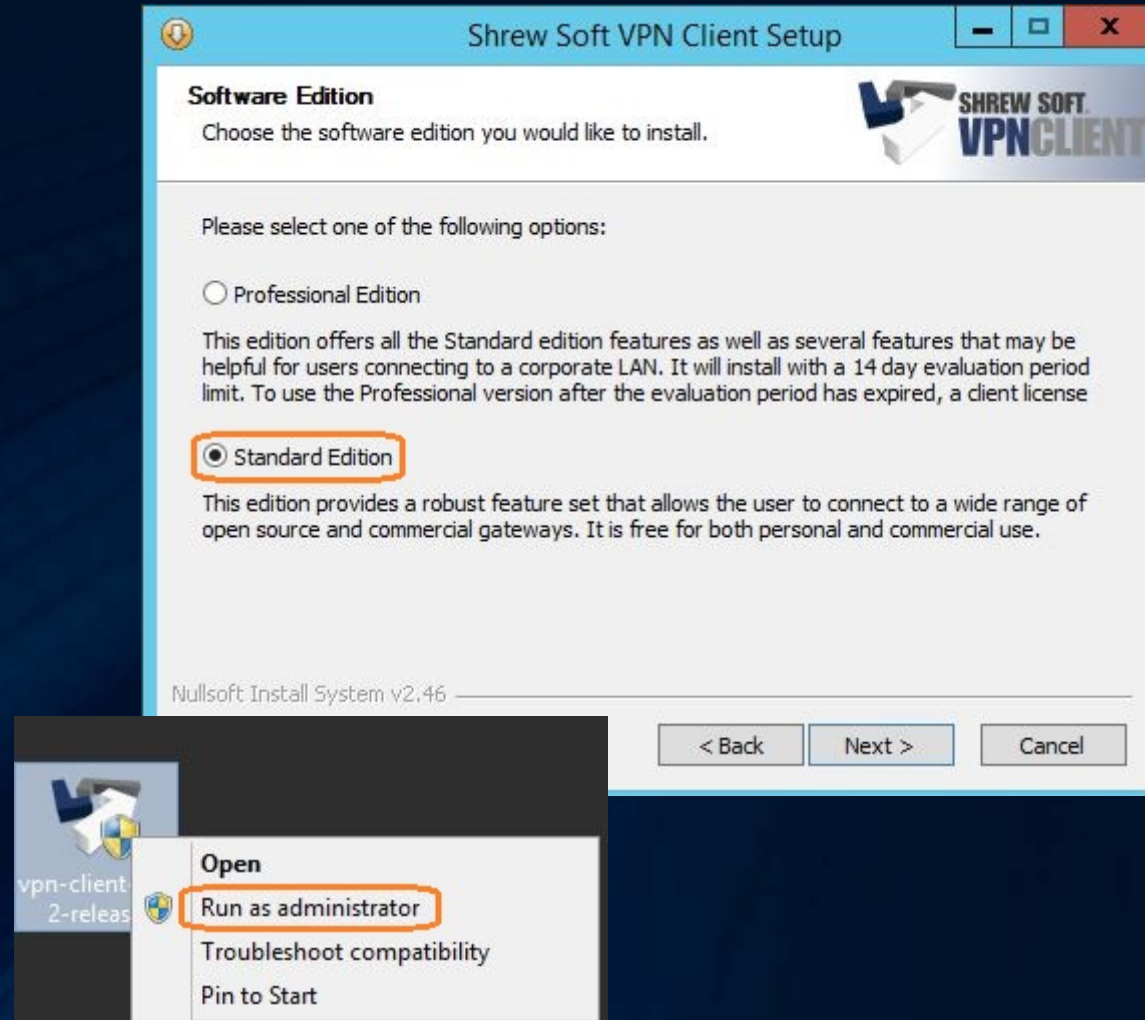
Note: Network Policy Server should already be registered with Active Directory but we can check that anyway



Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

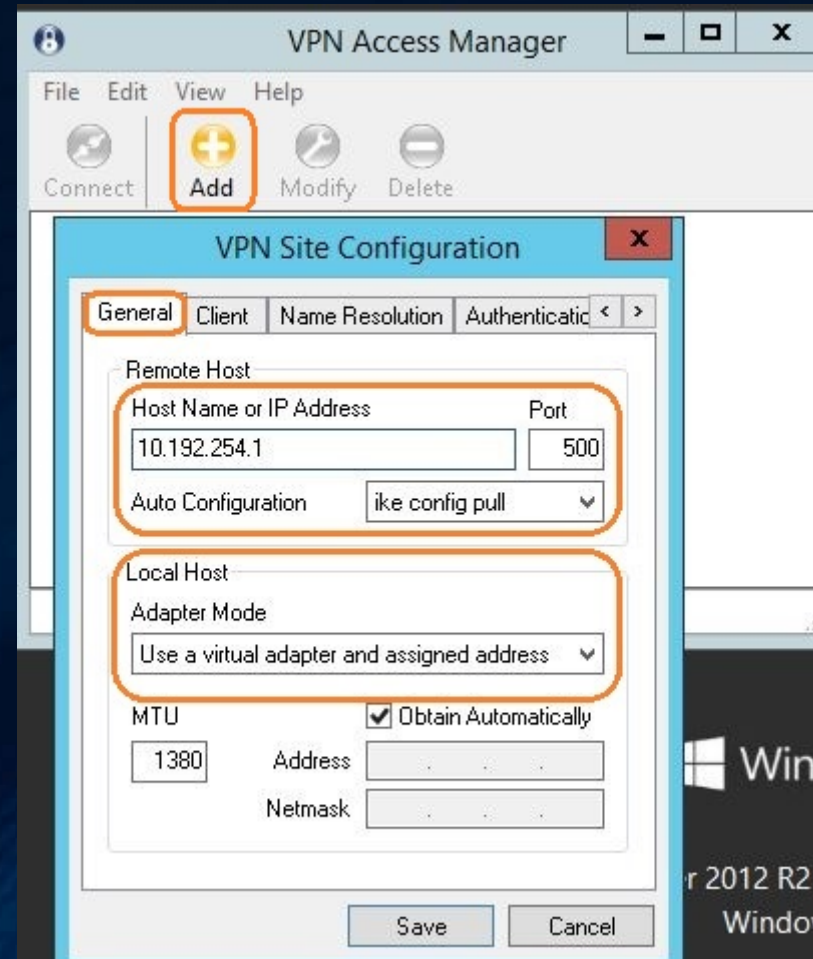
- The ShrewSoft Installer works in:
 - Professional (paid license)
 - Standard (free license)

Note: Always run the installer as admin privilege rights



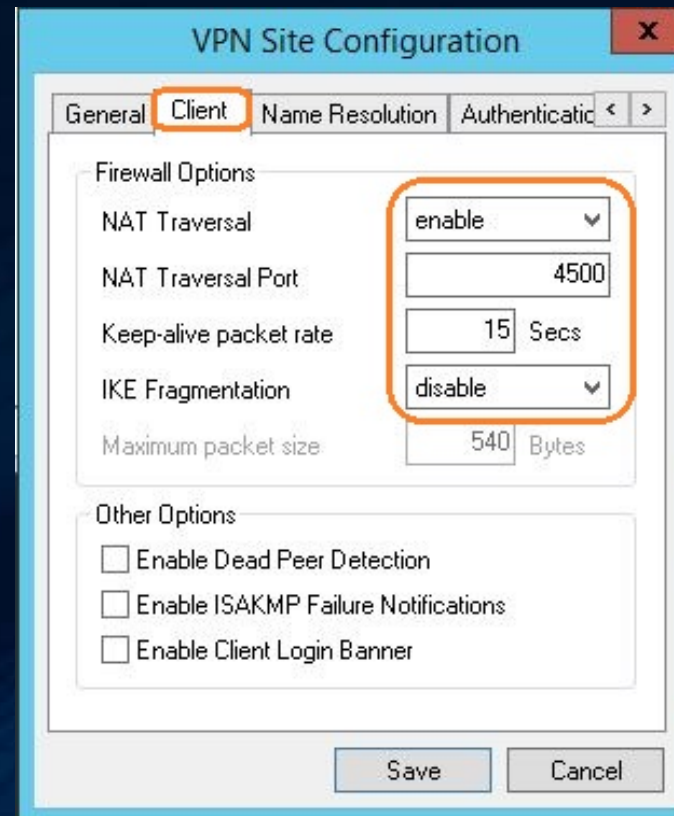
Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

- We now need to add a Site configuration profile using the Add button
- On General tab we need to configure Remote VPN Gateway Host Name or IP address using udp 500 and ike config pull
- The local host section can use a virtual adapter obtained automatically



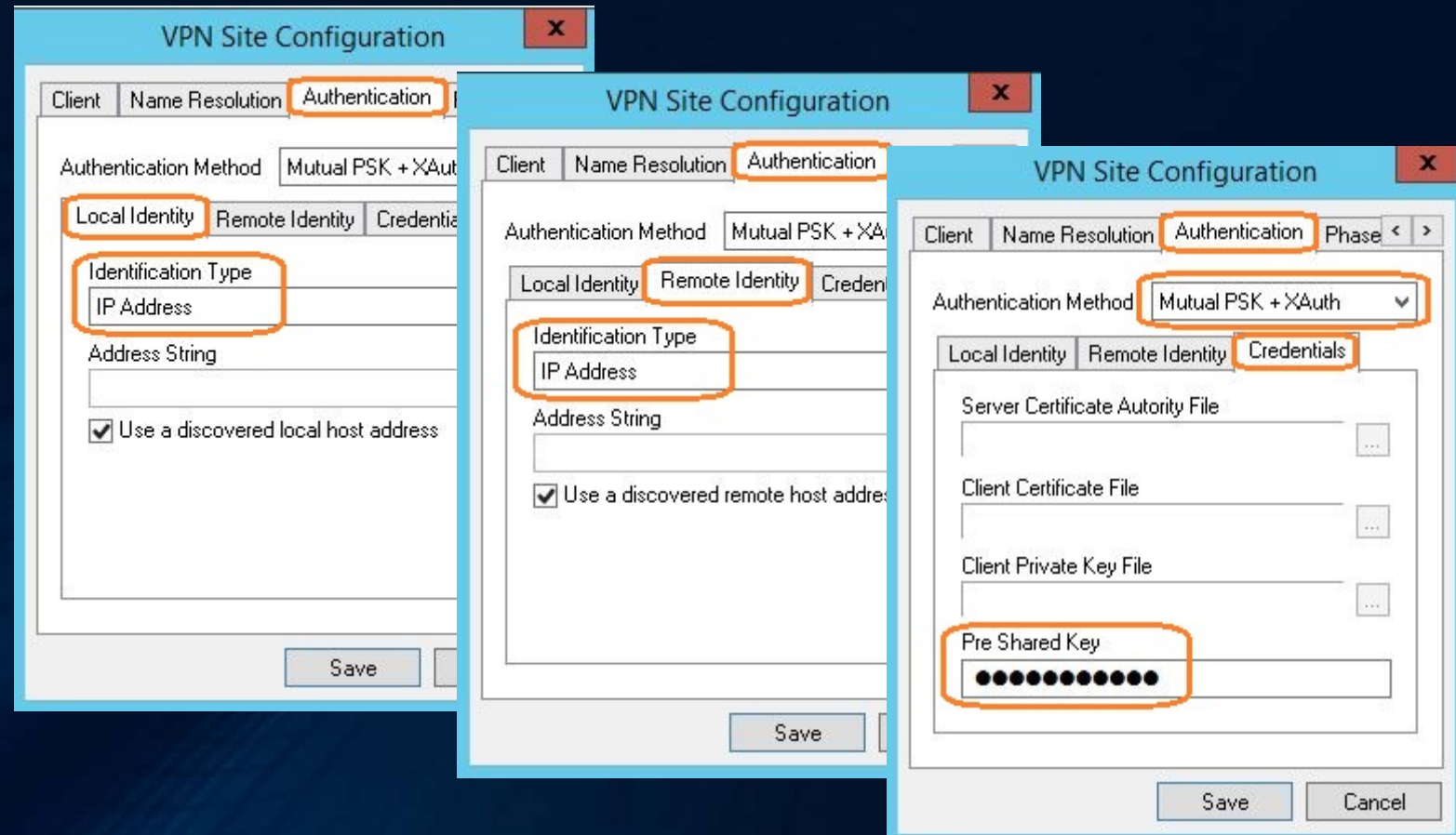
Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

- On the Client tab need to enable NAT-T mode
- Also we should disable IKE fragmentation



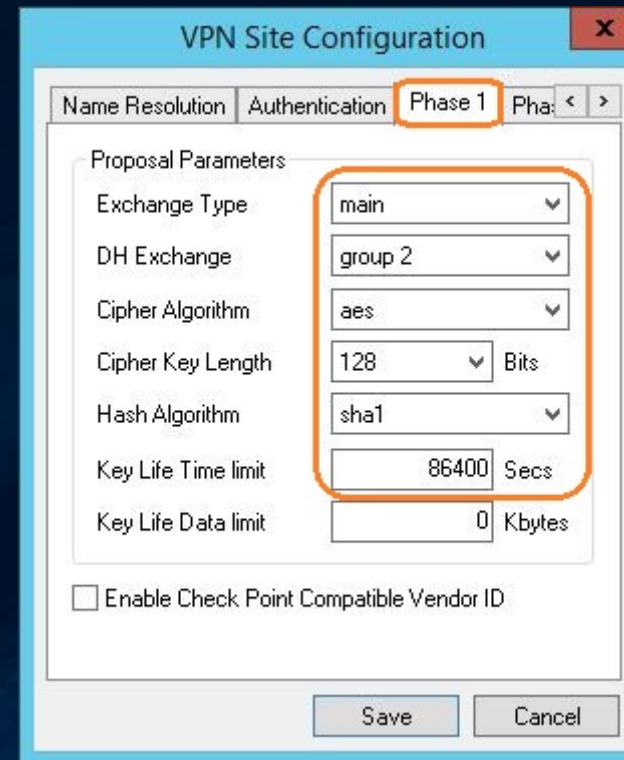
Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

- Leaving the Name Resolution tab as default we can continue with Authentication method Mutual PSK+XAuth
 - Local Identity should use IP Address as Identification type
 - Remote Identity should use same options
 - Credentials Pre Shared Key must match with IPsec PSK configured at step 7 from the RouterOS IPsec configuration section



Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

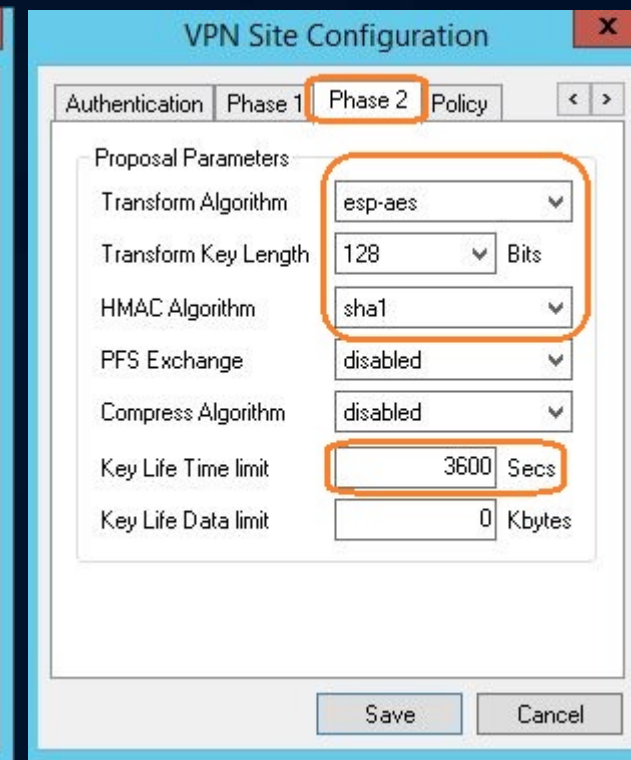
- Phase 1 menu options must match with Peer profiles setting at step 6 from RouterOS IPsec configuration section
 - Sha1, aes-128 , modp 1024
 - Lifetime 1 day
 - NAT-T enabled
- Phase 2 menu options should match with Policy proposals at step 5 from RouterOS IPsec configuration section
 - Authentication sha1
 - Encryption aes-128 cbc (cypher block chain)
 - Lifetime of 1 hour



The image shows the 'VPN Site Configuration' window with the 'Phase 1' tab selected. The 'Proposal Parameters' section is highlighted with an orange box. The settings are as follows:

Parameter	Value
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

At the bottom, there is an unchecked checkbox labeled 'Enable Check Point Compatible Vendor ID' and 'Save' and 'Cancel' buttons.



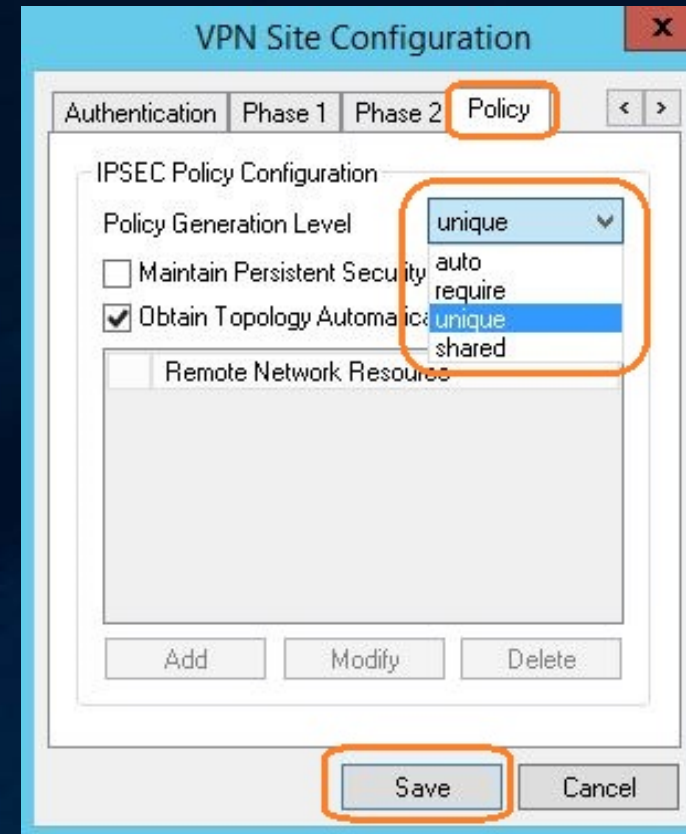
The image shows the 'VPN Site Configuration' window with the 'Phase 2' tab selected. The 'Proposal Parameters' section is highlighted with an orange box. The settings are as follows:

Parameter	Value
Transform Algorithm	esp-aes
Transform Key Length	128 Bits
HMAC Algorithm	sha1
PFS Exchange	disabled
Compress Algorithm	disabled
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes

At the bottom, there are 'Save' and 'Cancel' buttons.

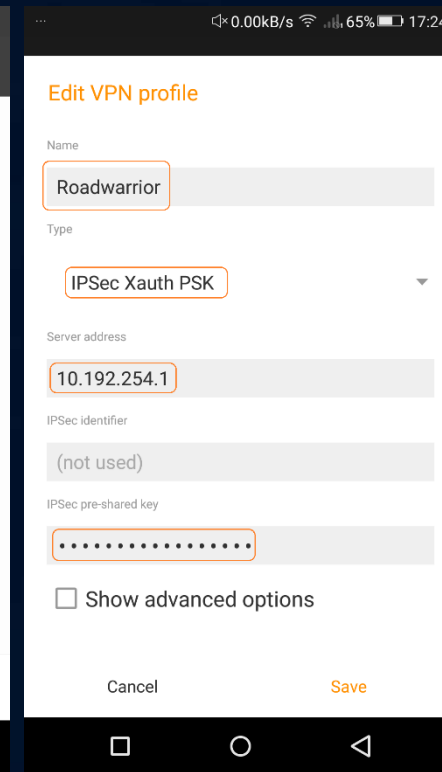
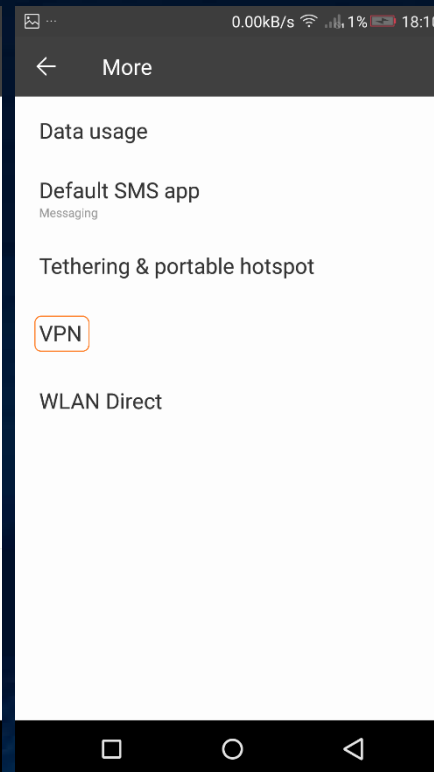
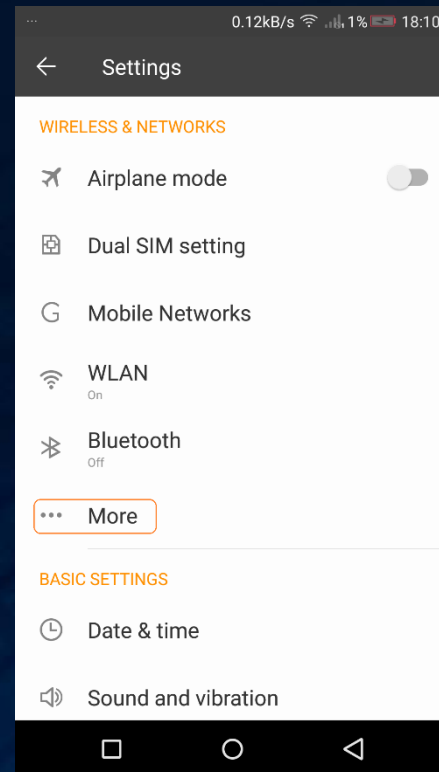
Preparing and configuring Microsoft Windows Client running ShrewSoft VPN software

- Policy configuration menu is where we configure the policy generation level
 - Auto (Cisco Vendor-ID format)
 - Require
 - Unique
 - Shared
- MikroTik RouterOS can work with Require or Unique options

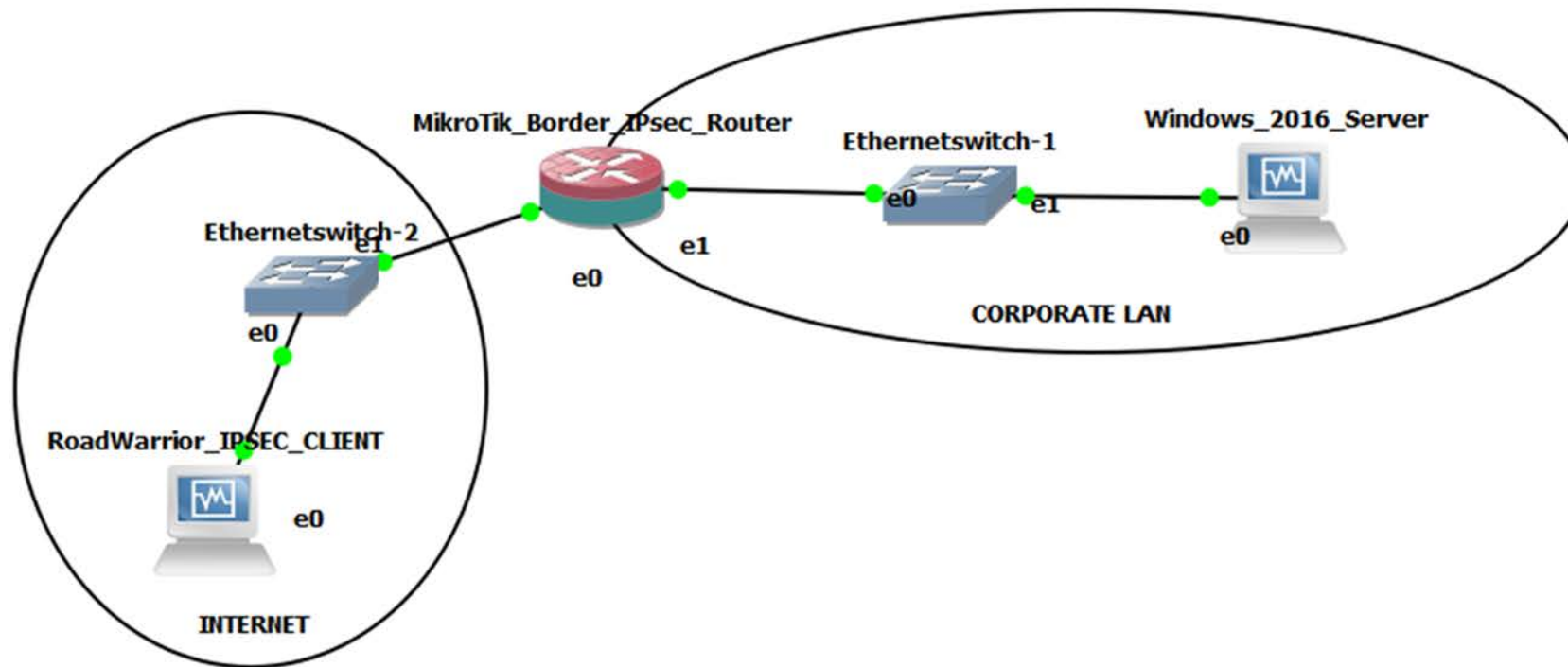


Preparing and configuring ANDROID mobile IPsec VPN client

- On ANDROID mobile you need to open Settings menu
- On Settings menu we need to open VPN
- On VPN we add VPN profile
- On edit VPN profile we add Server address, Xauth PSK mode and Pre Shared Key



Presentation Lab





<https://www.mikrotraining.ro>

Thank you!

Questions?