Konfigurasi MikroTIK di Sekolah Saya

Oleh Asep Jalaludin

Biodata

- Asep Jalaludin
- Pengajar Mapel Produktif TKJ dan Staf TI
- Trainer Mikrotik Academy dan Oracle Academy

SMK Bintang Nusantara School

- Mulai beroperasi sejak Juli 2011
- Berlokasi di Sepatan, Kab. Tangerang, Banten
- Memiliki 5 Jurusan (Teknik Komputer dan Jaringan, Multimedia, Keperawatan, Farmasi , Akuntansi)
- Jumlah siswa 123 orang (per TP 2015/2016)
- Oktober 2014, Menjadi Mikrotik Academy
- Agustus 2014, Menjadi Cisco Academy
- 2014, Menjadi Oracle Academy

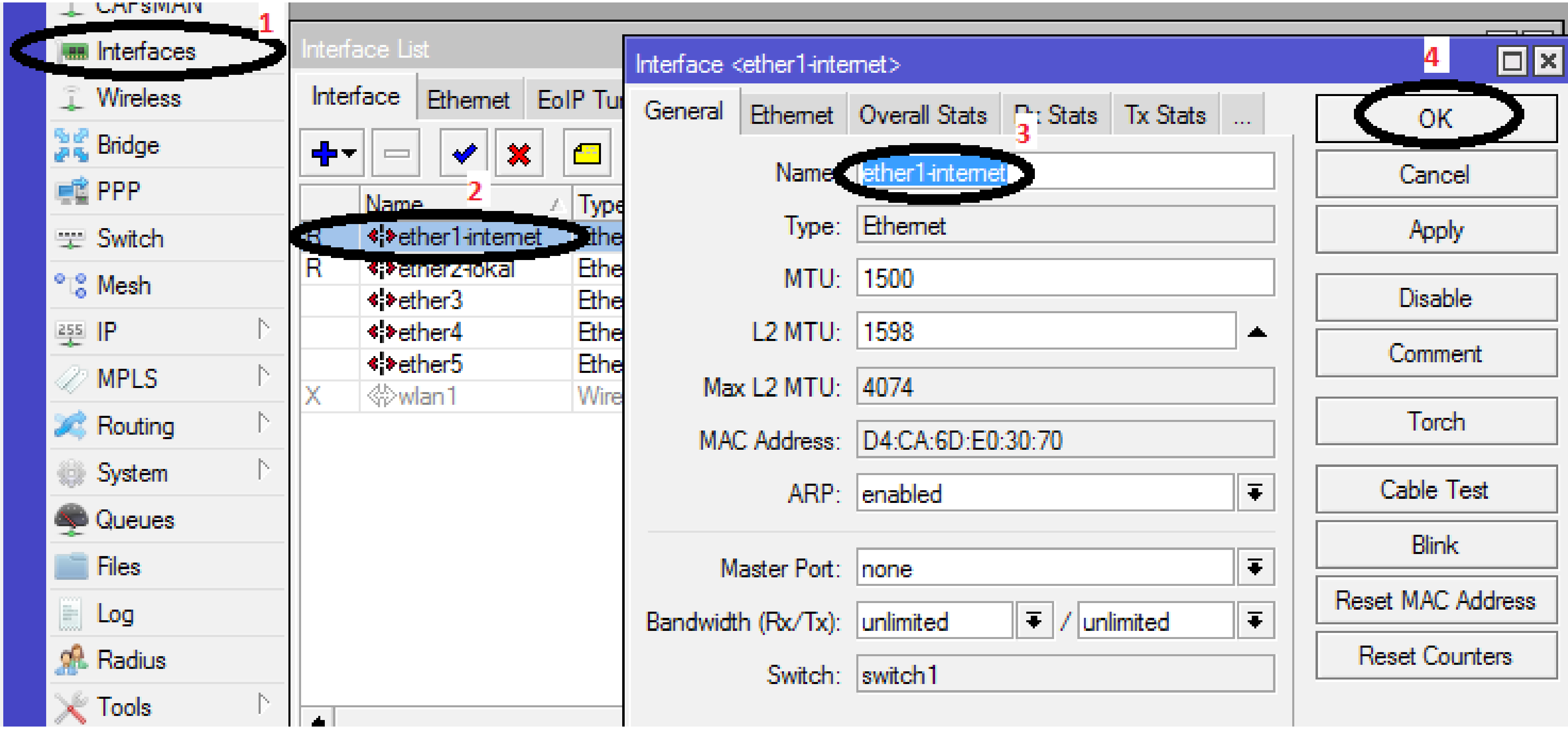
Materi

- Konfigurasi dasar mikrotik sampai terkoneksi internet
- Bandwidth management terintegrasi dengan hotspot
- Integrasi dengan radius server dari win server 2012
- Blokir website terjadwal
- Force DHCP
- Force DNS
- Pengamanan menggunakan port knocking

Konfigurasi internet

- Set nama interface
- Set DHCP client
- Set IP address
- Set DNS
- Set route (jika tidak menggunakan DHCP client)
- Set NAT (jika tidak menggunakan hotspot)
- Set DHCP server (jika tidak menggunakan hotspot)

Set interface name



	Name	Type
R	ether1-internet	Ethe
R	ether2-lokal	Ethe
	ether3	Ethe
	ether4	Ethe
	ether5	Ethe
X	wlan1	Wire

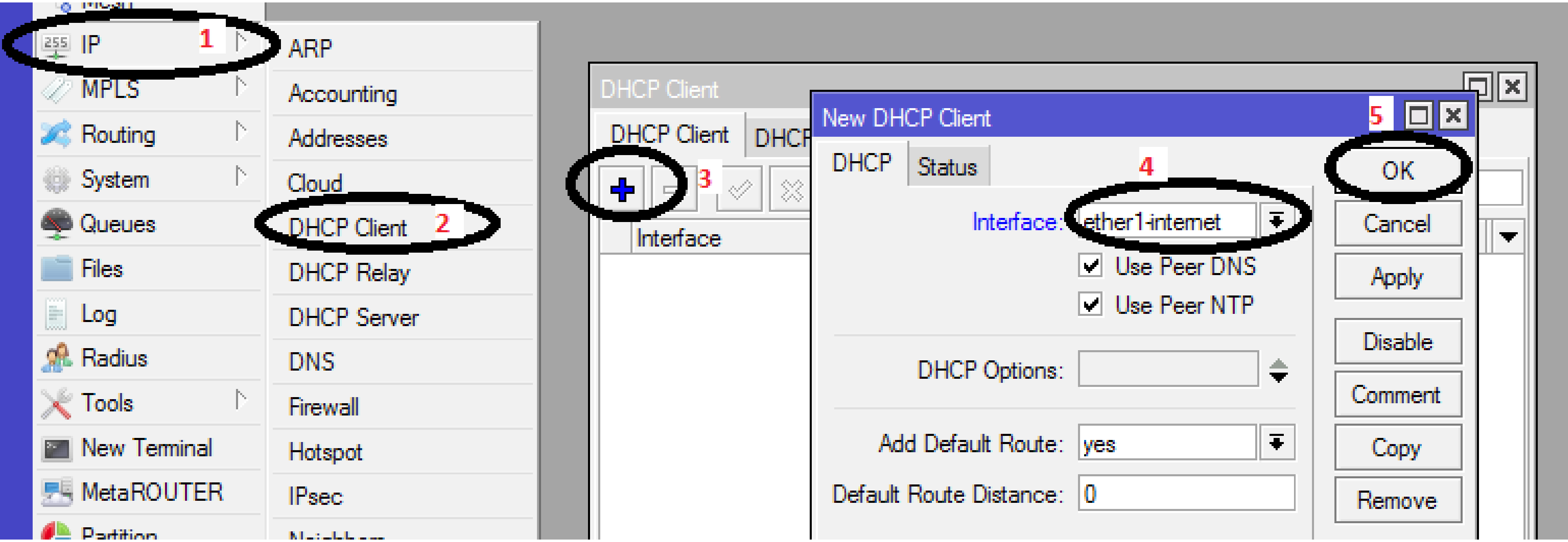
Interface <ether1-internet>

Name:	ether1-internet
Type:	Ethernet
MTU:	1500
L2 MTU:	1598
Max L2 MTU:	4074
MAC Address:	D4:CA:6D:E0:30:70
ARP:	enabled
Master Port:	none
Bandwidth (Rx/Tx):	unlimited / unlimited
Switch:	switch1

Set interface name

- /interface ethernet
- Set name=ether1-internet number=0
- Set name=ether2-lokal number=1

Set DHCP client



Interface: ether1-internet

☑ Use Peer DNS

☑ Use Peer NTP

DHCP Options:

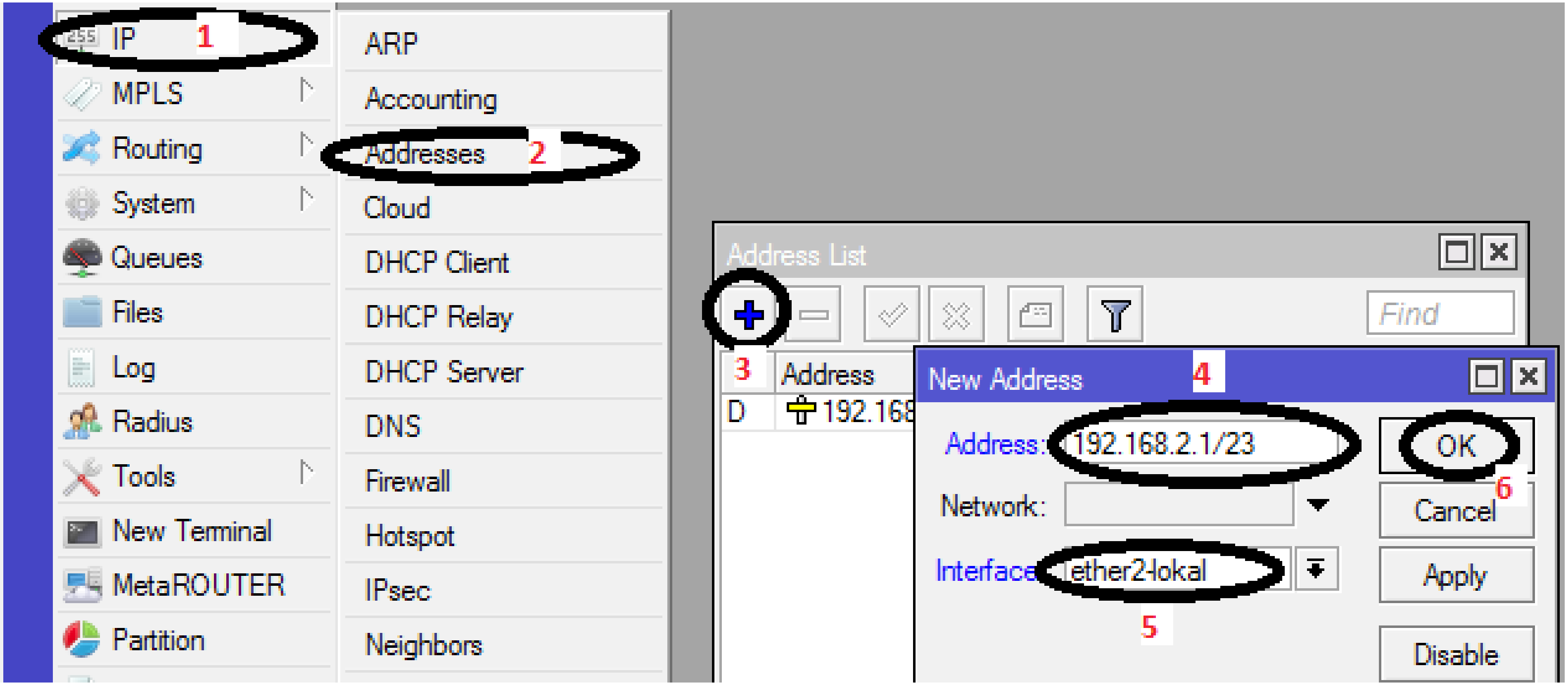
Add Default Route: yes

Default Route Distance: 0

Set DHCP client

```
/ip dhcp-client
add interface=ether1-internet
```

Set IP address



Address: 192.168.2.1/23

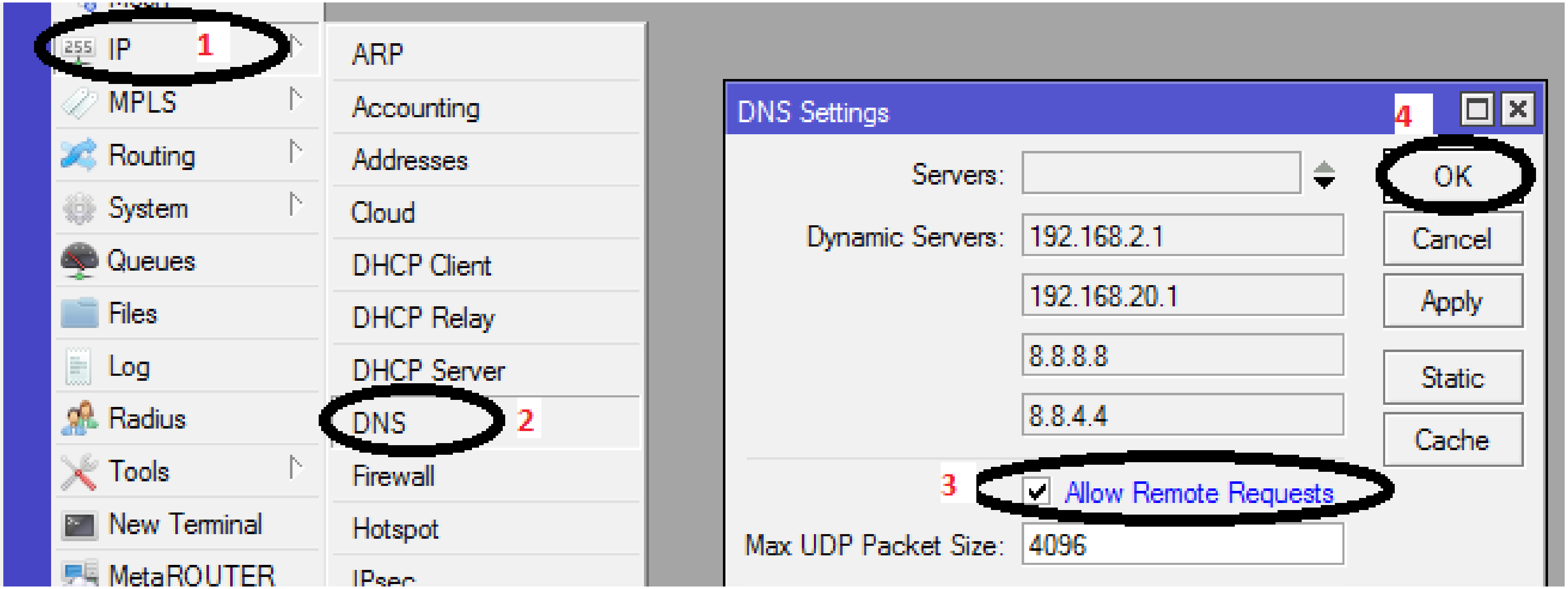
Network:

Interface: ether2-lokal

Set IP address

- /ip address
- add address=192.168.2.1/23 interface=ether2-lokal

Set DNS



Servers:

Dynamic Servers: 192.168.2.1

192.168.20.1

8.8.8.8

8.8.4.4

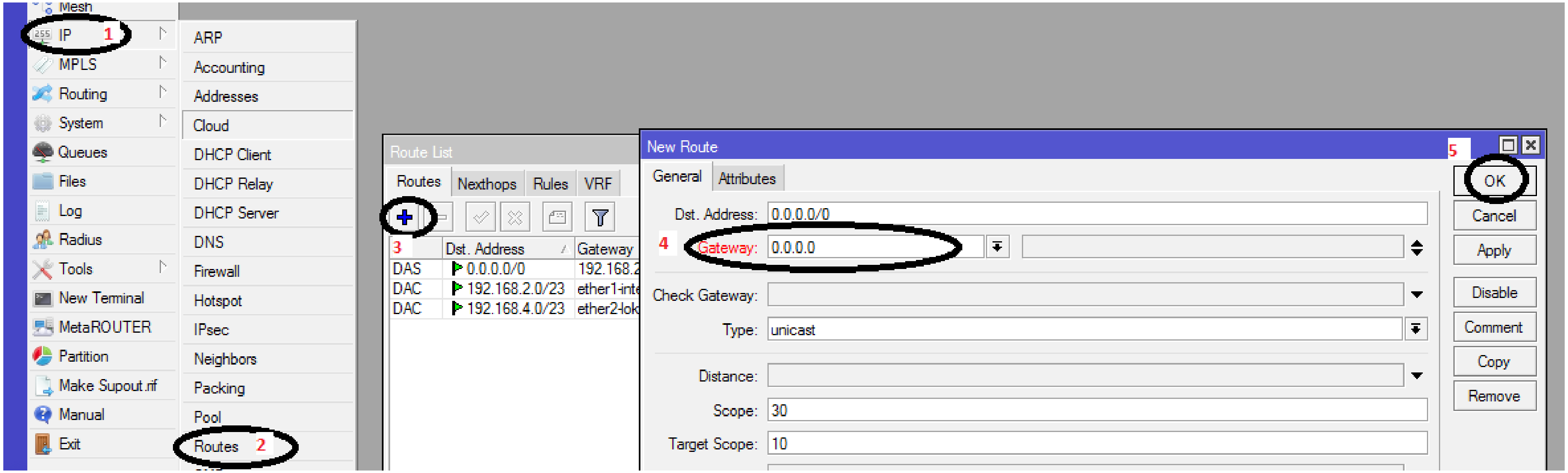
☑ Allow Remote Requests

Max UDP Packet Size: 4096

Set DNS

- /ip dns
- Set servers=8.8.8.8,8.8.4.4
- set allow-remote-requests=yes

Set Route



	Dst. Address	Gateway
DAS	0.0.0.0/0	192.168.2
DAC	192.168.2.0/23	ether1-inte
DAC	192.168.4.0/23	ether2-lok

Dst. Address: 0.0.0.0/0

Gateway: 0.0.0.0

Check Gateway:

Type: unicast

Distance:

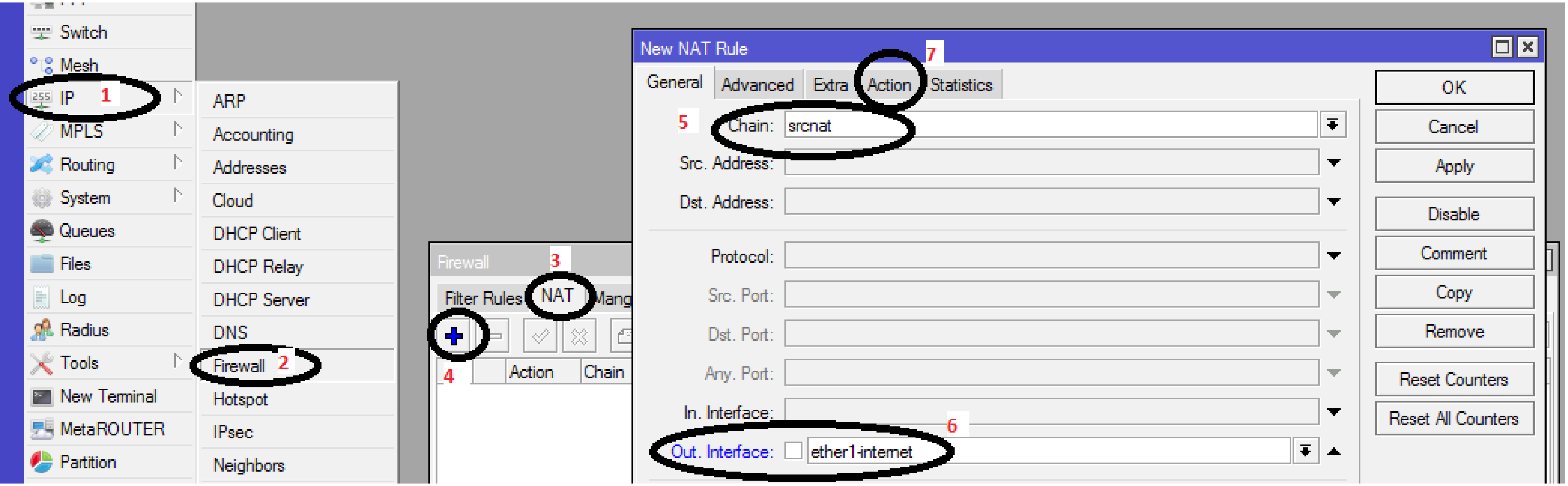
Scope: 30

Target Scope: 10

Set Route

- /ip route
- add gateway=192.168.20.1

Set NAT



1 IP

2 Firewall

3 NAT

4 +

5 Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

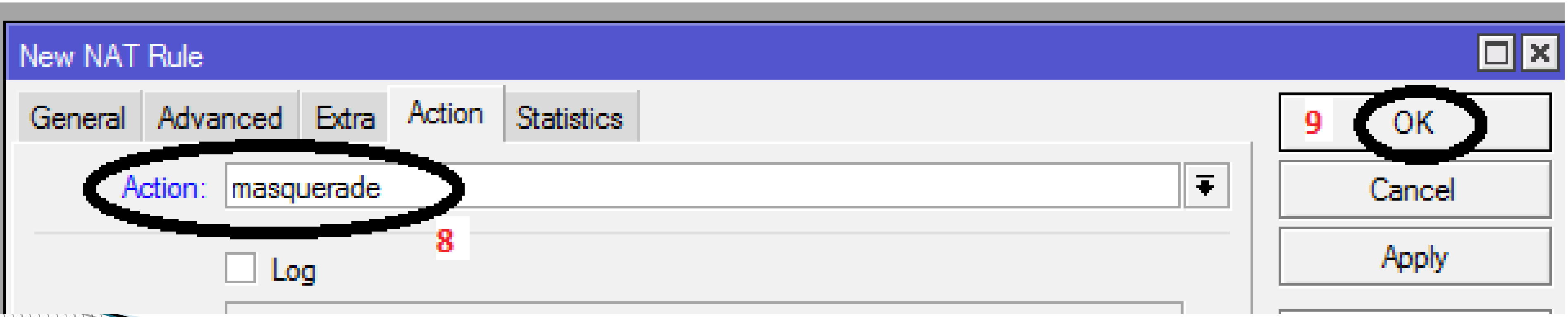
Dst. Port:

Any. Port:

In. Interface:

6 Out. Interface: □ ether1-internet

7 Action



8 Action: masquerade

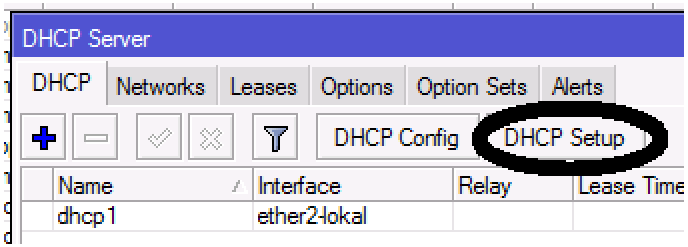
□ Log

9 OK

Set NAT

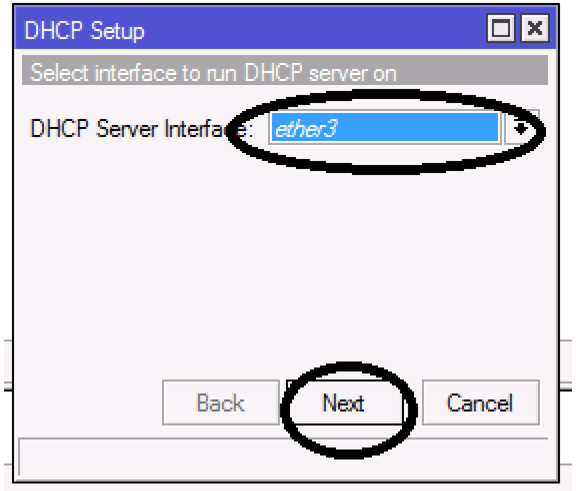
- /ip firewall nat
- add action=masquerade chain=srcnat out-interface=ether1-internet

Set DHCP-Server (1)



Name	Interface	Relay	Lease Time
dhcp1	ether2-lokal		

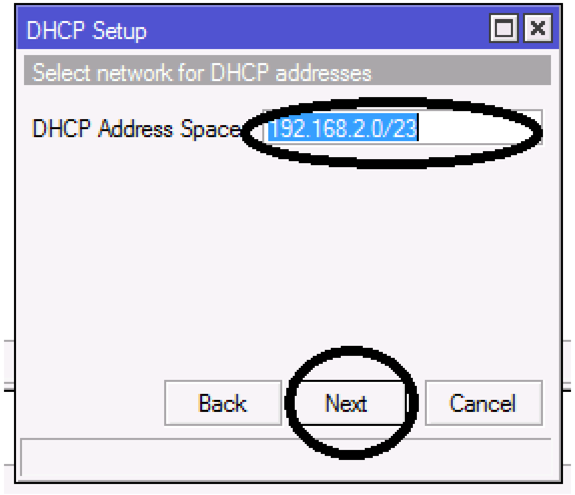
Tahap 1



Select interface to run DHCP server on

DHCP Server Interface: ether3

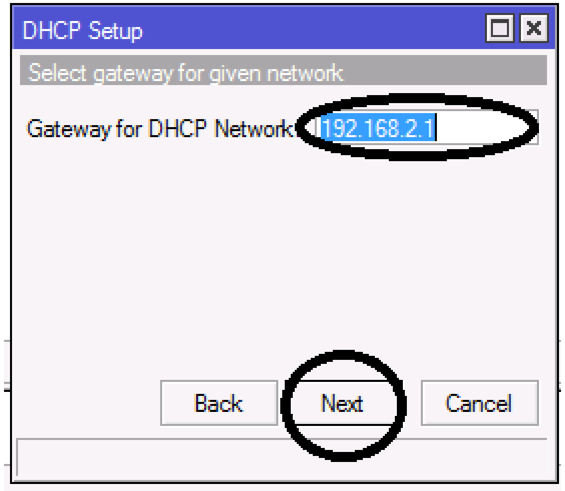
Tahap 2



Select network for DHCP addresses

DHCP Address Space: 192.168.2.0/23

Tahap 3

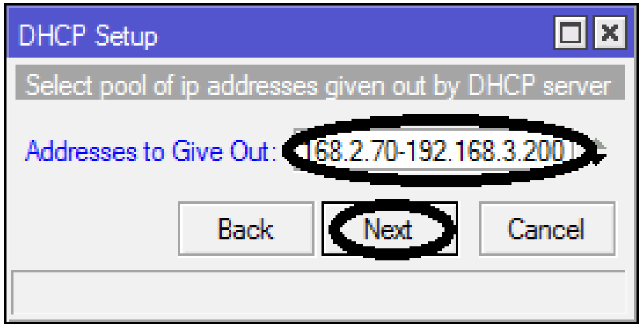


Select gateway for given network

Gateway for DHCP Network: 192.168.2.1

Tahap 4

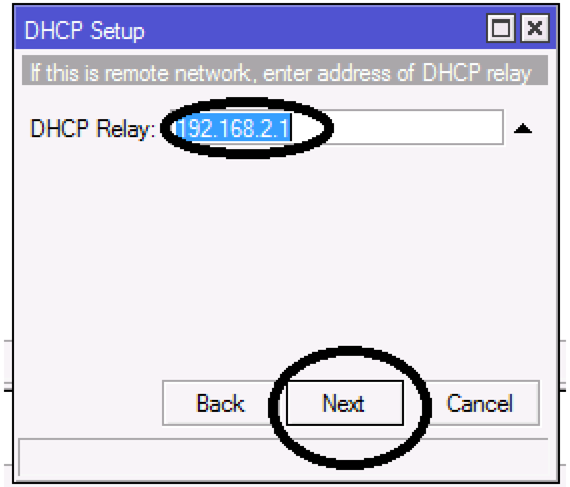
Set DHCP-Server (2)


DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 168.2.70-192.168.3.200

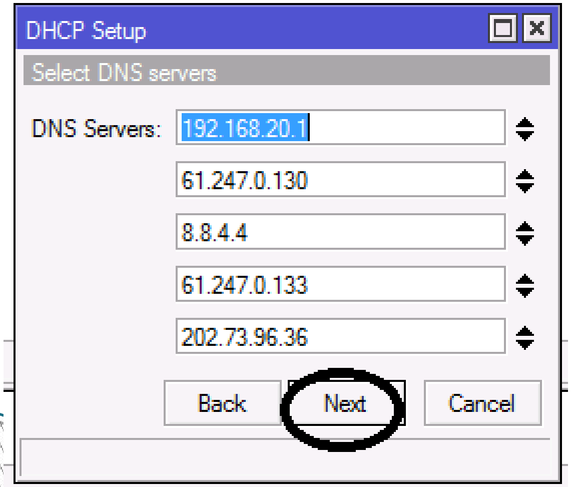
Tahap 5


DHCP Setup

If this is remote network, enter address of DHCP relay

DHCP Relay: 192.168.2.1

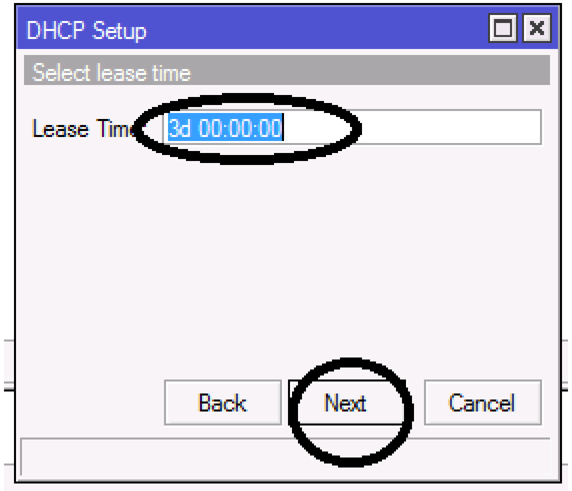
Tahap 6


DHCP Setup

Select DNS servers

DNS Servers: 192.168.20.1
61.247.0.130
8.8.4.4
61.247.0.133
202.73.96.36

Tahap 7

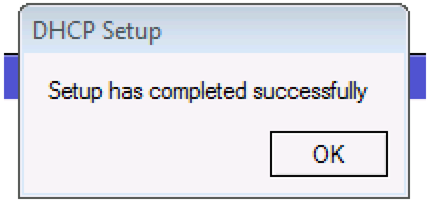

DHCP Setup

Select lease time

Lease Time: 3d 00:00:00

Tahap 8

Tahap 9


DHCP Setup

Setup has completed successfully

Set DHCP-Server (1)

- /ip dhcp-server setup
- Select interface to run DHCP server on
- dhcp server interface: ether2-lokal
- Select network for DHCP addresses
- dhcp address space: 192.168.2.0/23
- Select gateway for given network

Set DHCP-Server (2)

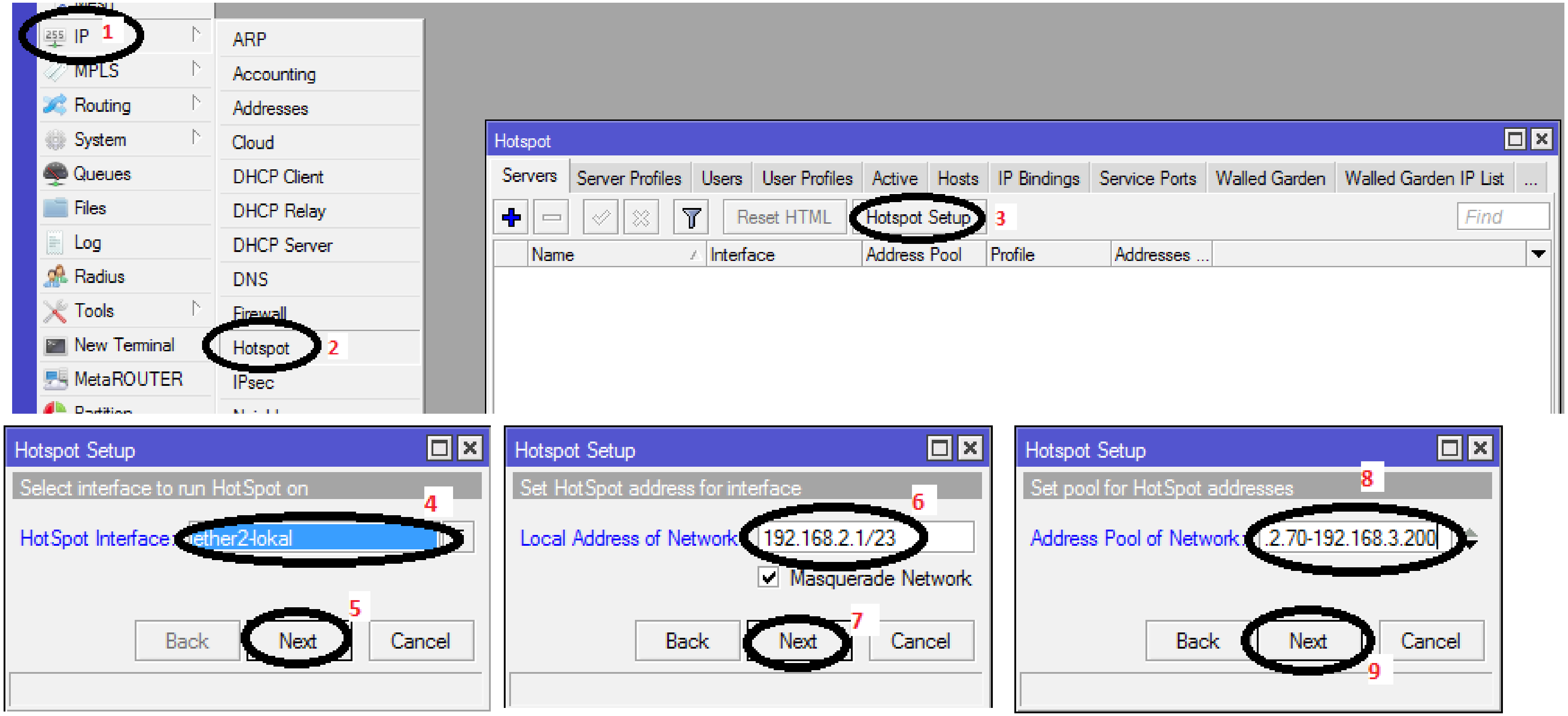
- gateway for dhcp network: 192.168.2.1
- Select pool of ip addresses given out by DHCP server
- addresses to give out: 192.168.2.70-192.168.3.200
- Select DNS servers
- dns servers: 192.168.2.1,192.168.20.1

- Select lease time
- lease time: 3d

Hotspot dan QoS

- Setup Hotspot
- Set IP Binding
- Set Walled Garden
- Set Hotspot User Profile untuk manajemen bandwidth
- Tampilan simple queues setelah terpasang Hotspot
- Tampilan NAT setelah terpasang Hotspot

Set Hotspot (1)



Select interface to run HotSpot on

HotSpot Interface: ether2-lokal

Set HotSpot address for interface

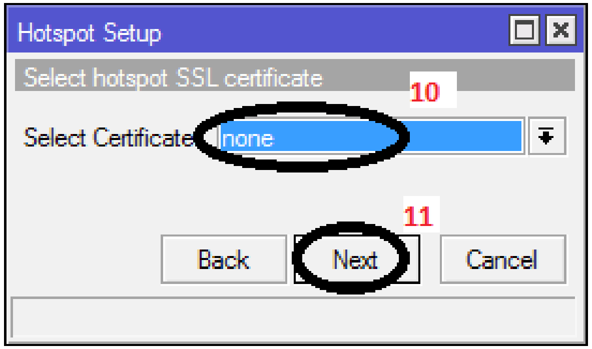
Local Address of Network: 192.168.2.1/23

☑ Masquerade Network

Set pool for HotSpot addresses

Address Pool of Network: .2.70-192.168.3.200

Set Hotspot (2)

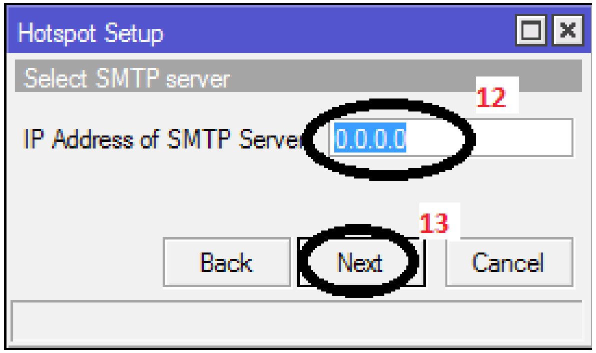


Hotspot Setup

Select hotspot SSL certificate

10 Select Certificate: none

11 Next

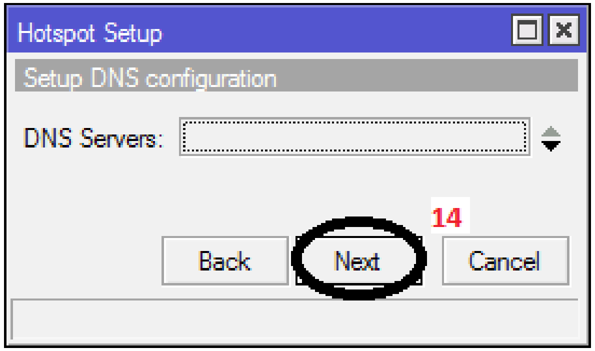


Hotspot Setup

Select SMTP server

12 IP Address of SMTP Server: 0.0.0.0

13 Next

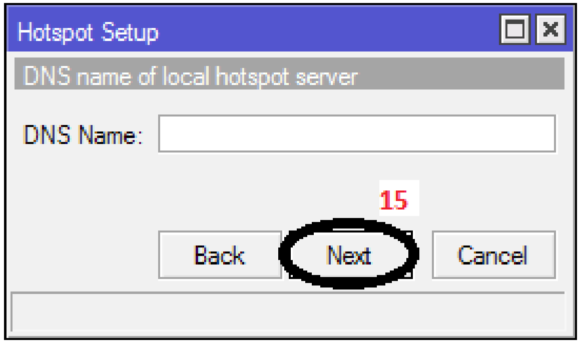


Hotspot Setup

Setup DNS configuration

DNS Servers:

14 Next

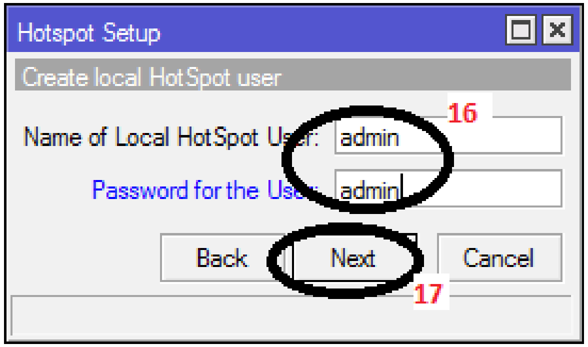


Hotspot Setup

DNS name of local hotspot server

DNS Name:

15 Next



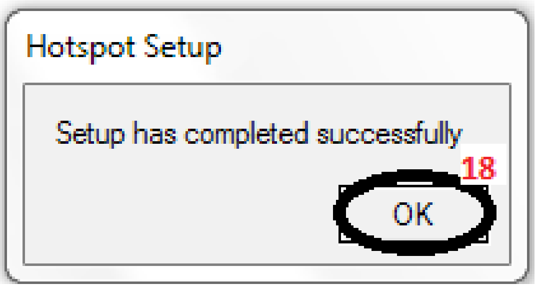
Hotspot Setup

Create local HotSpot user

16 Name of Local HotSpot User: admin

Password for the User: admin

17 Next



Hotspot Setup

Setup has completed successfully

18 OK

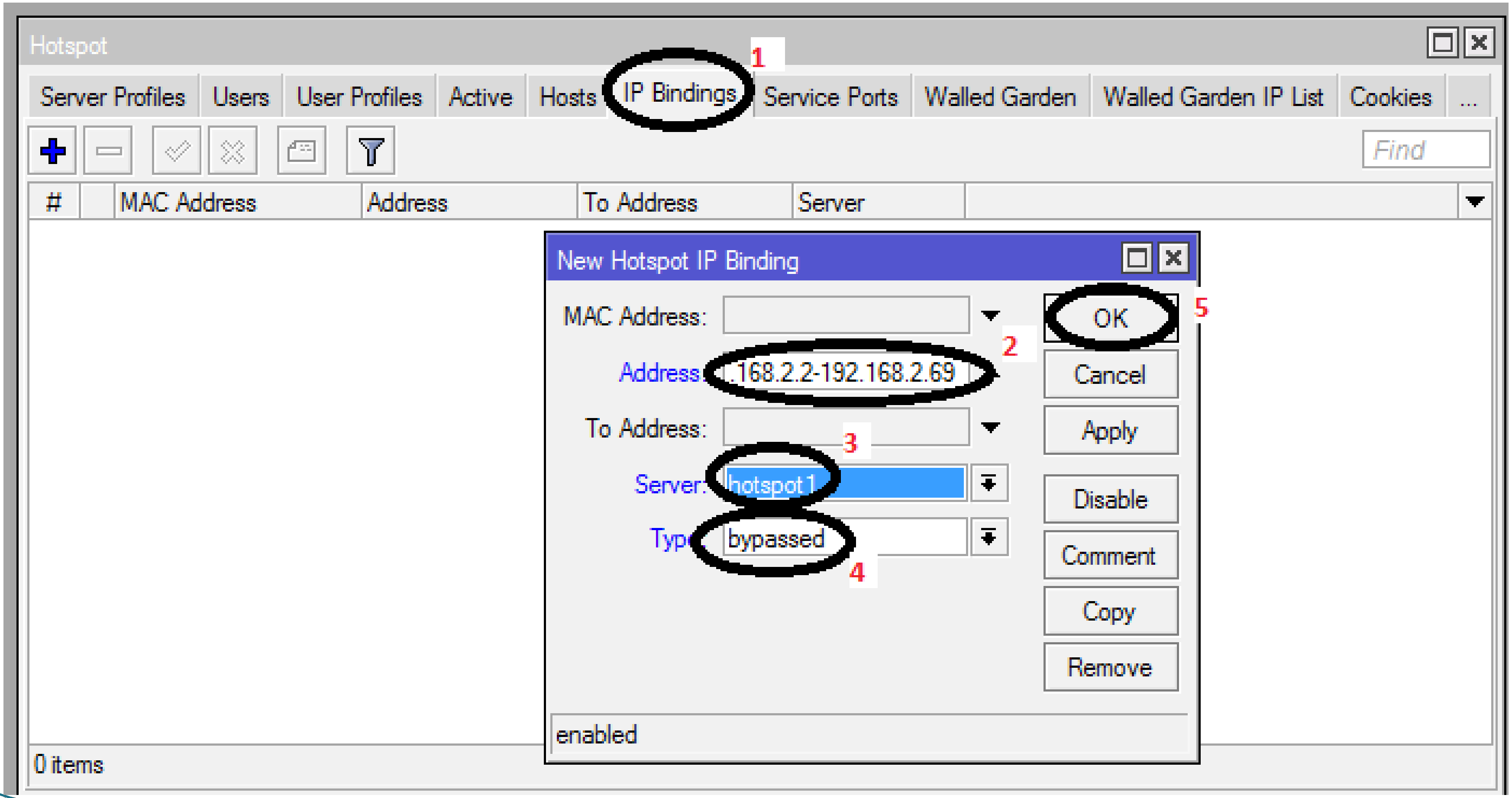
Set Hotspot (1)

- /ip hotspot setup
- Select interface to run HotSpot on
- hotspot interface: ether2-lokal
- Set HotSpot address for interface
- local address of network: 192.168.2.1/23
- masquerade network: yes
- Set pool for HotSpot addresses
- address pool of network: 192.168.2.70-192.168.3.200

Set Hotspot (2)

- Select hotspot SSL certificate
- select certificate: none
- Select SMTP server
- ip address of smtp server: 0.0.0.0
- Setup DNS configuration
- dns servers:
- DNS name of local hotspot server
- dns name:
- Create local hotspot user
- name of local hotspot user: admin
- password for the user: admin

Set IP binding Hotspot



MAC Address:

Address: .168.2.2-192.168.2.69

To Address:

Server: hotspot1

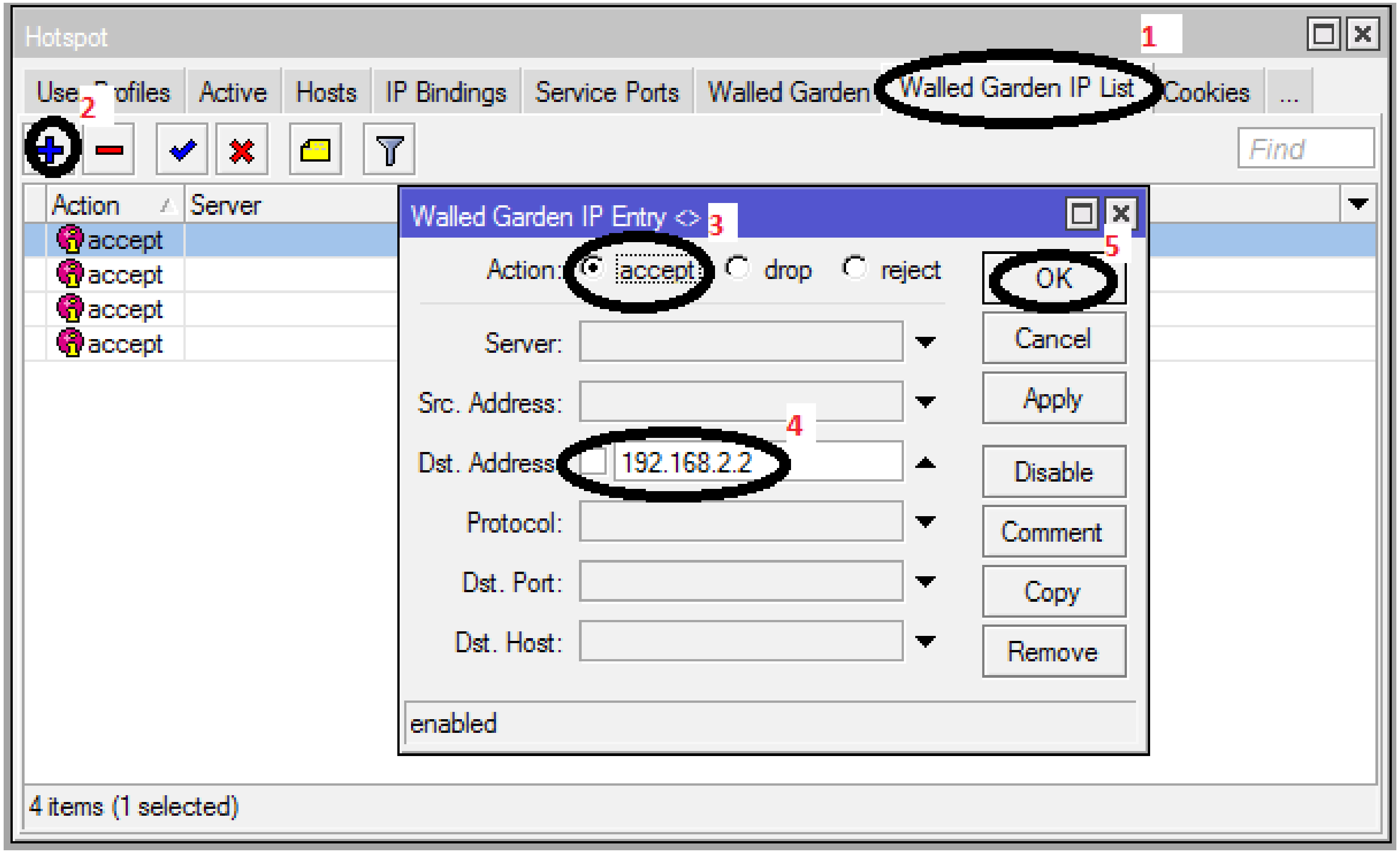
Type: bypassed

enabled

Set IP binding Hotspot

```
/ip hotspot ip-binding add
address=192.168.2.2-192.168.2.69
server=hotspot1 type=bypassed
```

Set Walled Garden Hotspot



Action: ● accept ○ drop ○ reject

Server:

Src. Address:

Dst. Address: □ 192.168.2.2

Protocol:

Dst. Port:

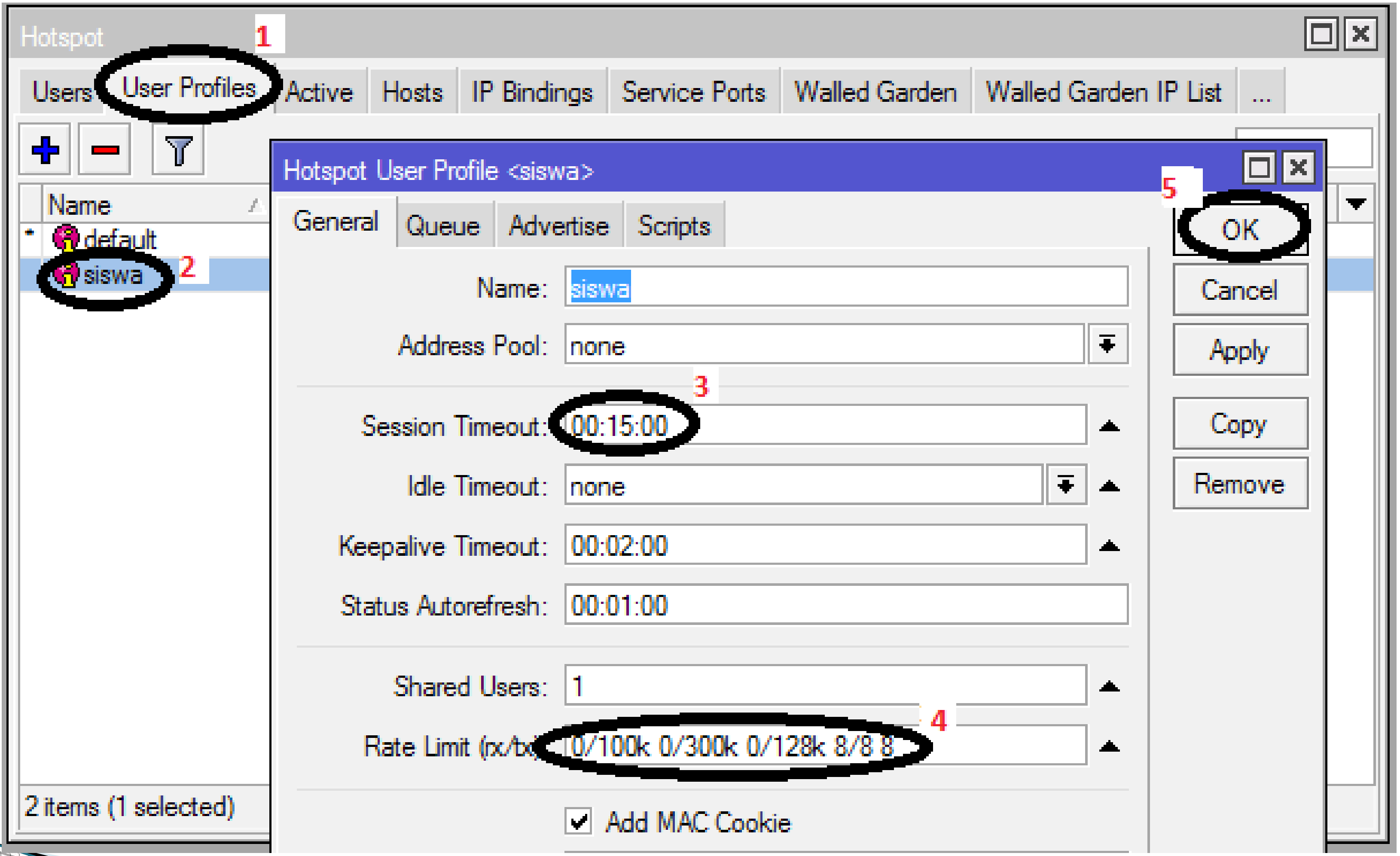
Dst. Host:

enabled

Set Walled Garden Hotspot

```
/ip hotspot walled-garden ip add action=accept disabled=no dst-address=192.168.2.2
```

Set Hotspot User Profile untuk manajemen bandwidth



Name: siswa

Address Pool: none

Session Timeout: 00:15:00

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

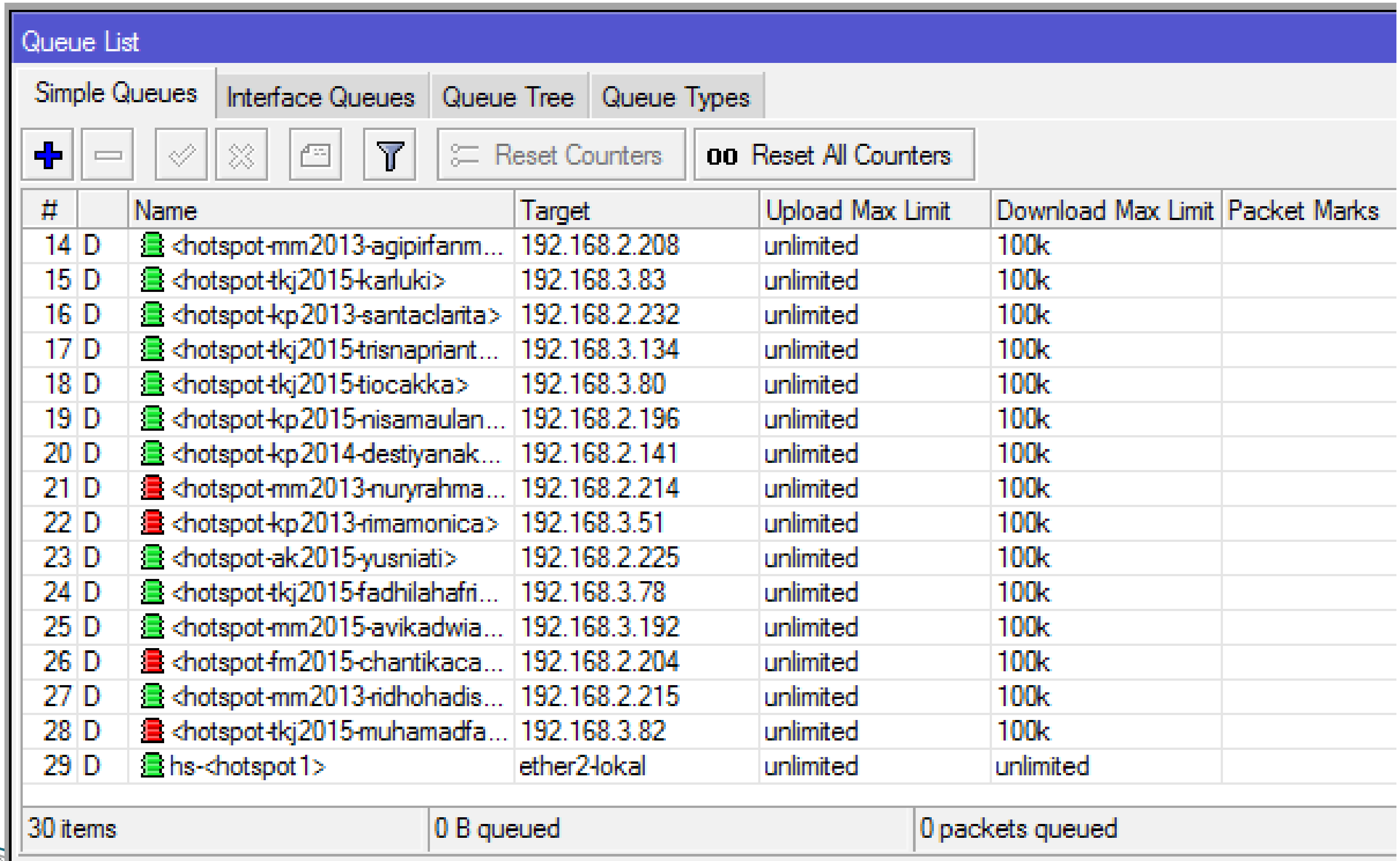
Rate Limit (rx/tx): 0/100k 0/300k 0/128k 8/8 8

☑ Add MAC Cookie

Set Hotspot User Profile untuk manajemen bandwidth

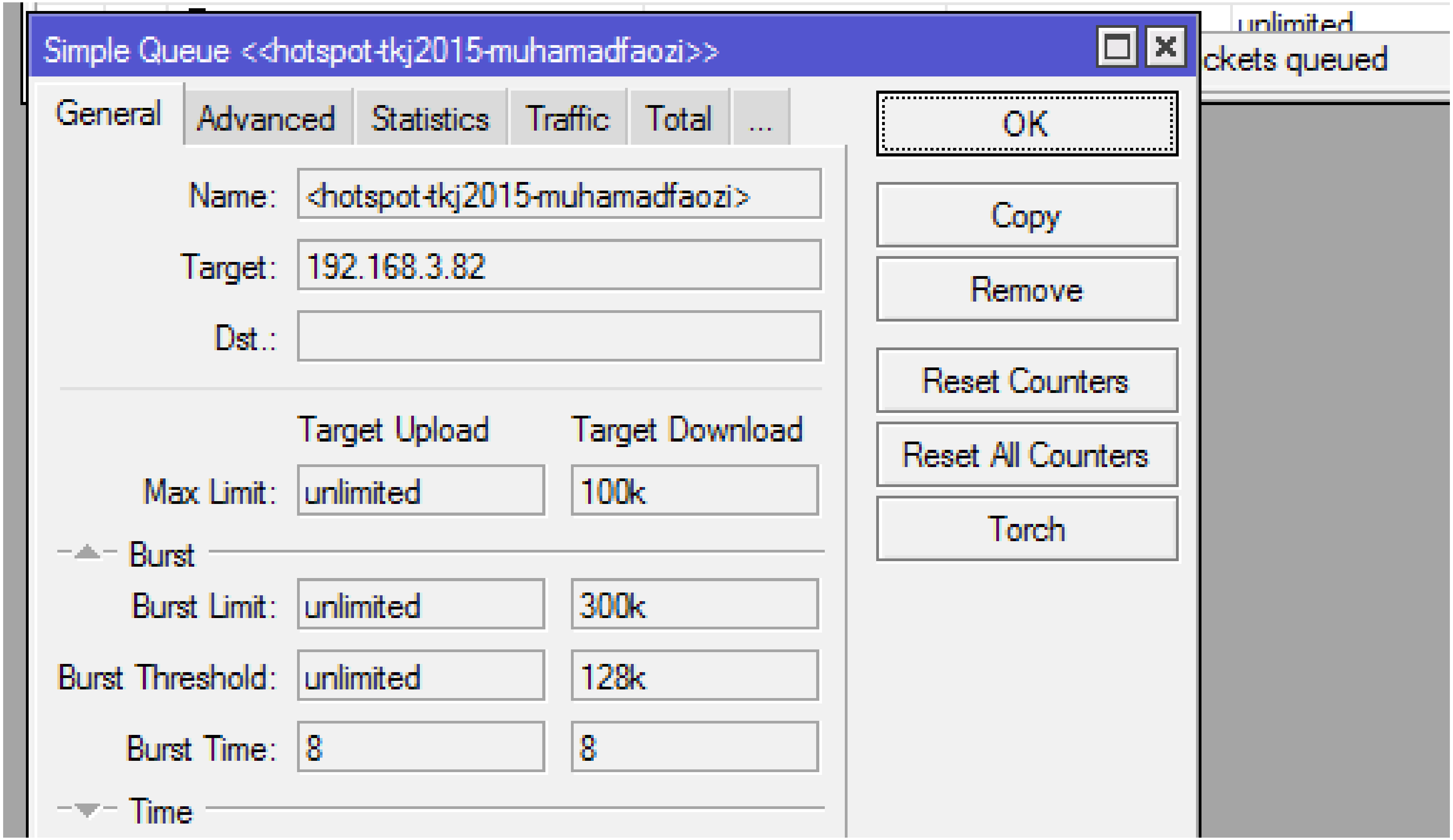
-
  ```
  /ip hotspot user profile add name=siswa rate-limit="0/100k 0/300k 0/128k 8/8 8" session-timeout=15m transparent-proxy=yes
  ```

Tampilan simple queues setelah terpasang Hotspot



#		Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
14	D	🟩 <hotspot-mm2013-agipirfanm...	192.168.2.208	unlimited	100k	
15	D	🟩 <hotspot-tkj2015-karluki>	192.168.3.83	unlimited	100k	
16	D	🟩 <hotspot-kp2013-santaclarita>	192.168.2.232	unlimited	100k	
17	D	🟩 <hotspot-tkj2015-trisnapriant...	192.168.3.134	unlimited	100k	
18	D	🟩 <hotspot-tkj2015-tiocakka>	192.168.3.80	unlimited	100k	
19	D	🟩 <hotspot-kp2015-nisamaulan...	192.168.2.196	unlimited	100k	
20	D	🟩 <hotspot-kp2014-destiyanak...	192.168.2.141	unlimited	100k	
21	D	🟥 <hotspot-mm2013-nuryrahma...	192.168.2.214	unlimited	100k	
22	D	🟥 <hotspot-kp2013-rimamonica>	192.168.3.51	unlimited	100k	
23	D	🟩 <hotspot-ak2015-yusniati>	192.168.2.225	unlimited	100k	
24	D	🟩 <hotspot-tkj2015-fadhilahafri...	192.168.3.78	unlimited	100k	
25	D	🟩 <hotspot-mm2015-avikadwia...	192.168.3.192	unlimited	100k	
26	D	🟥 <hotspot-fm2015-chantikaca...	192.168.2.204	unlimited	100k	
27	D	🟩 <hotspot-mm2013-ridhohadis...	192.168.2.215	unlimited	100k	
28	D	🟥 <hotspot-tkj2015-muhamadfa...	192.168.3.82	unlimited	100k	
29	D	🟩 hs-<hotspot1>	ether2-lokal	unlimited	unlimited	

30 items | 0 B queued | 0 packets queued



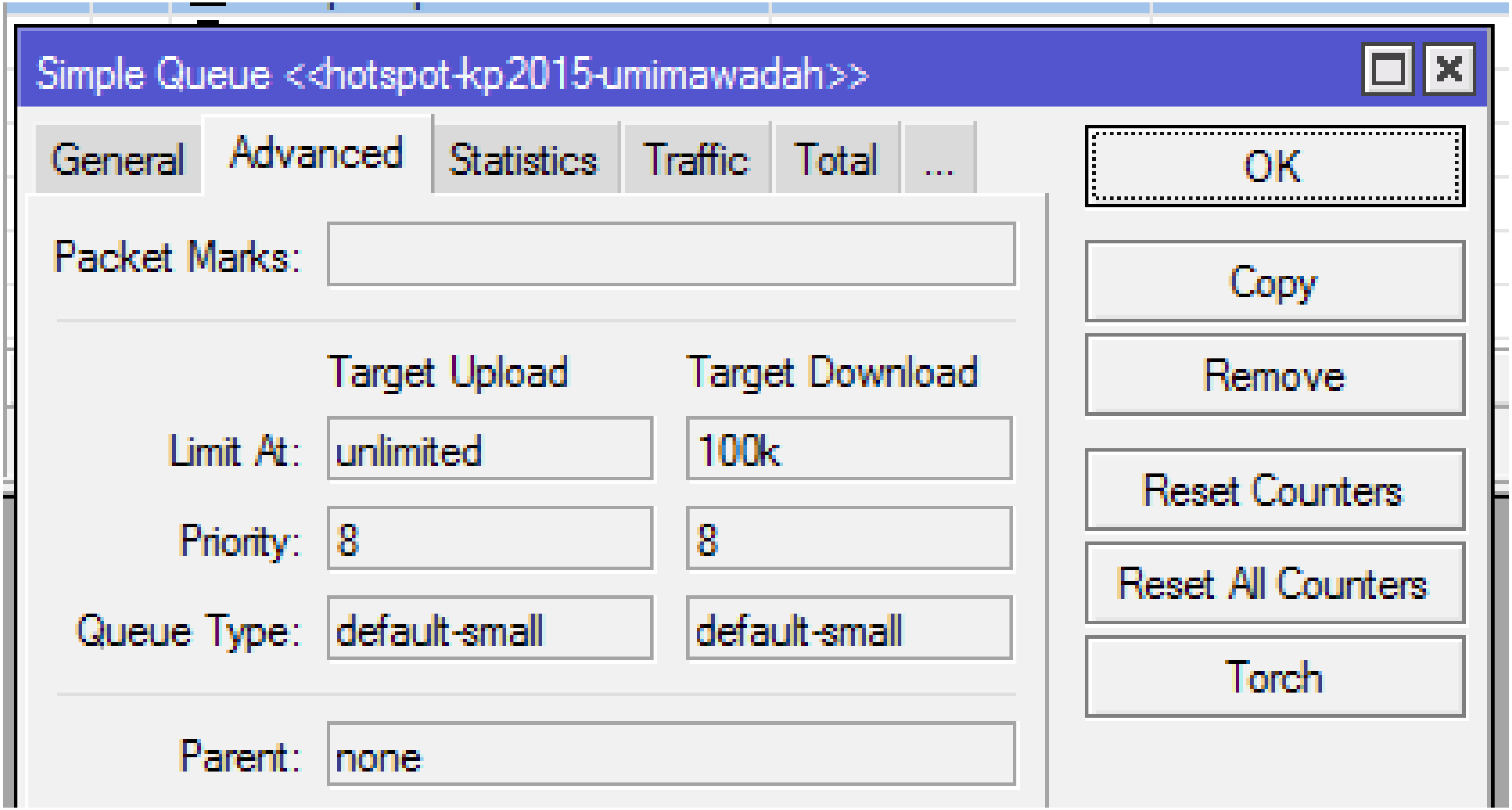
Simple Queue <<hotspot-tkj2015-muhamadfaozi>>

Name: <hotspot-tkj2015-muhamadfaozi>

Target: 192.168.3.82

Dst.:

	Target Upload	Target Download
Max Limit:	unlimited	100k
Burst Limit:	unlimited	300k
Burst Threshold:	unlimited	128k
Burst Time:	8	8

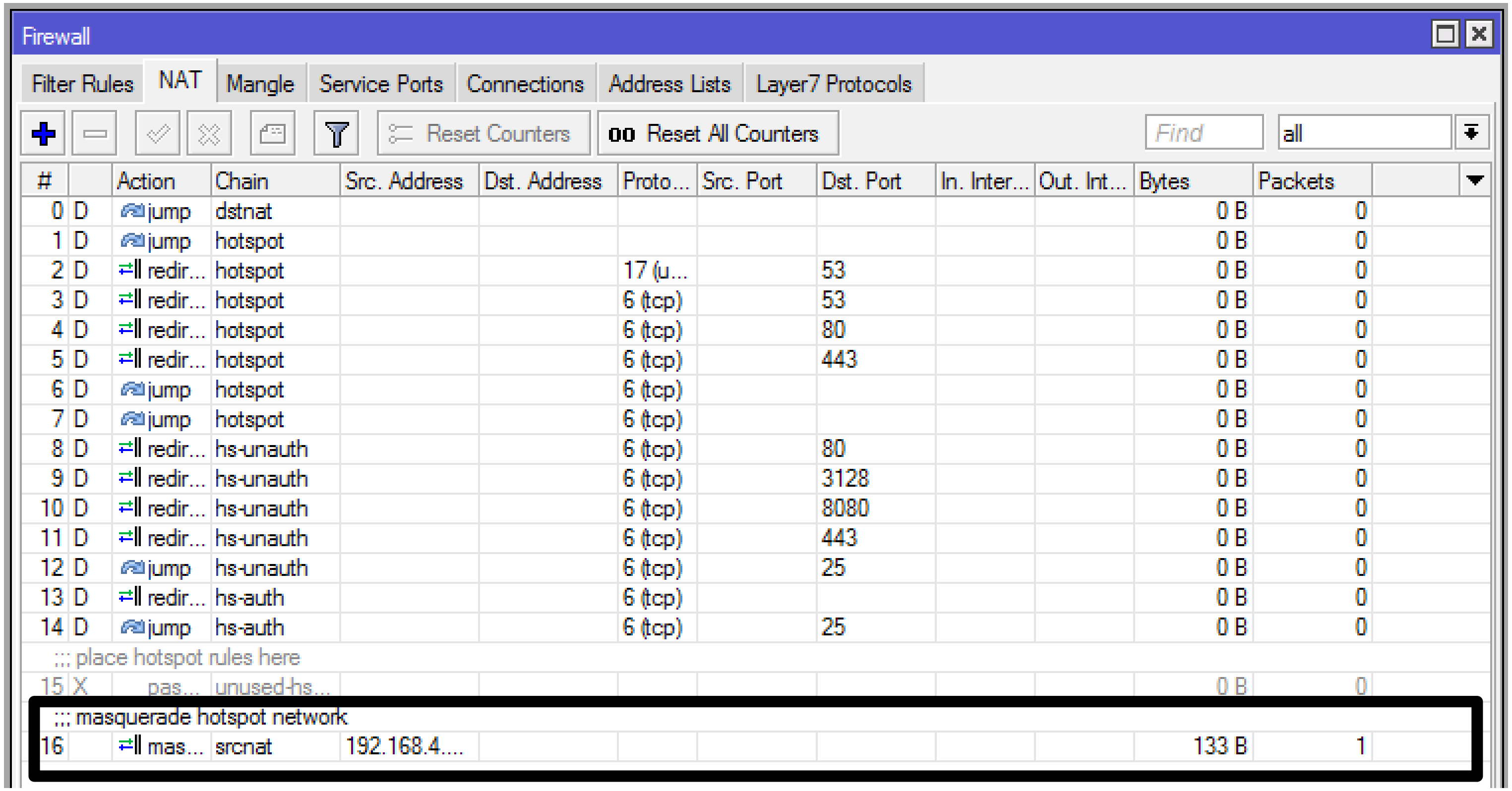

Simple Queue <<hotspot-kp2015-umimawadah>>

Packet Marks:

	Target Upload	Target Download
Limit At:	unlimited	100k
Priority:	8	8
Queue Type:	default-small	default-small

Parent: none

Tampilan NAT setelah terpasang Hotspot



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	D	jump	dstnat								0 B	0
1	D	jump	hotspot								0 B	0
2	D	redir...	hotspot			17 (u...		53			0 B	0
3	D	redir...	hotspot			6 (tcp)		53			0 B	0
4	D	redir...	hotspot			6 (tcp)		80			0 B	0
5	D	redir...	hotspot			6 (tcp)		443			0 B	0
6	D	jump	hotspot			6 (tcp)					0 B	0
7	D	jump	hotspot			6 (tcp)					0 B	0
8	D	redir...	hs-unauth			6 (tcp)		80			0 B	0
9	D	redir...	hs-unauth			6 (tcp)		3128			0 B	0
10	D	redir...	hs-unauth			6 (tcp)		8080			0 B	0
11	D	redir...	hs-unauth			6 (tcp)		443			0 B	0
12	D	jump	hs-unauth			6 (tcp)		25			0 B	0
13	D	redir...	hs-auth			6 (tcp)					0 B	0
14	D	jump	hs-auth			6 (tcp)		25			0 B	0
;;; place hotspot rules here												
15	X	pas...	unused-hs...								0 B	0
;;; masquerade hotspot network												
16		mas...	srcnat	192.168.4....							133 B	1

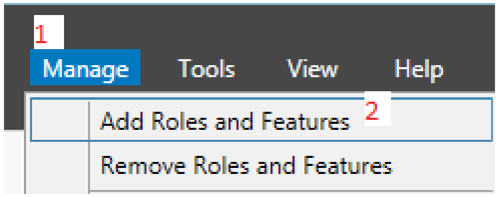
Integrasi dengan radius server dari win server 2012

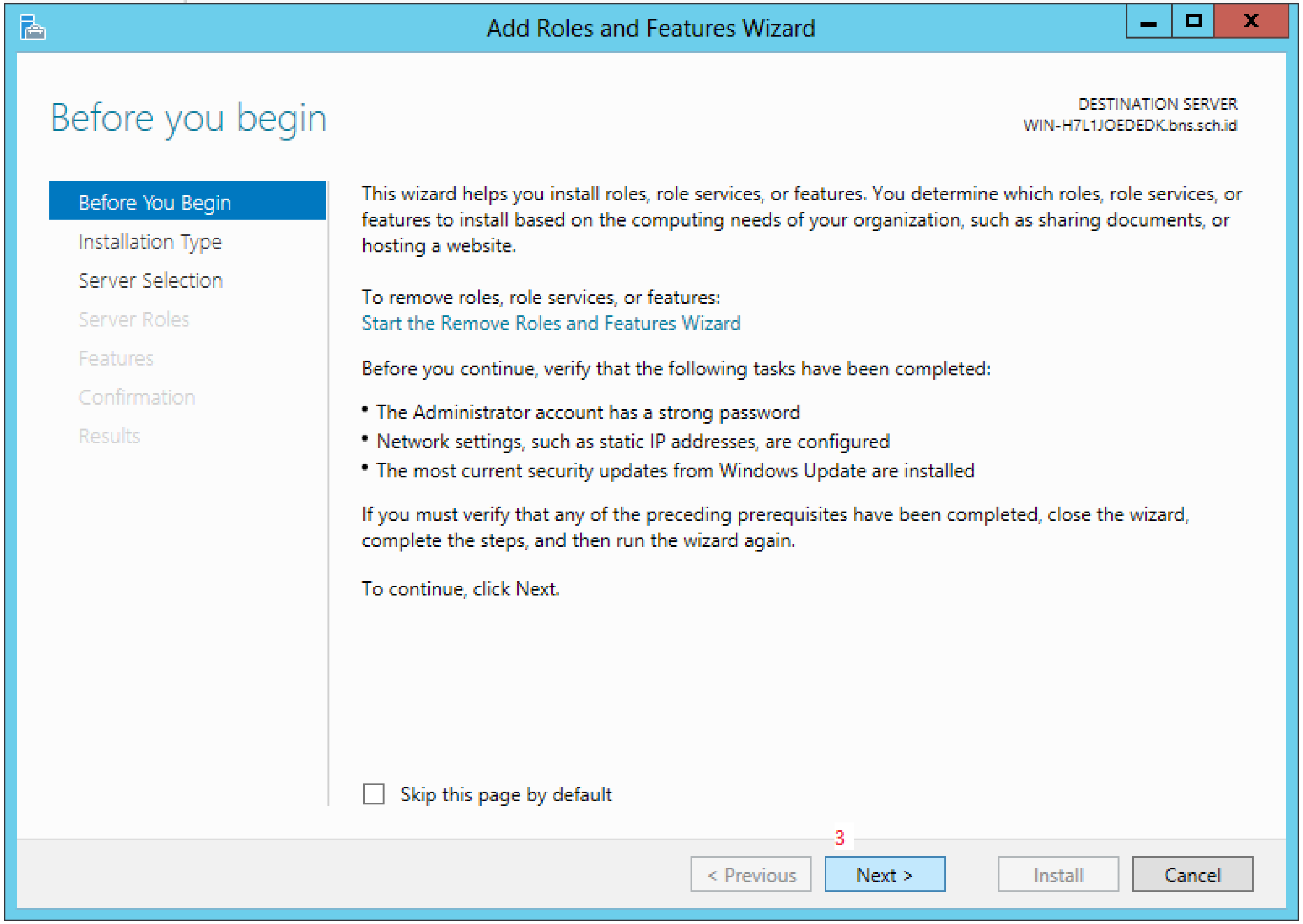
- Persiapan
- Instal NPAS (Network Policy and Access Services)
- Konfigurasi NPAS
- Konfigurasi Password Container
- Set Radius di Mikrotik
- Info tambahan integrasi radius server

Persiapan

- Pastikan sudah terinstal DNS server
- Pastikan sudah terinstal Active Directory
- Pastikan sudah di promote Active Directory-nya
- Pastikan sudah ada grup untuk user-user hotspot
- Pastikan ada user di grup untuk hotspot
- Pastikan IP server radius sudah ada di Binding dan ada di Walled Garden-nya hotspot

Instal NPAS





Before you begin

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

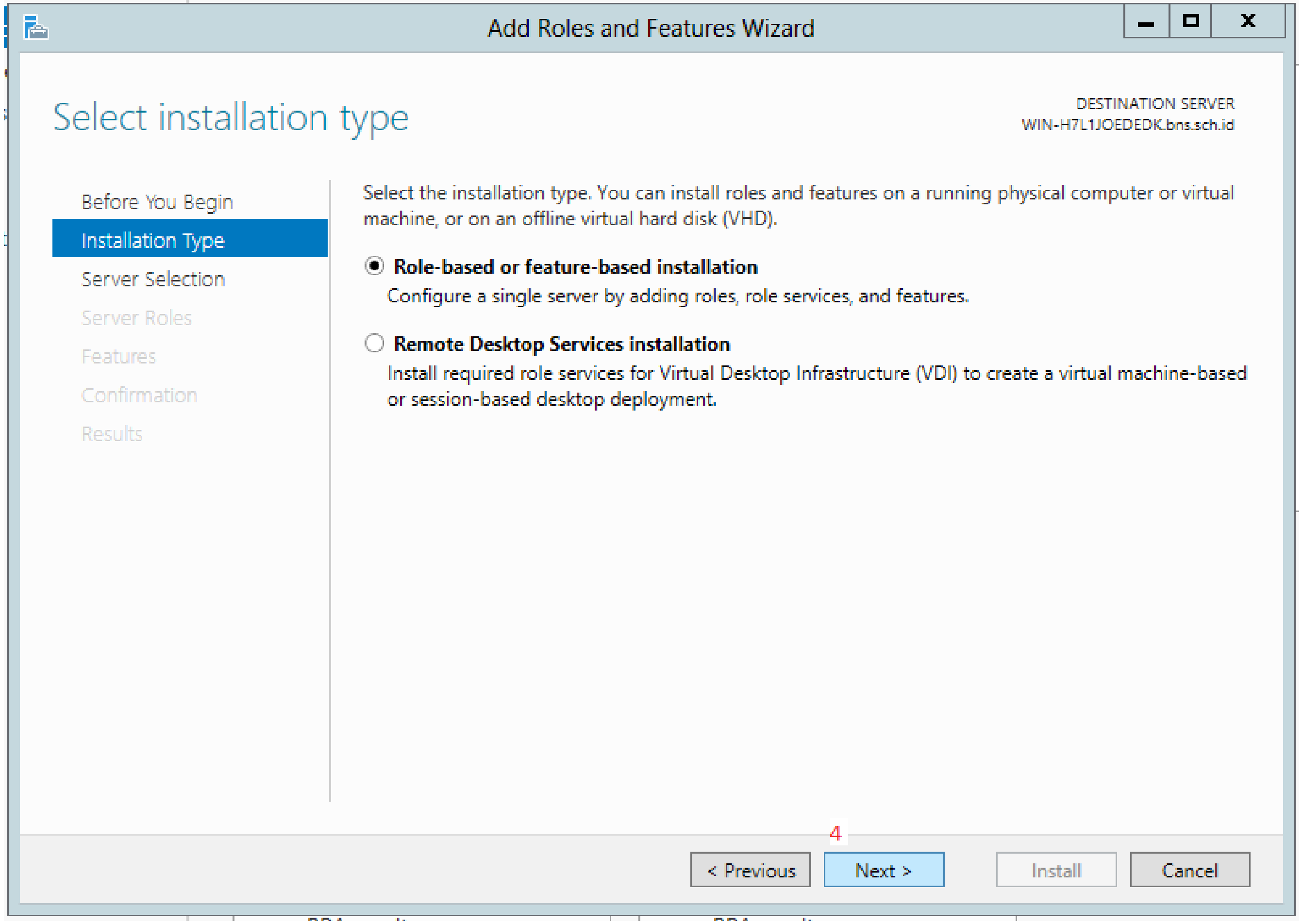
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

Instal NPAS



Select installation type

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

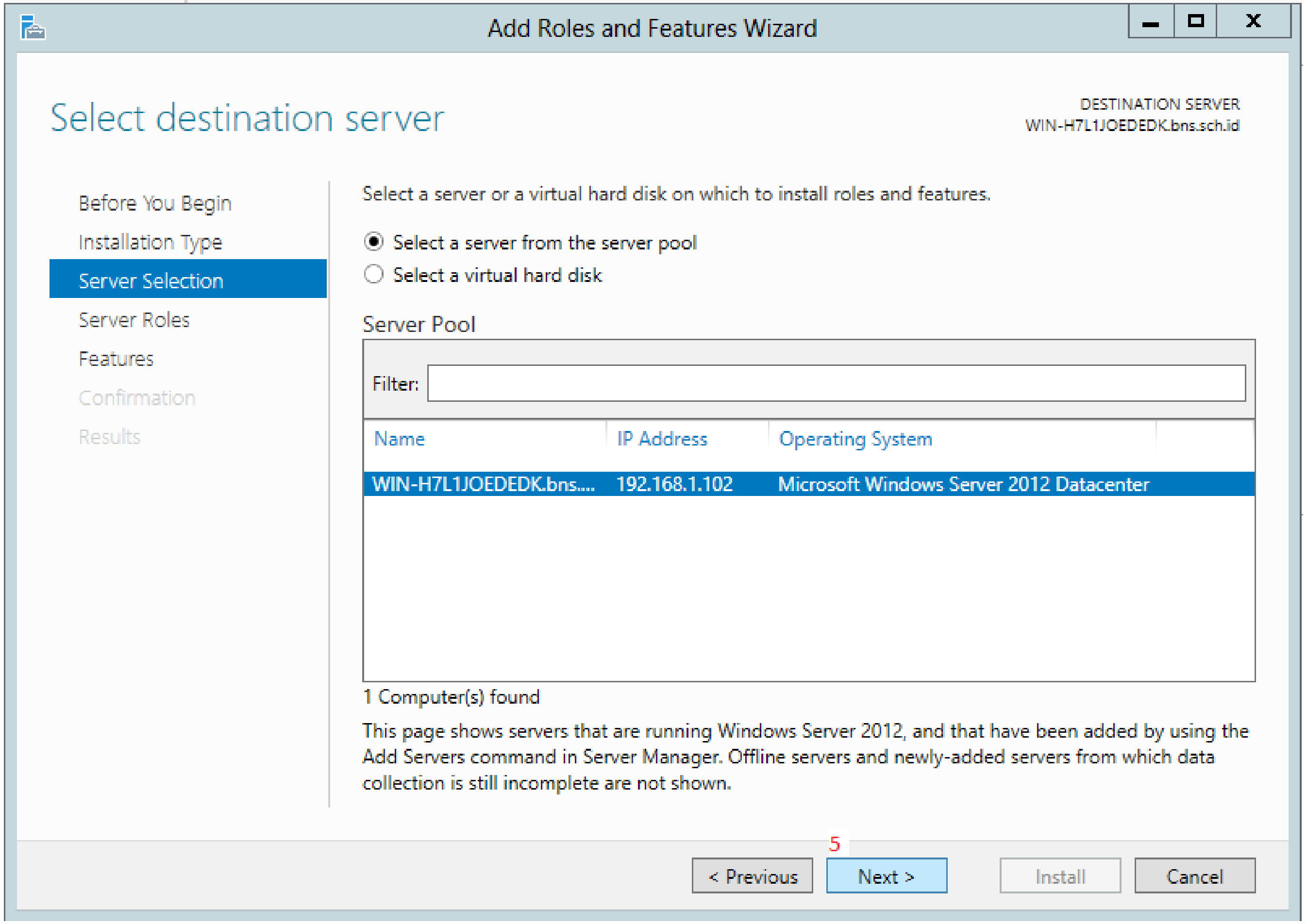
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **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.

4

Instal NPAS



Select destination server

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

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:

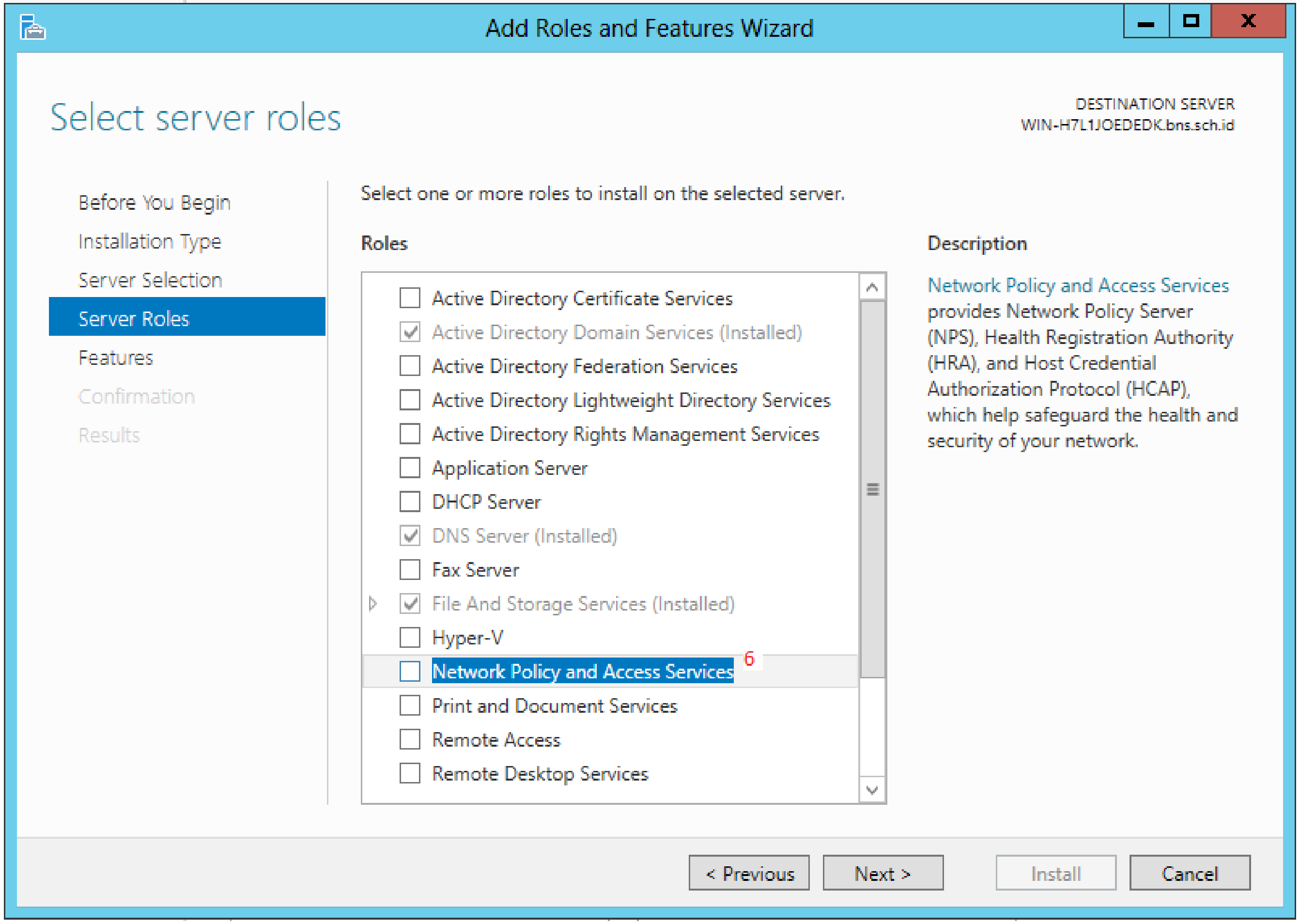
Name	IP Address	Operating System
WIN-H7L1JOEDEDK.bns....	192.168.1.102	Microsoft Windows Server 2012 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012, 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.

5

Instal NPAS



Select server roles

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

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

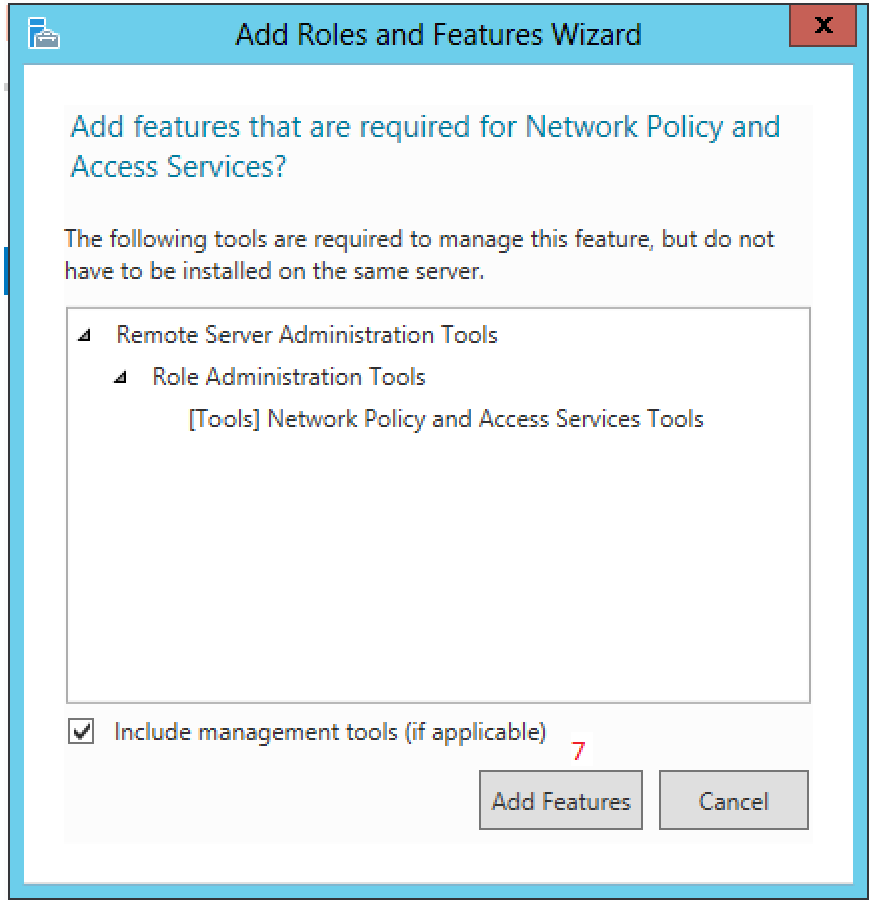
Roles

- ☐ 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
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services 6
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

Instal NPAS



Add features that are required for Network Policy and Access Services?

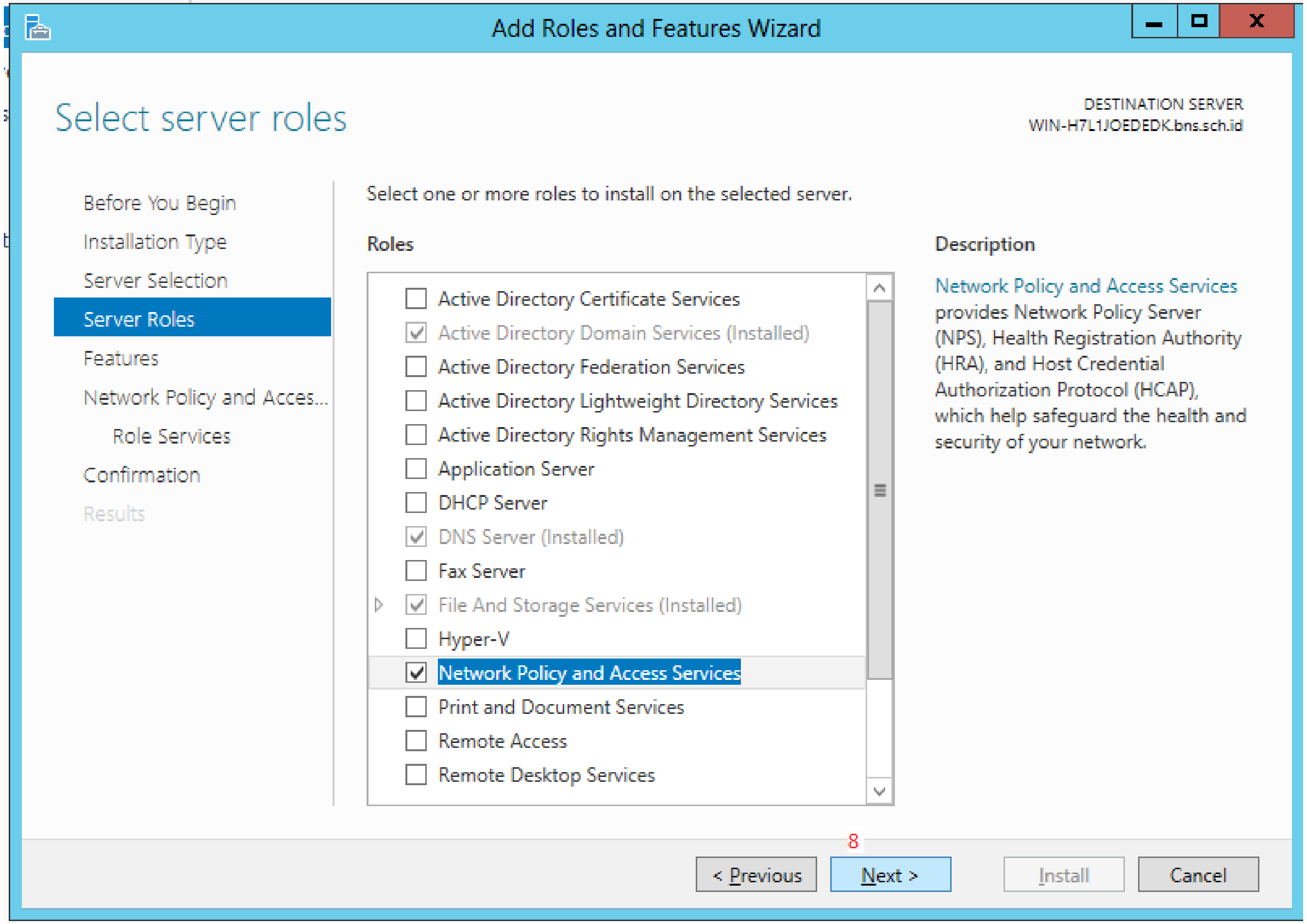
The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] Network Policy and Access Services Tools

☑ Include management tools (if applicable)

7

Instal NPAS



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

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

Roles

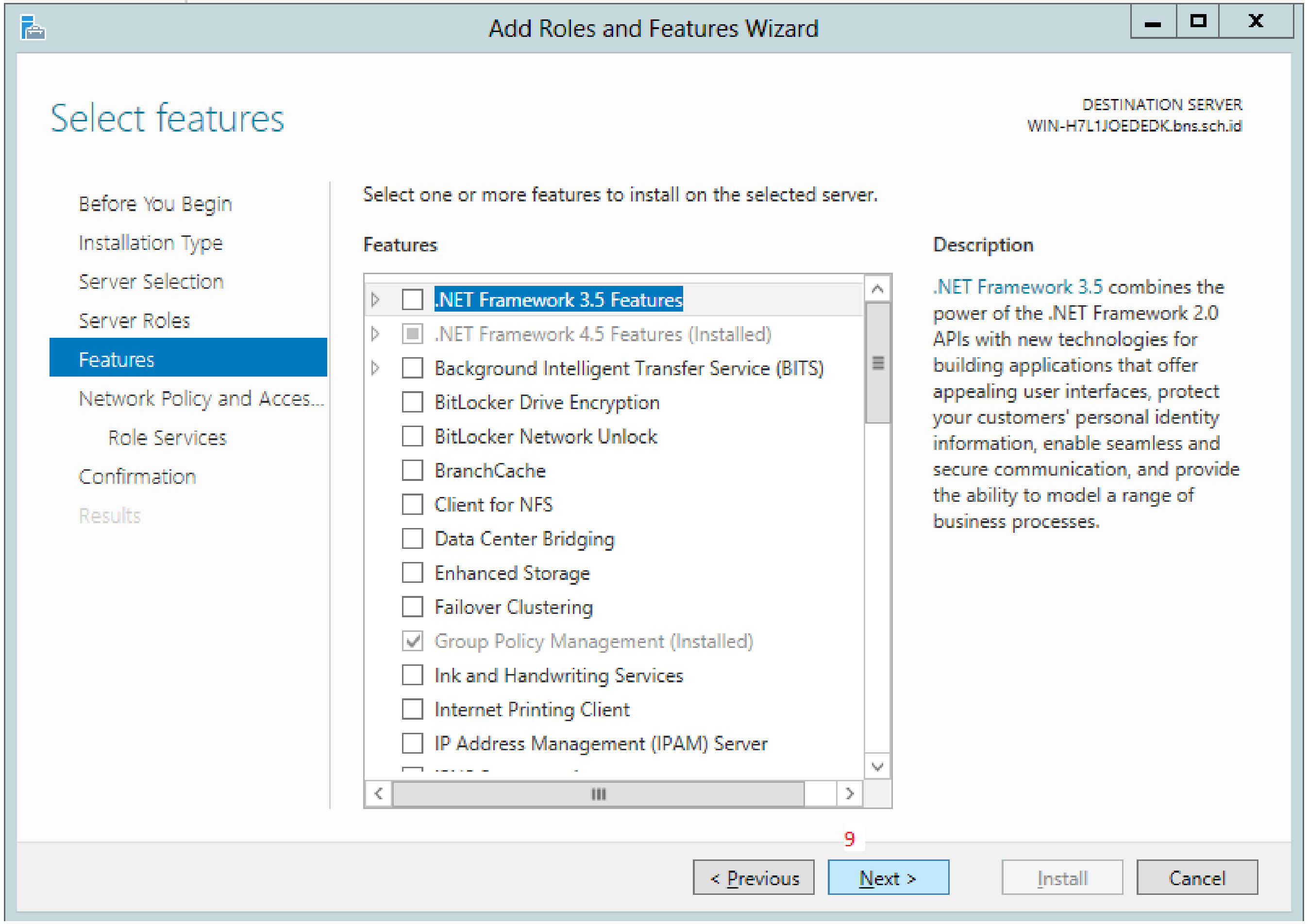
- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ File And Storage Services (Installed)
- ☐ Hyper-V
- ☑ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

8

Instal NPAS



Select features

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

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

Features

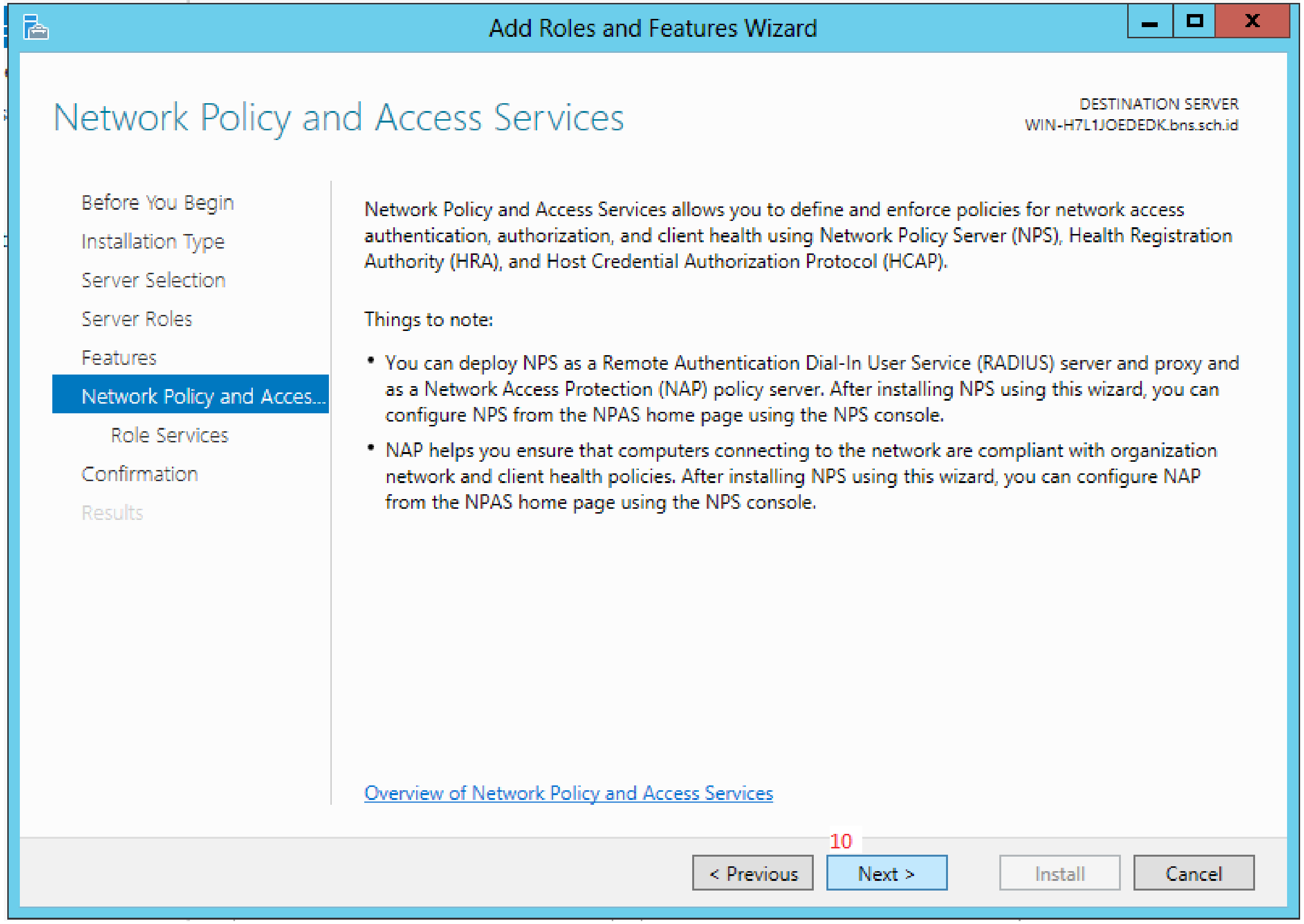
- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.5 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

9

Instal NPAS



Network Policy and Access Services

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

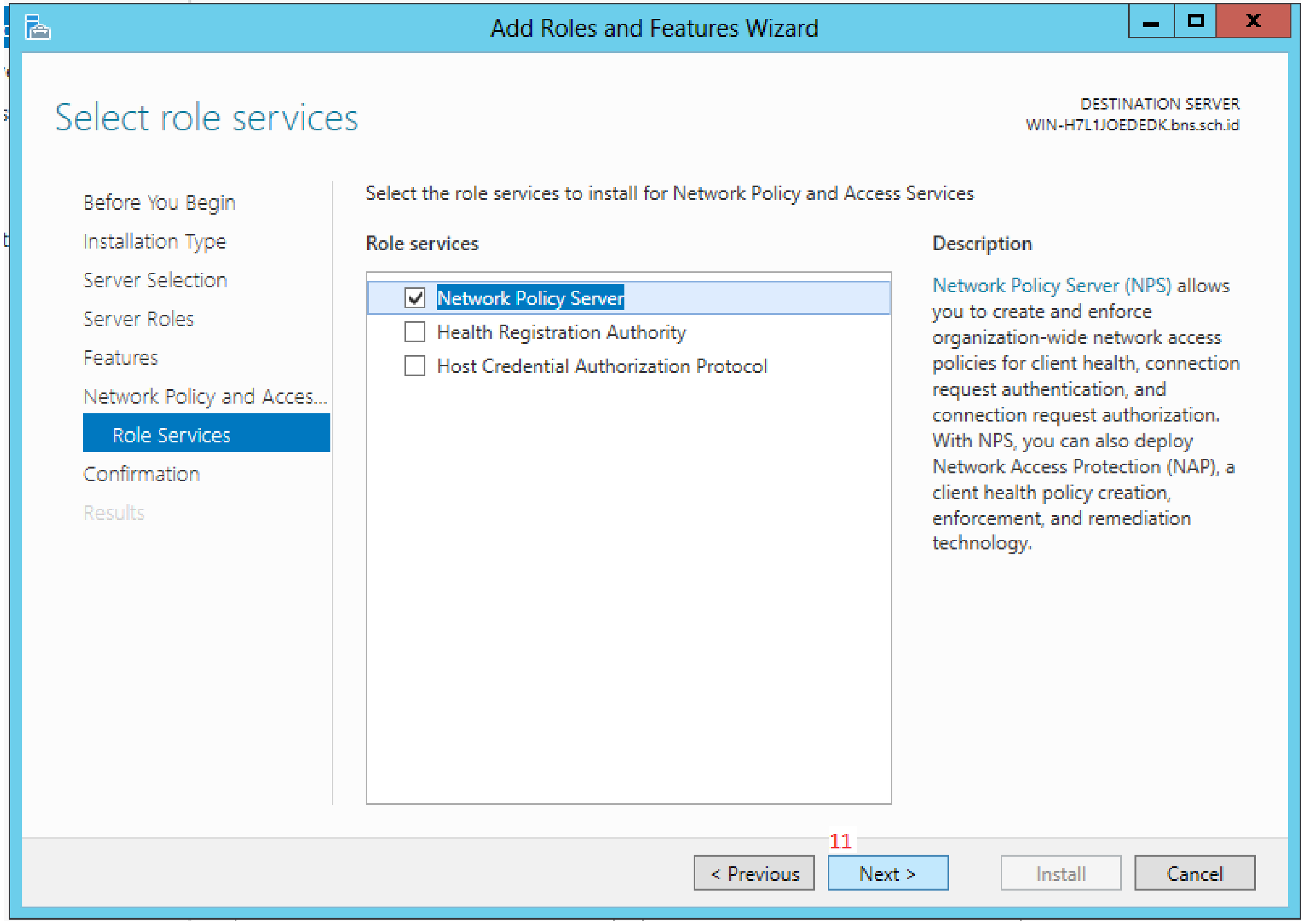
Network Policy and Access Services allows you to define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

Things to note:

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.
- NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NAP from the NPAS home page using the NPS console.

Overview of Network Policy and Access Services

Instal NPAS



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

Select the role services to install for Network Policy and Access Services

Role services

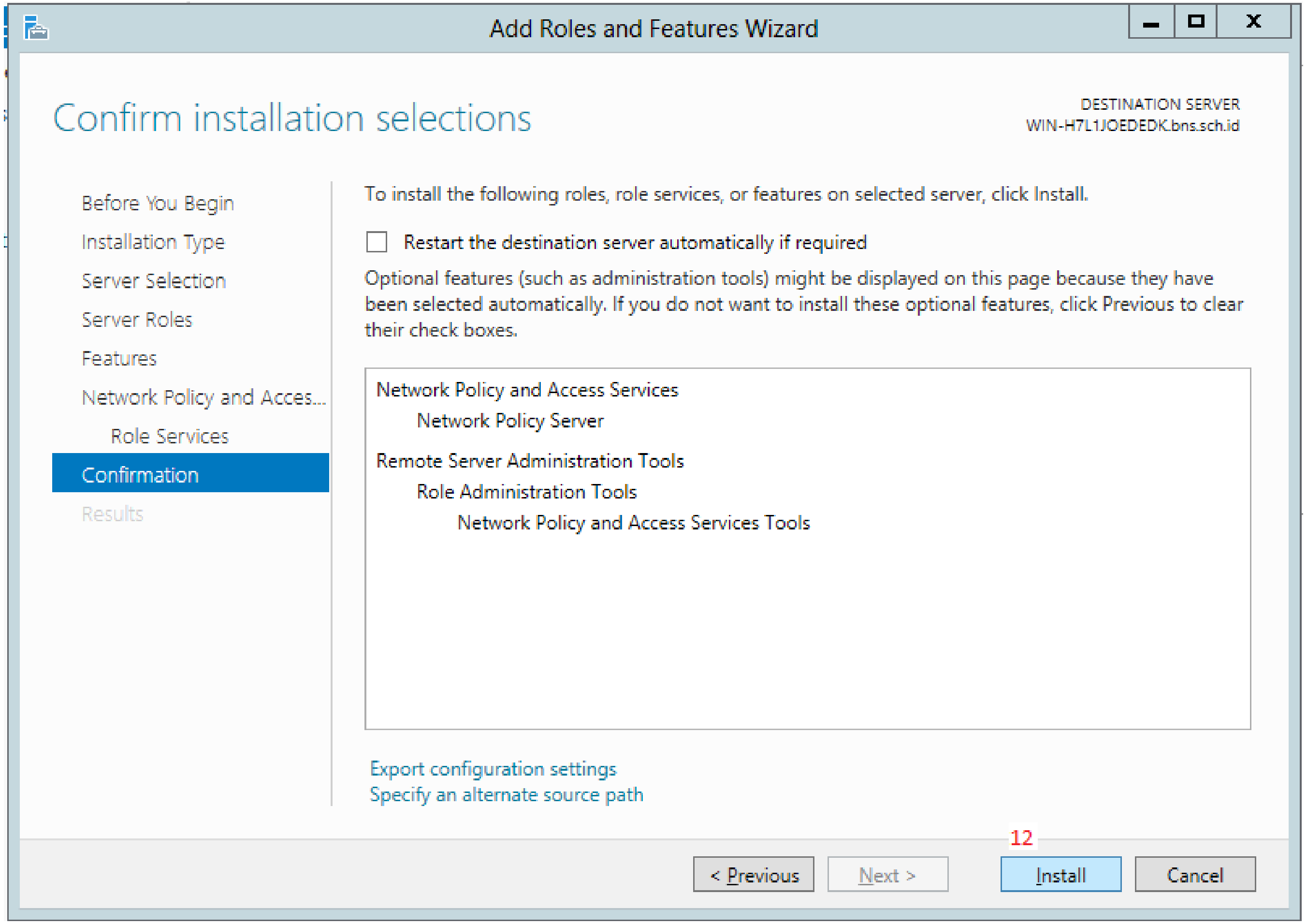
☑ Network Policy Server
□ Health Registration Authority
□ Host Credential Authorization Protocol

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.

11

Instal NPAS



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

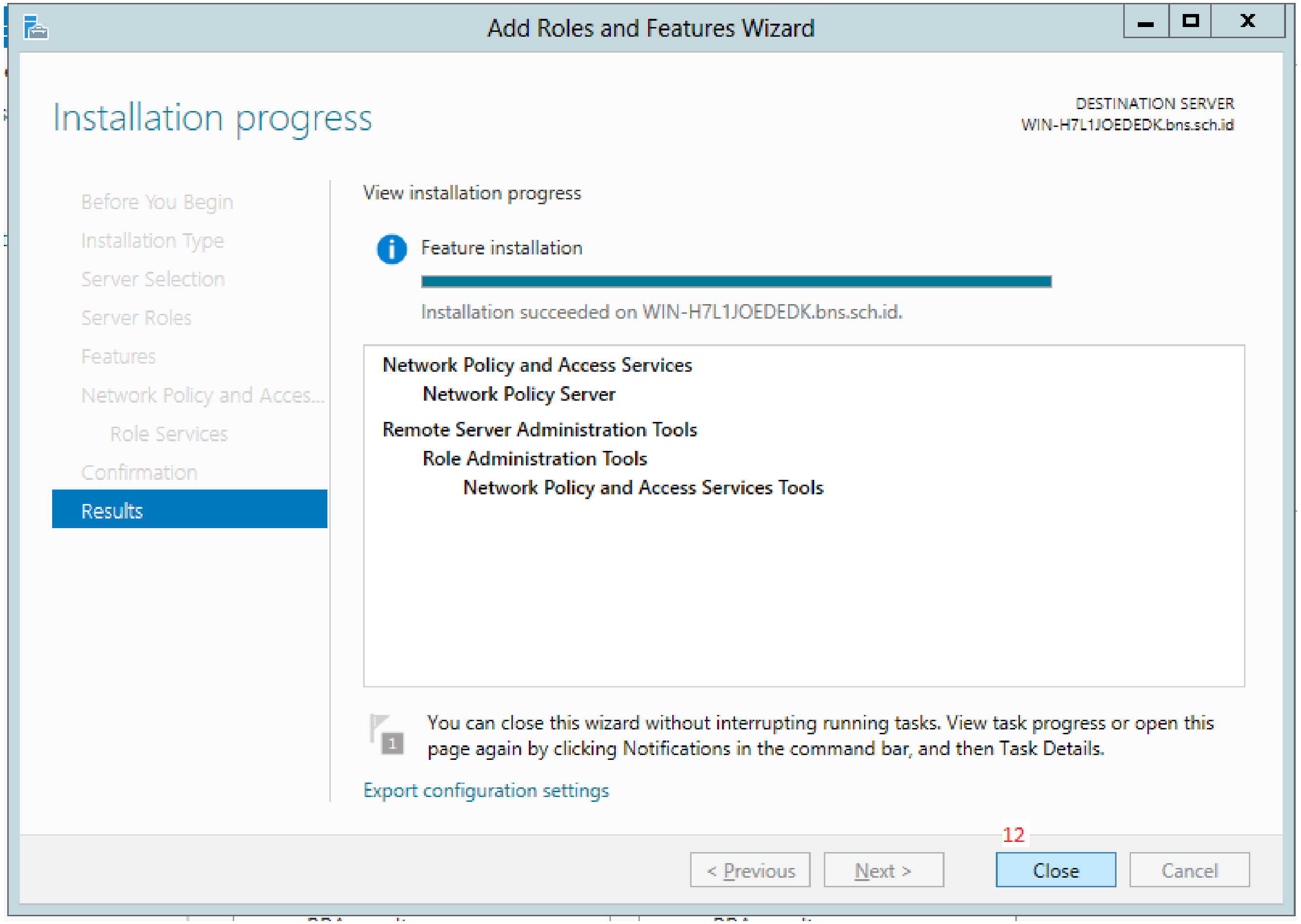
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Network Policy and Access Services
- Network Policy Server

Remote Server Administration Tools
- Role Administration Tools
  - Network Policy and Access Services Tools

Export configuration settings
Specify an alternate source path
12
< Previous
Next >
Install
Cancel

Instal NPAS



Installation progress

DESTINATION SERVER
WIN-H7L1JOEDEDK.bns.sch.id

View installation progress

Feature installation

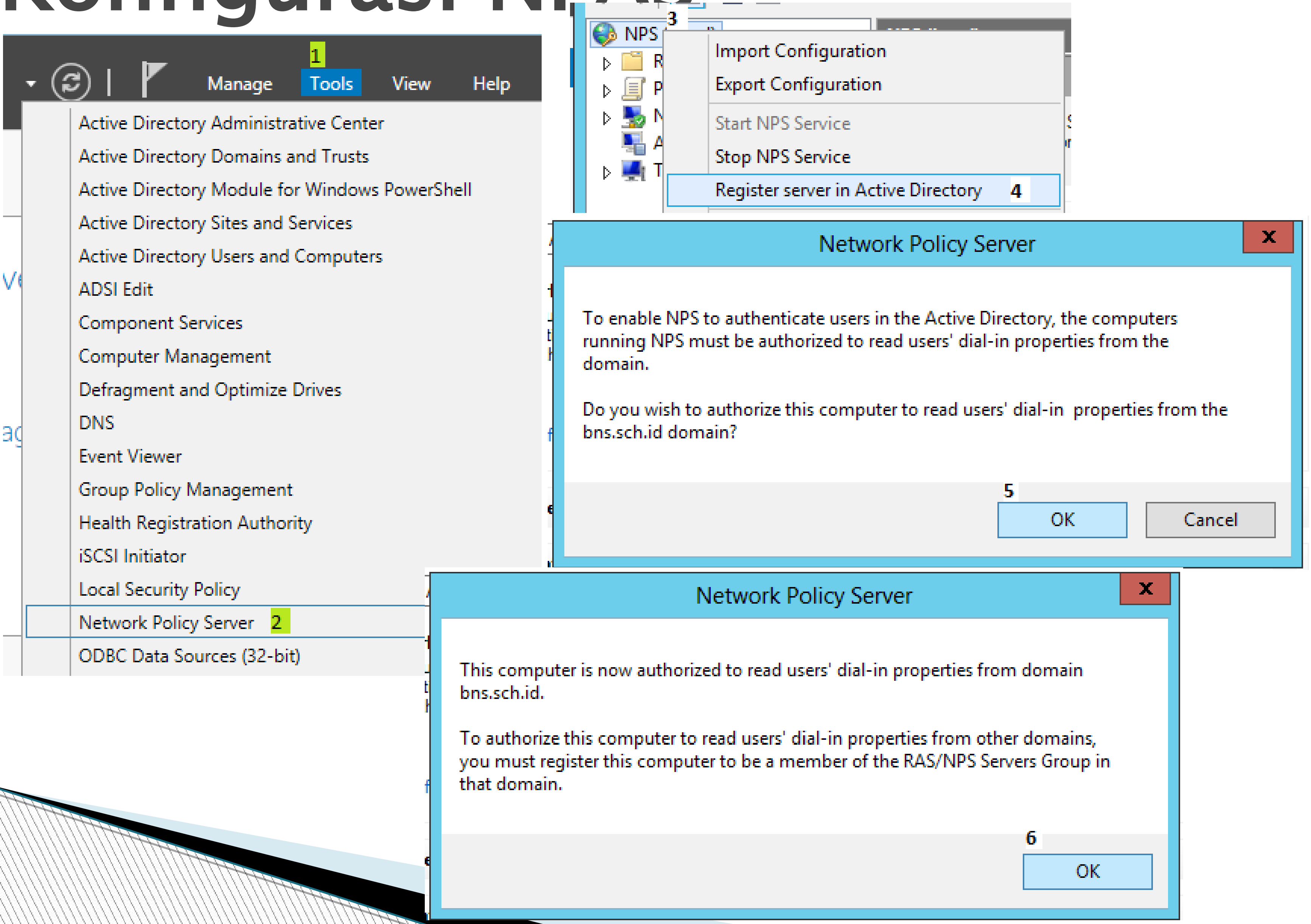
Installation succeeded on WIN-H7L1JOEDEDK.bns.sch.id.

Network Policy and Access Services
  Network Policy Server
Remote Server Administration Tools
  Role Administration Tools
    Network Policy and Access Services Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Konfigurasi NPAS



Manage
1
Tools
View
Help
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
DNS
Event Viewer
Group Policy Management
Health Registration Authority
iSCSI Initiator
Local Security Policy
Network Policy Server 2
ODBC Data Sources (32-bit)
3
NPS
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory 4
Network Policy Server
5
OK
Cancel
Network Policy Server
6
OK

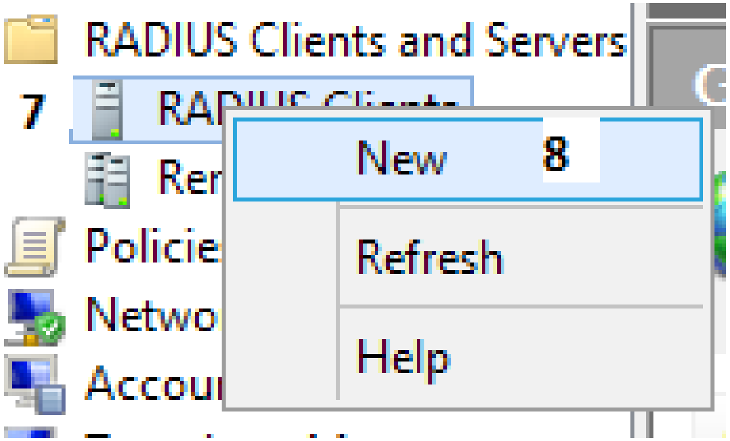
To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

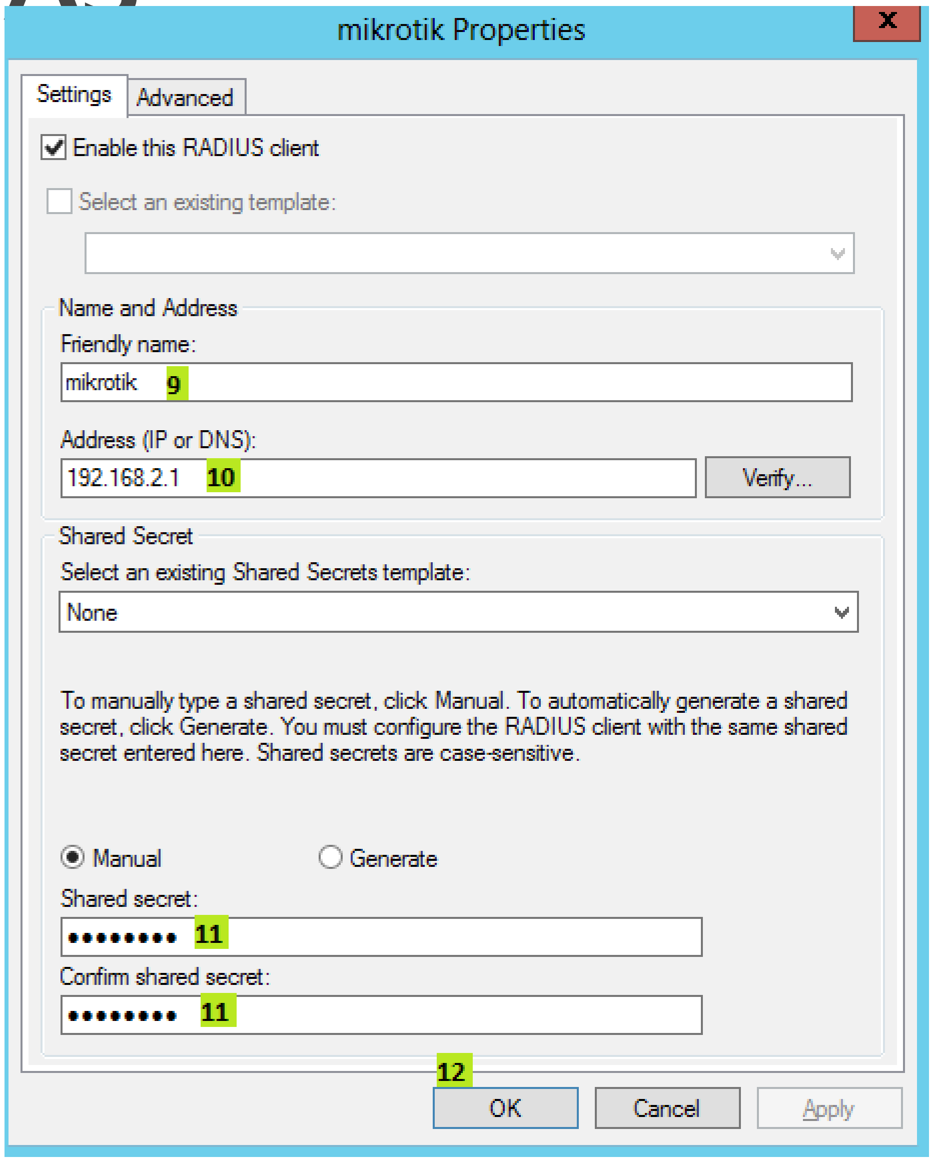
Do you wish to authorize this computer to read users' dial-in properties from the bns.sch.id domain?

This computer is now authorized to read users' dial-in properties from domain bns.sch.id.

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

Konfigurasi NPAS





mikrotik Properties

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: mikrotik 9

Address (IP or DNS): 192.168.2.1 10 [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

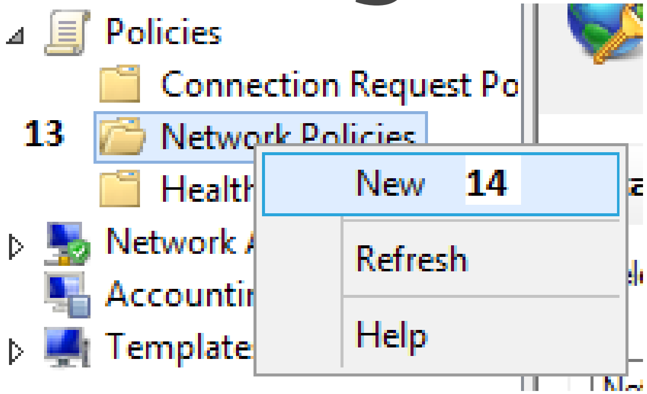
Shared secret: ••••••••• 11

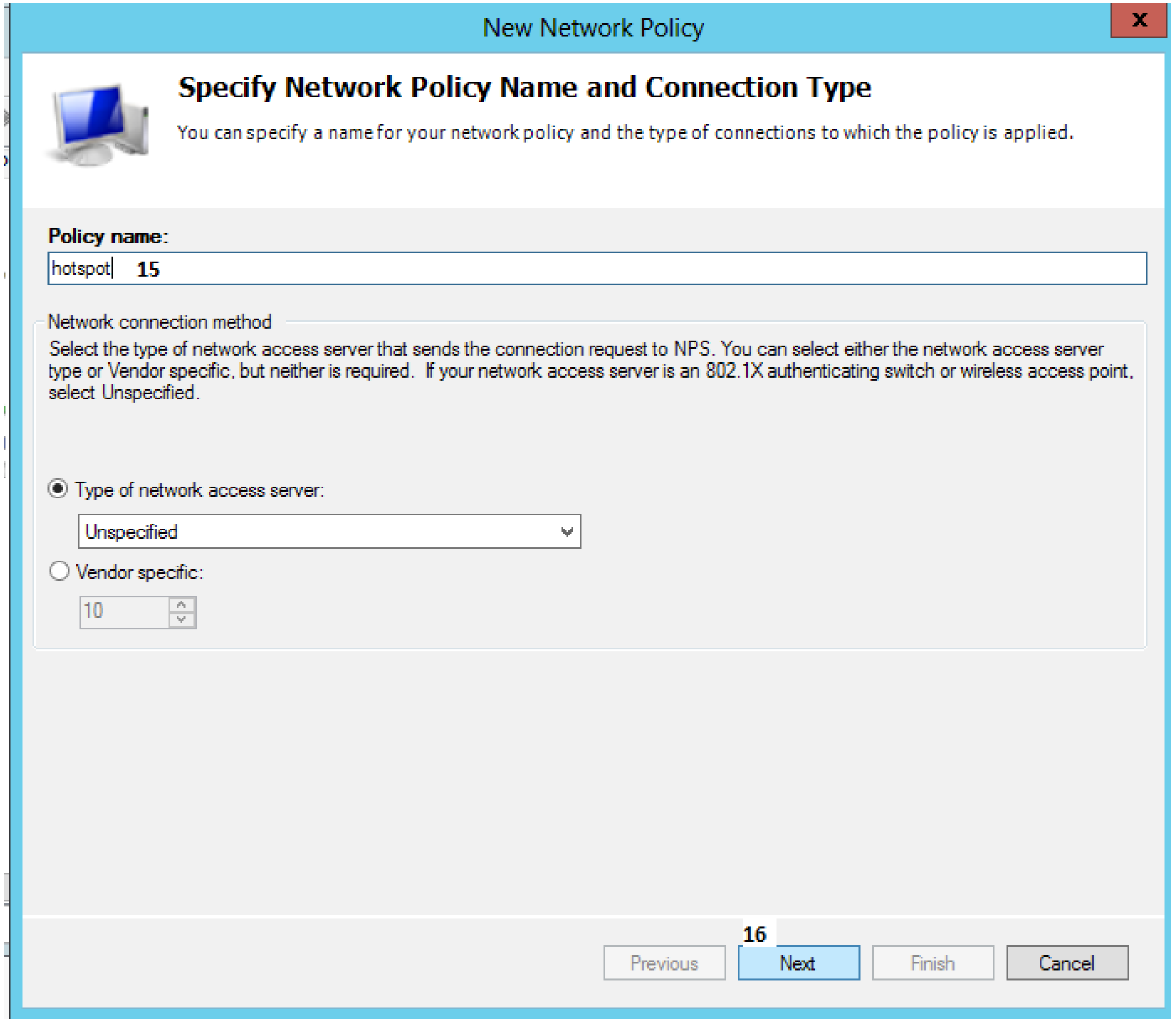
Confirm shared secret: ••••••••• 11

12

[OK] [Cancel] [Apply]

Konfigurasi NPAS





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:

hotspot 15

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:

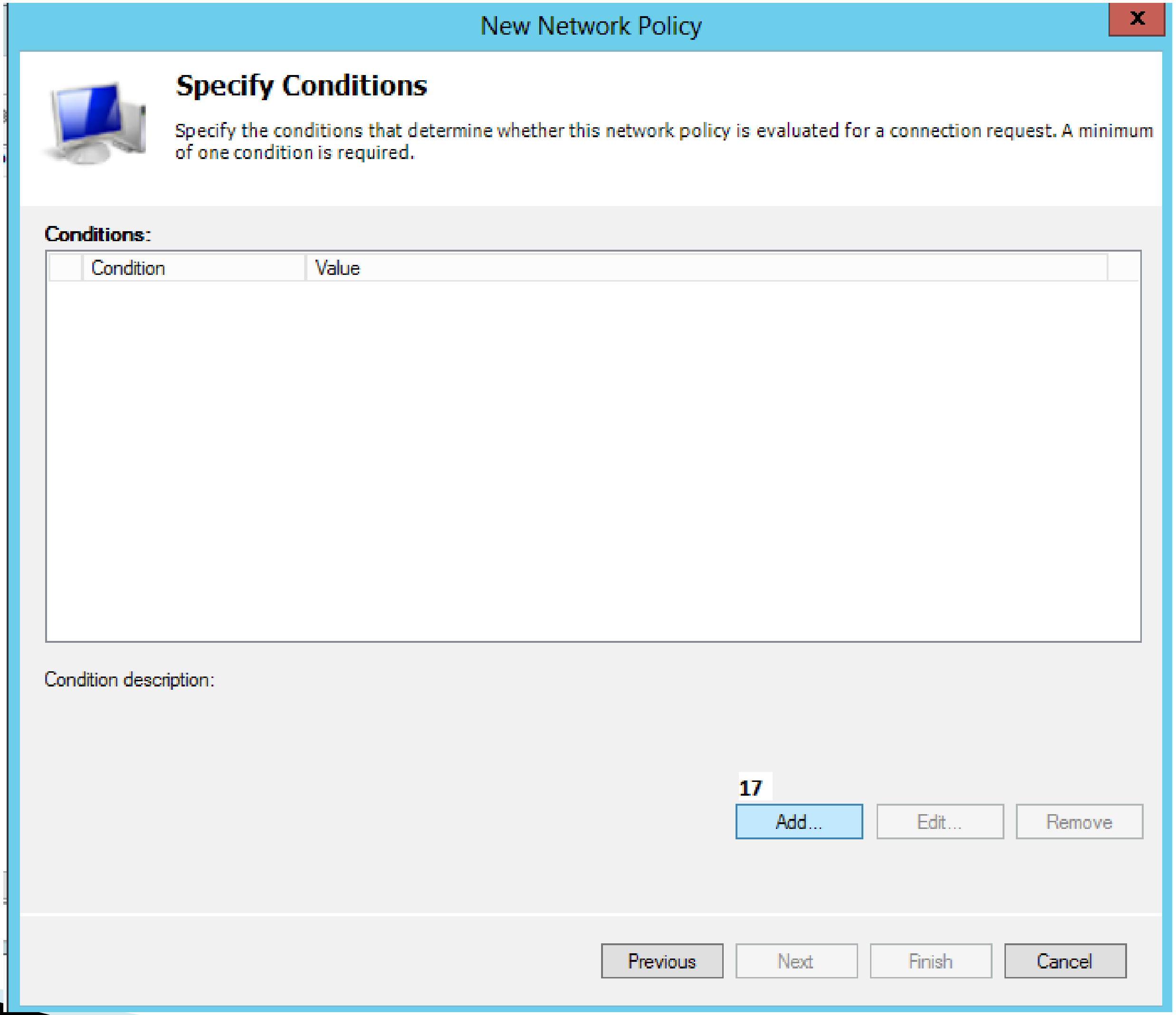
Unspecified

○ Vendor specific:

10

16

Konfigurasi NPAS



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

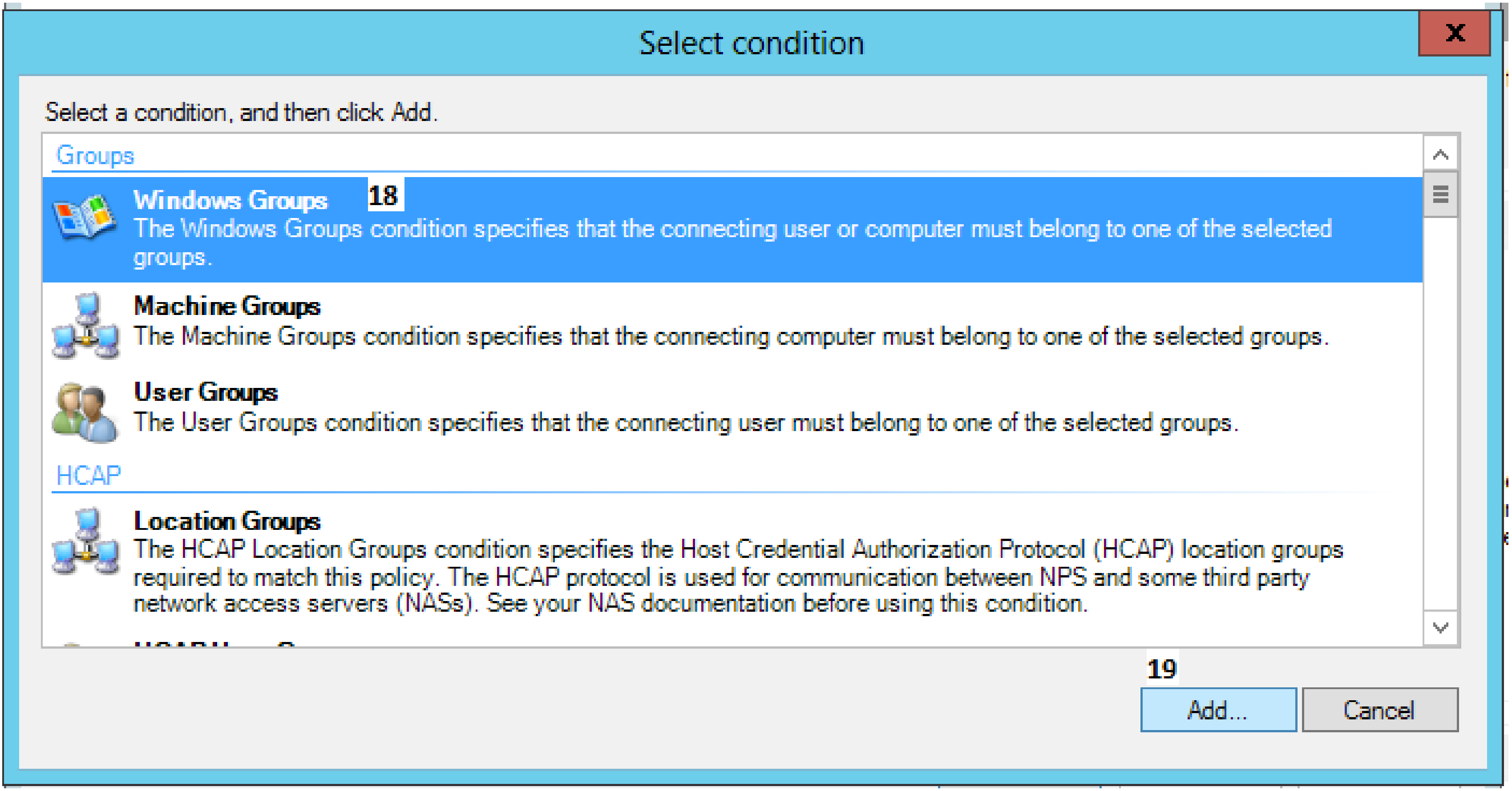
Conditions:

	Condition	Value

Condition description:

17

Konfigurasi NPAS



Select condition

Select a condition, and then click Add.

Groups

Windows Groups 18
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

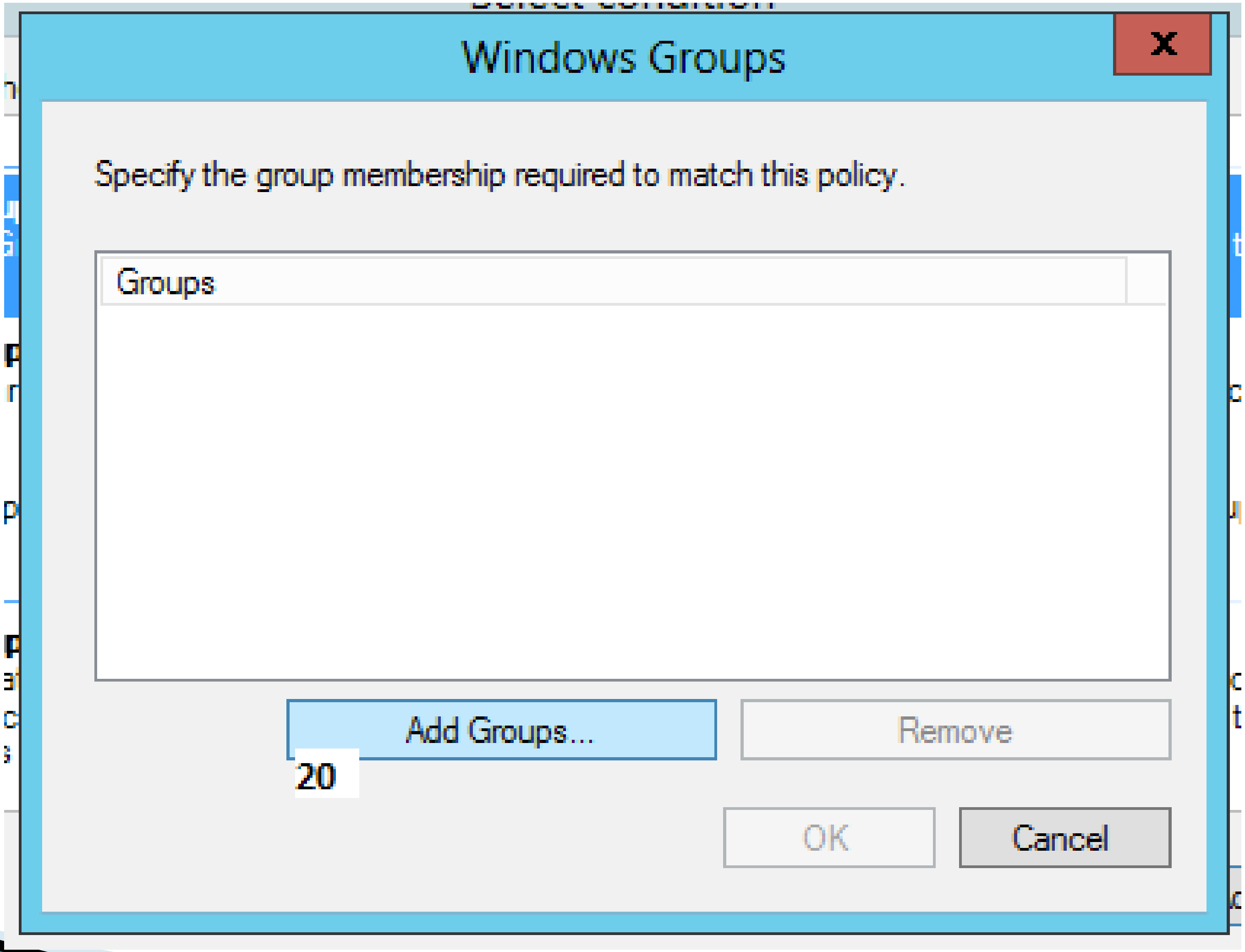
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

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

HCAP

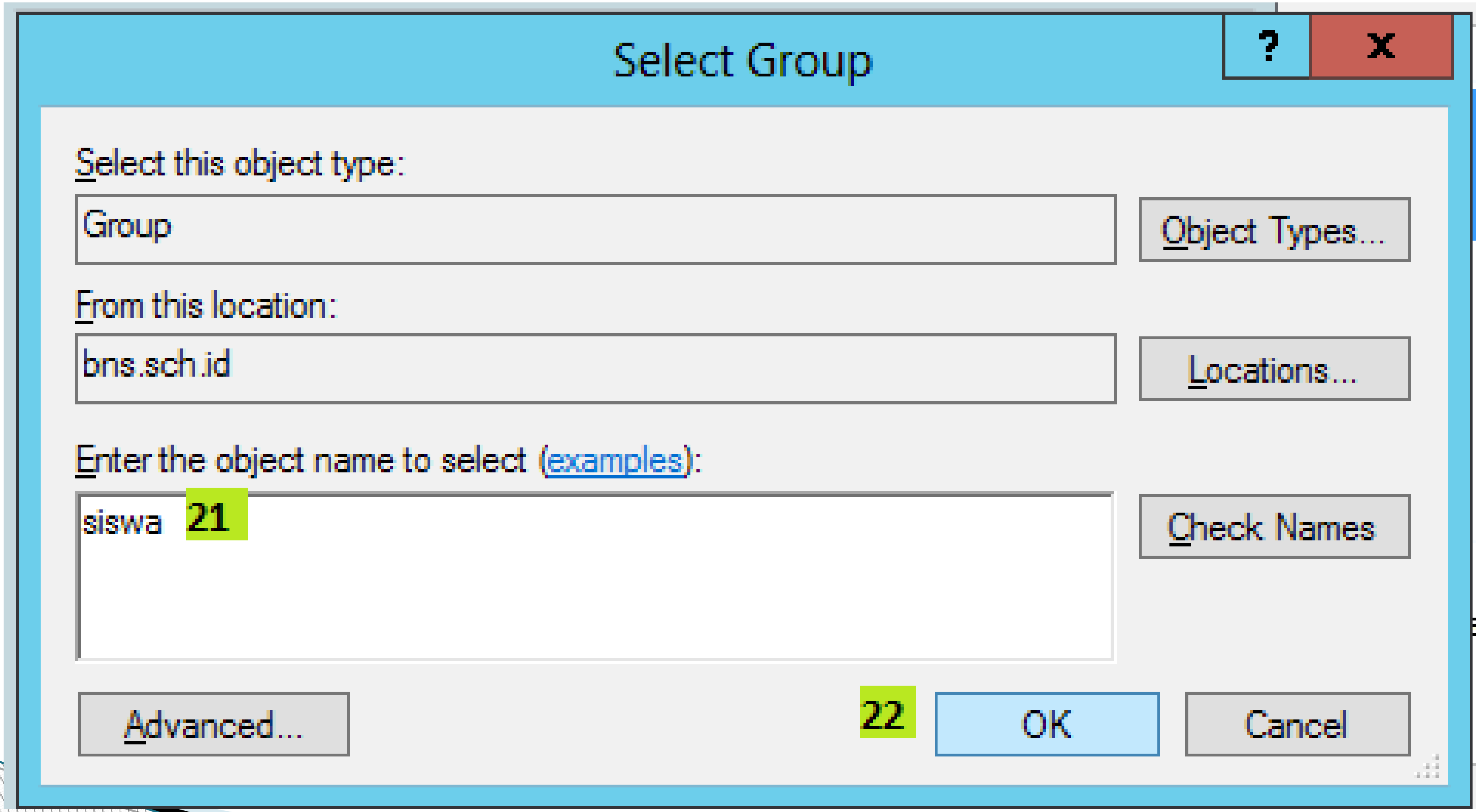
Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Konfigurasi NPAS



Specify the group membership required to match this policy.

Konfigurasi NPAS



Select this object type:

Group

From this location:

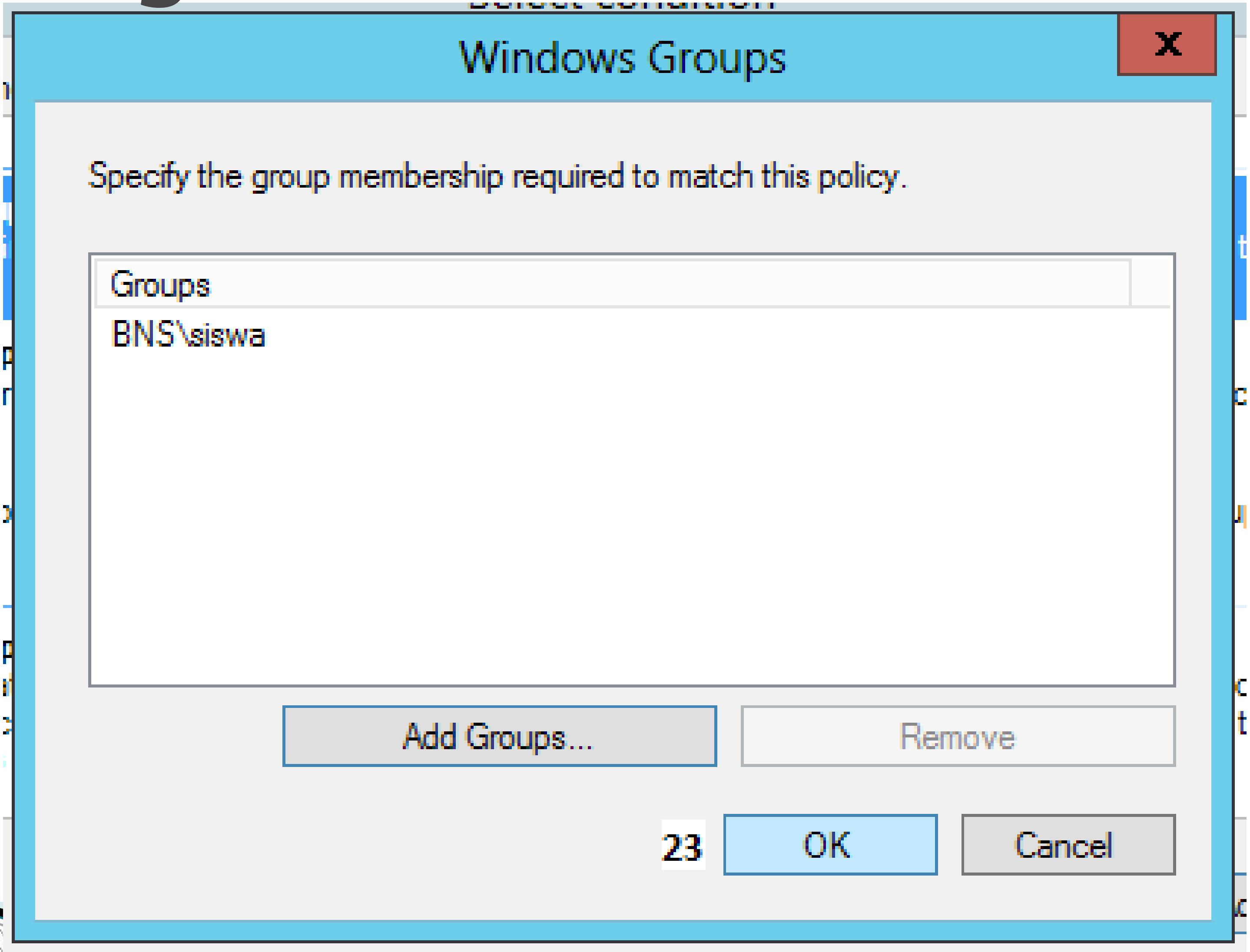
bns.sch.id

Enter the object name to select (examples):

siswa 21

22 OK

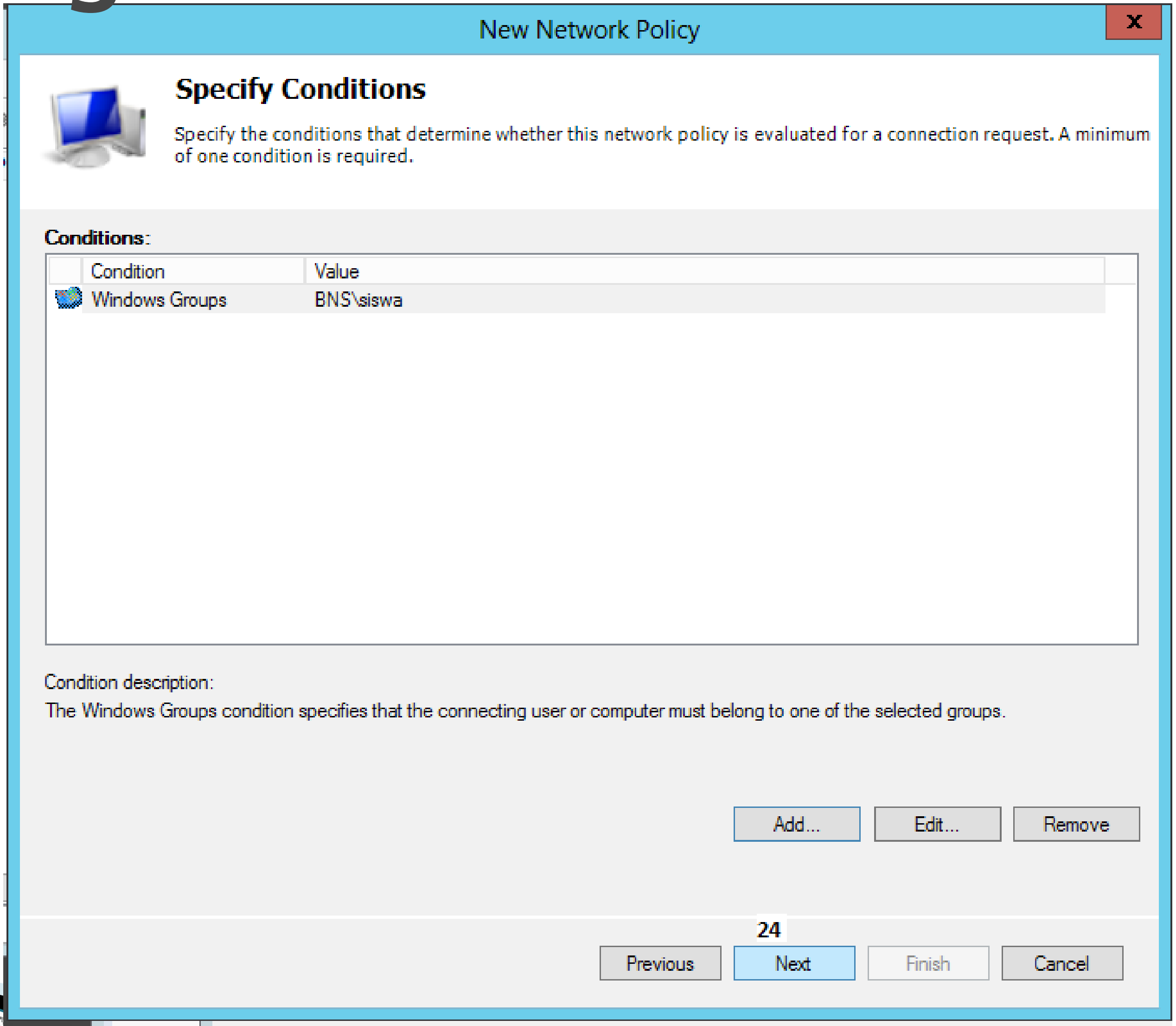
Konfigurasi NPAS


Specify the group membership required to match this policy.

Groups

BNS\siswa

Konfigurasi NPAS



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

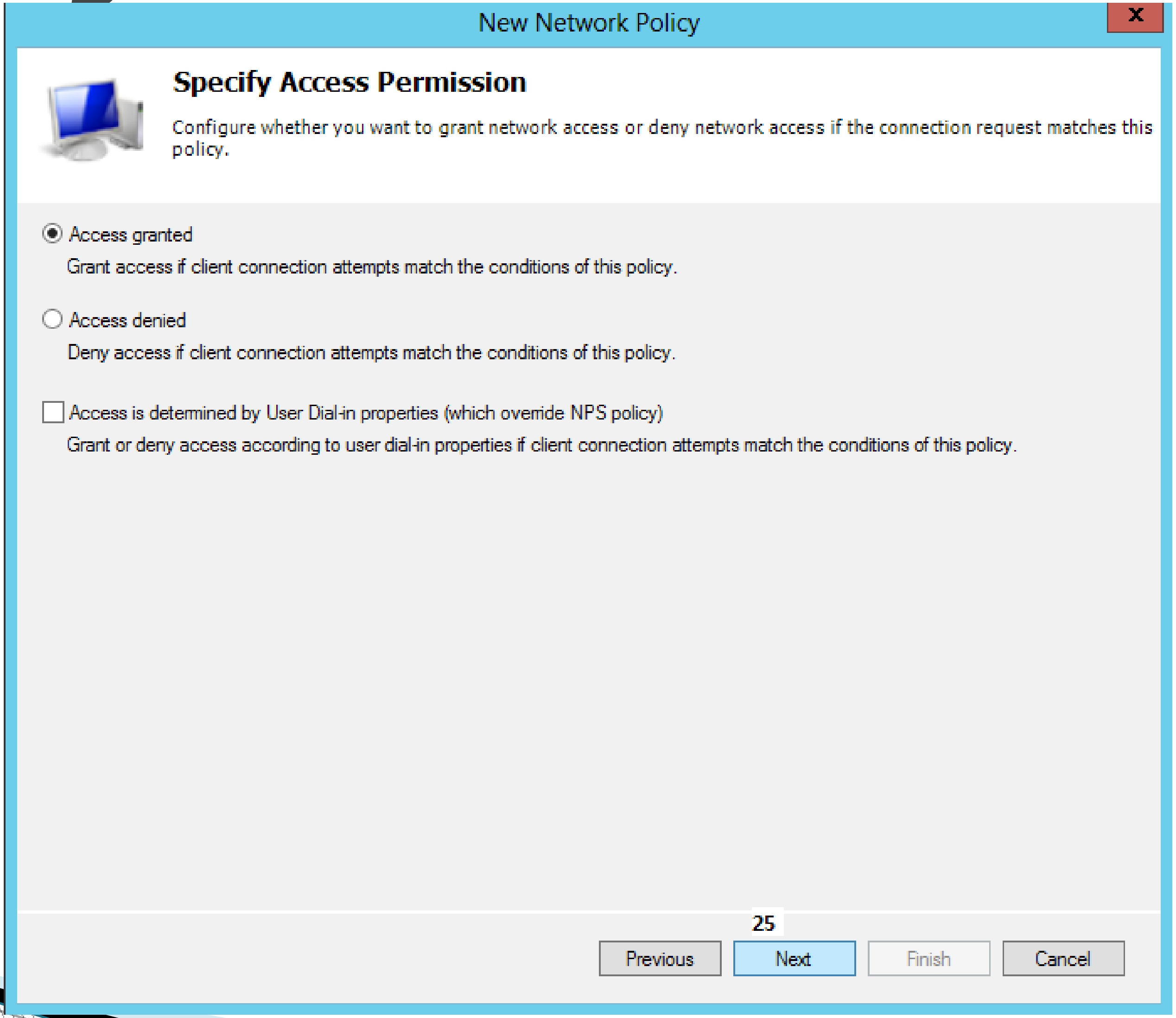
Conditions:

Condition	Value
Windows Groups	BNS\siswa

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Konfigurasi NPAS



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.

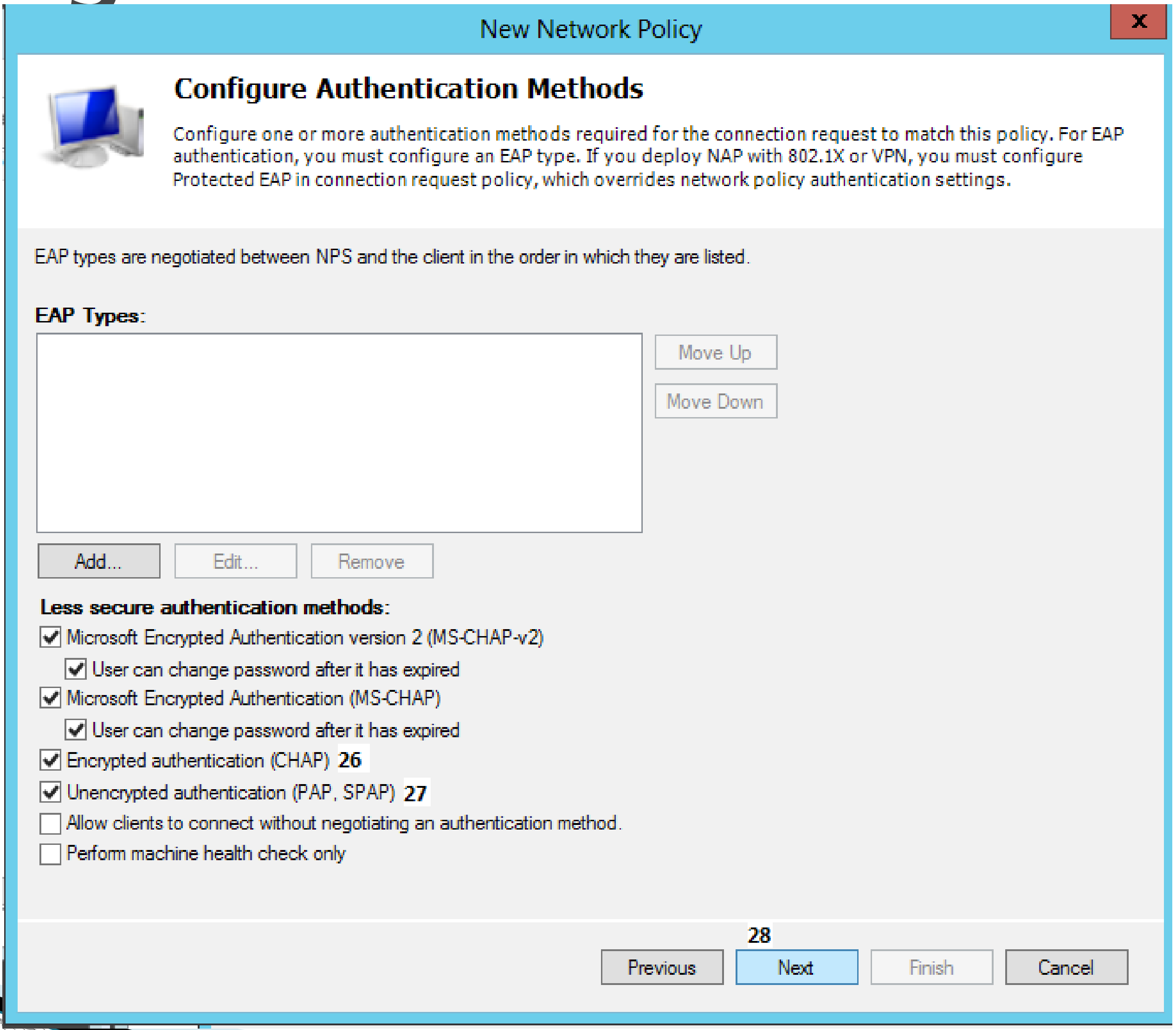
○ Access denied

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.

Konfigurasi NPAS



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.

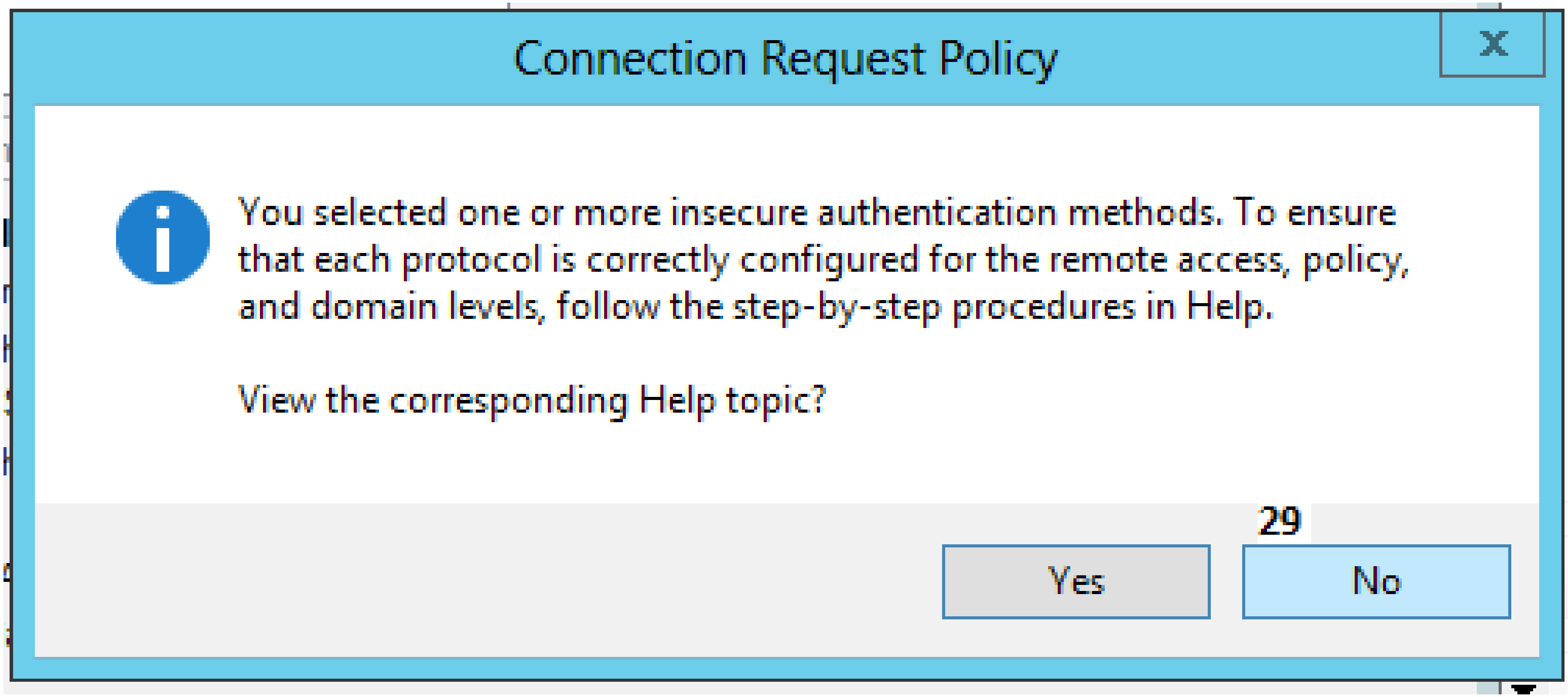
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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) 26
- ☑ Unencrypted authentication (PAP, SPAP) 27
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Konfigurasi NPAS

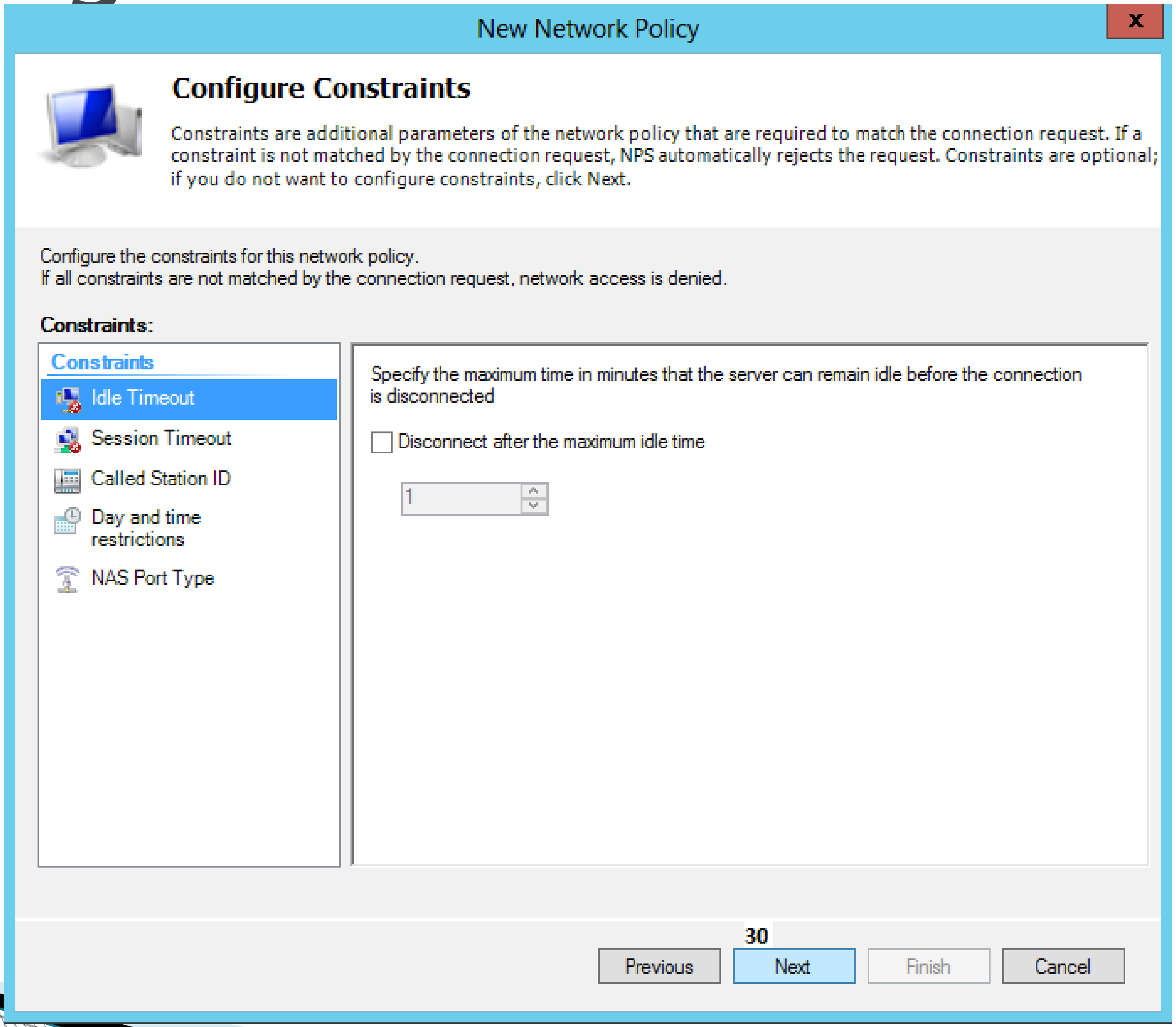


Connection Request Policy

You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

Konfigurasi NPAS



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.

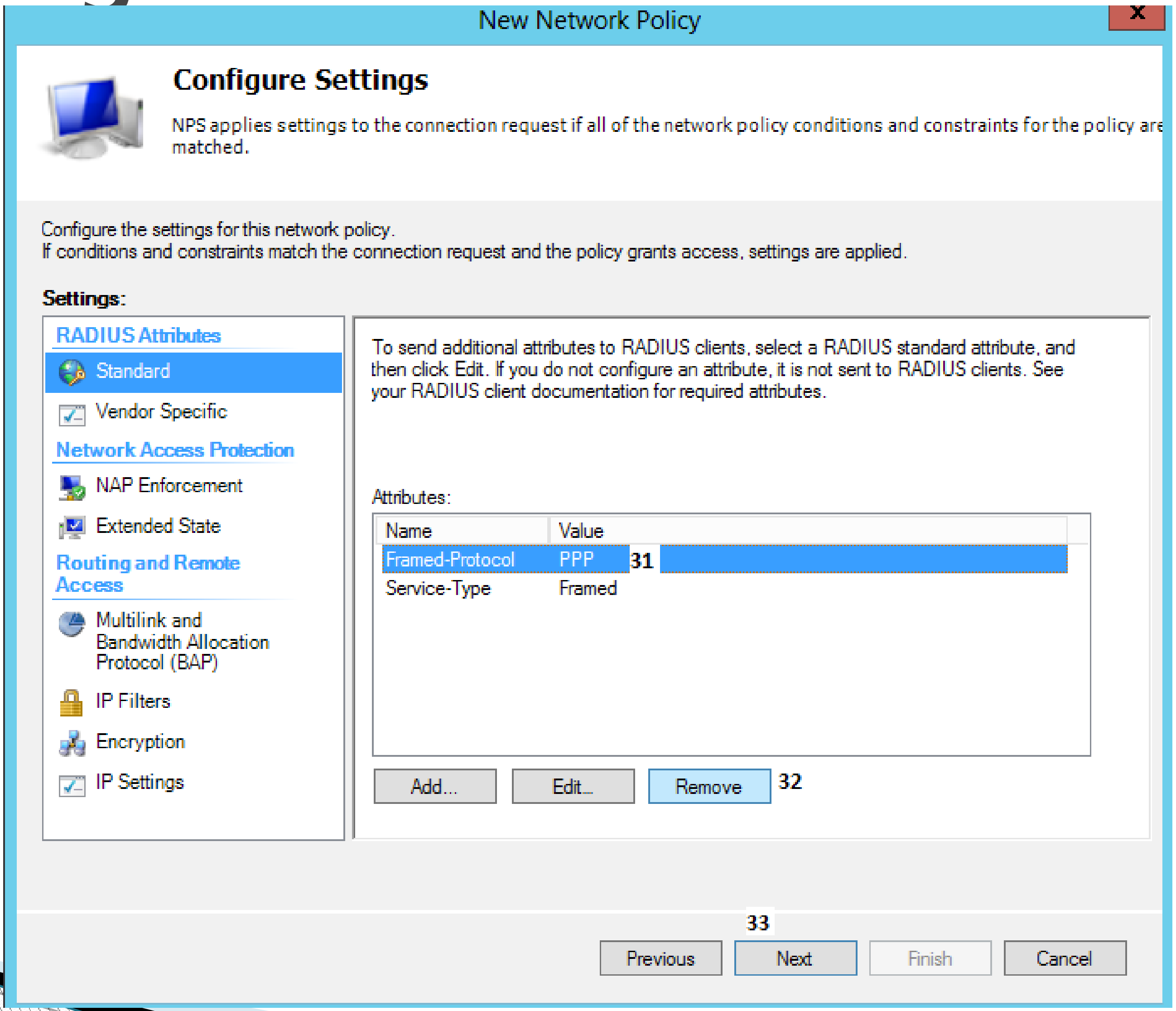
Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1

Konfigurasi NPAS



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.

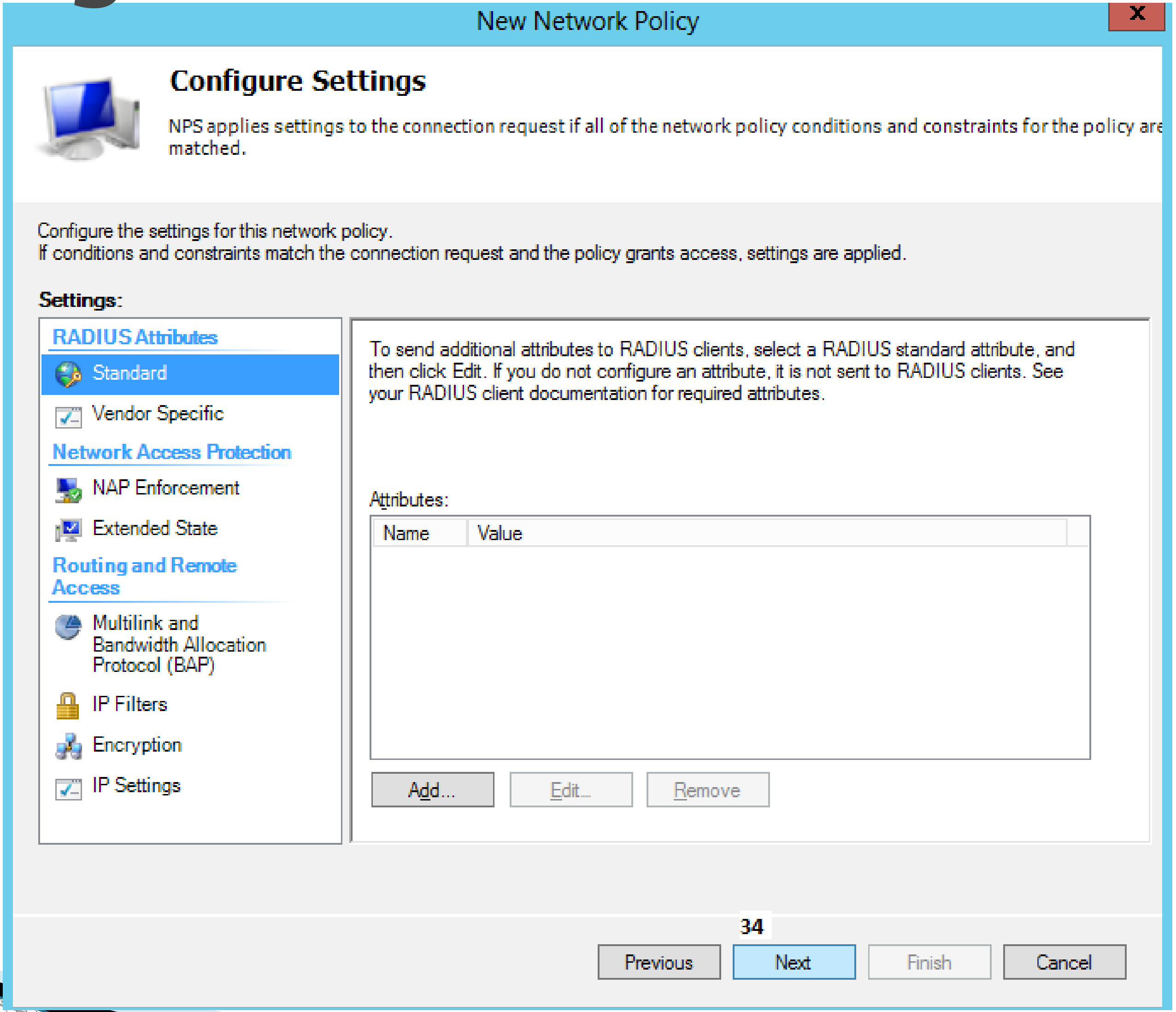
Settings:

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

Konfigurasi NPAS



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.

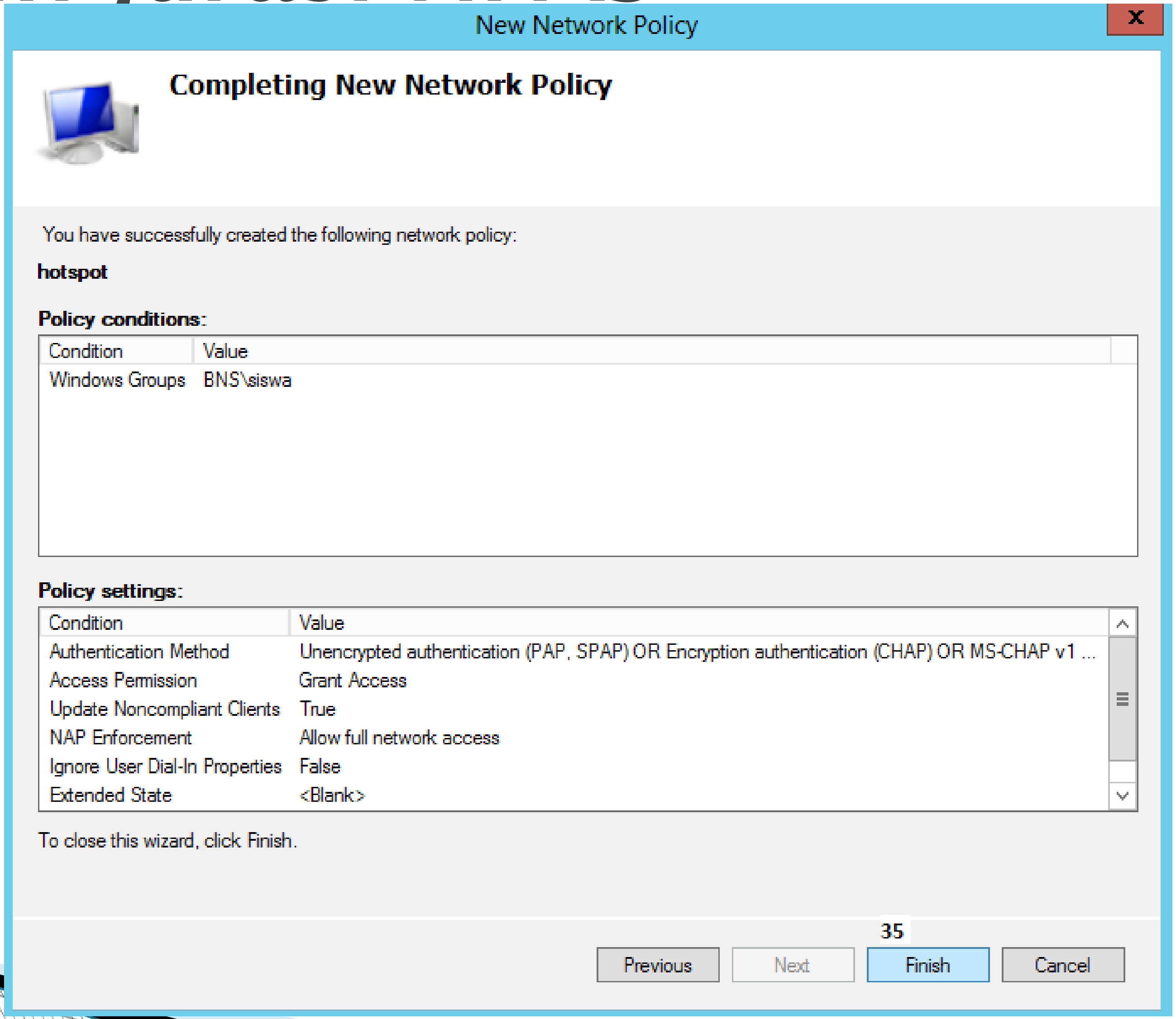
Settings:

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

Konfigurasi NPAS



Completing New Network Policy

You have successfully created the following network policy:

hotspot

Policy conditions:

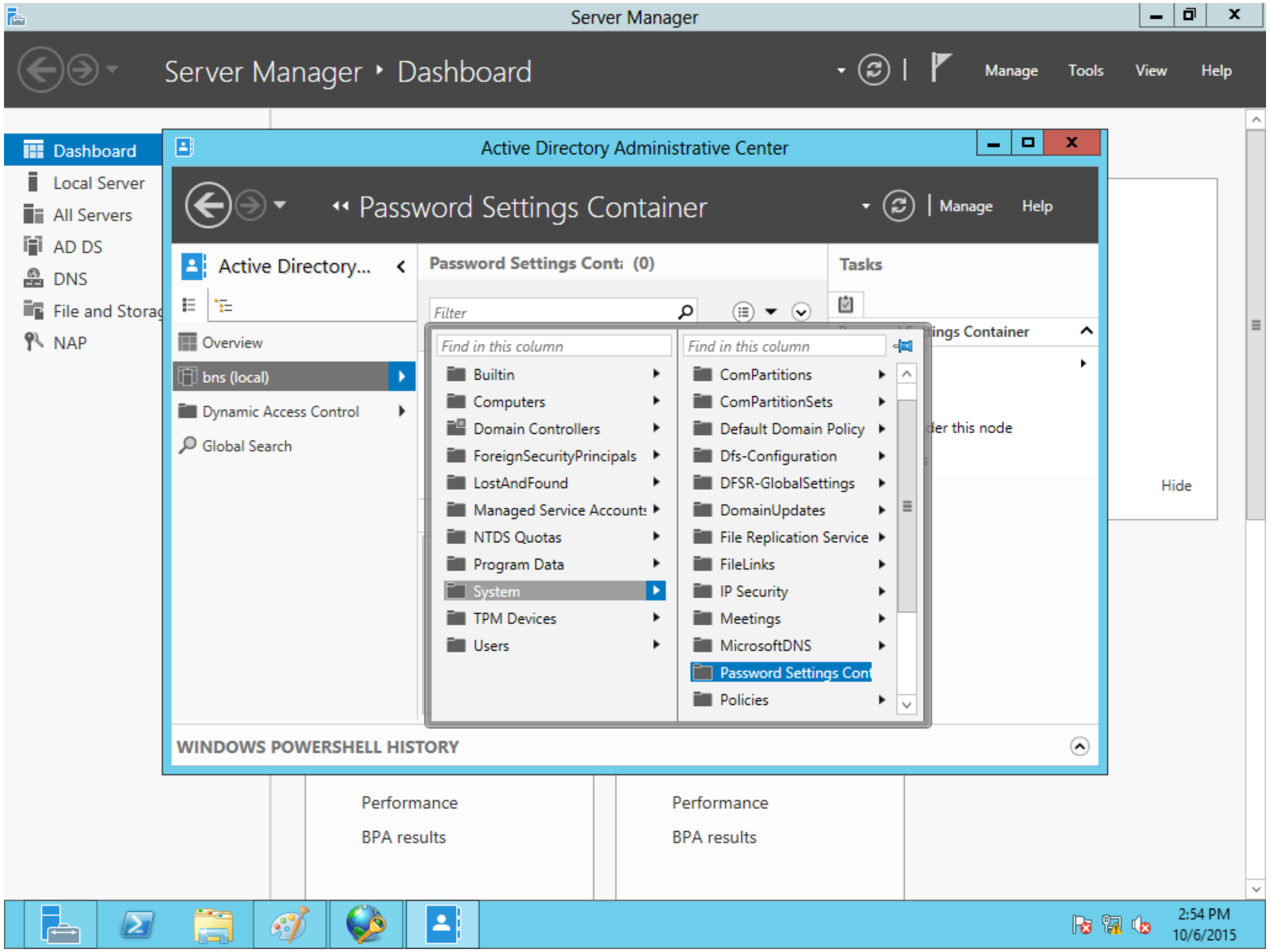
Condition	Value
Windows Groups	BNS\siswa

Policy settings:

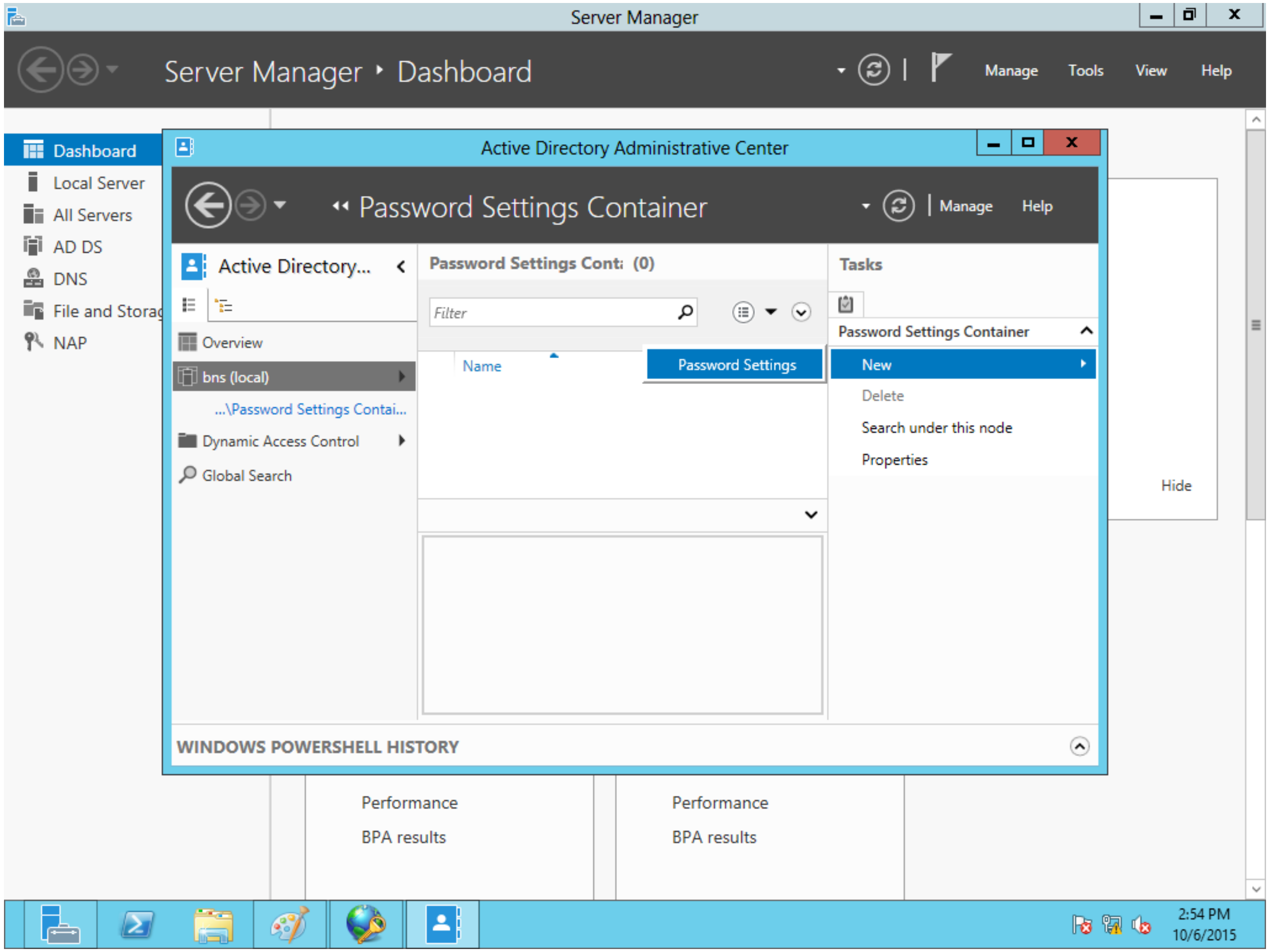
Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Ignore User Dial-In Properties	False
Extended State	<Blank>

To close this wizard, click Finish.

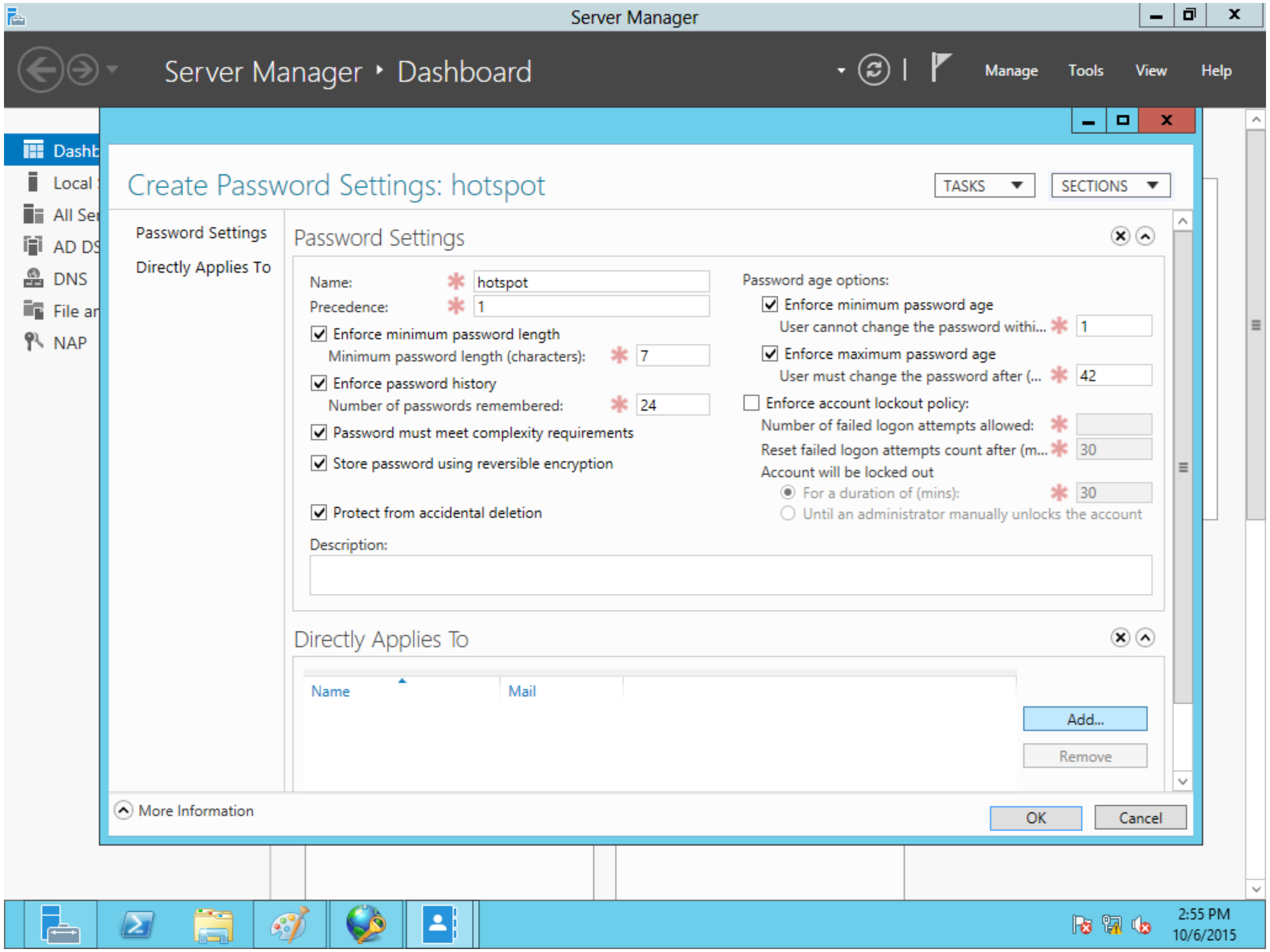
Konfigurasi Password Container



Konfigurasi Password Container



Konfigurasi Password Container



Create Password Settings: hotspot

Password Settings

Name: * hotspot

Precedence: * 1

☑ Enforce minimum password length

Minimum password length (characters): * 7

☑ Enforce password history

Number of passwords remembered: * 24

☑ Password must meet complexity requirements

☑ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:

☑ Enforce minimum password age

User cannot change the password withi... * 1

☑ Enforce maximum password age

User must change the password after (... * 42

□ Enforce account lockout policy:

Number of failed logon attempts allowed: *

Reset failed logon attempts count after (m... * 30

Account will be locked out

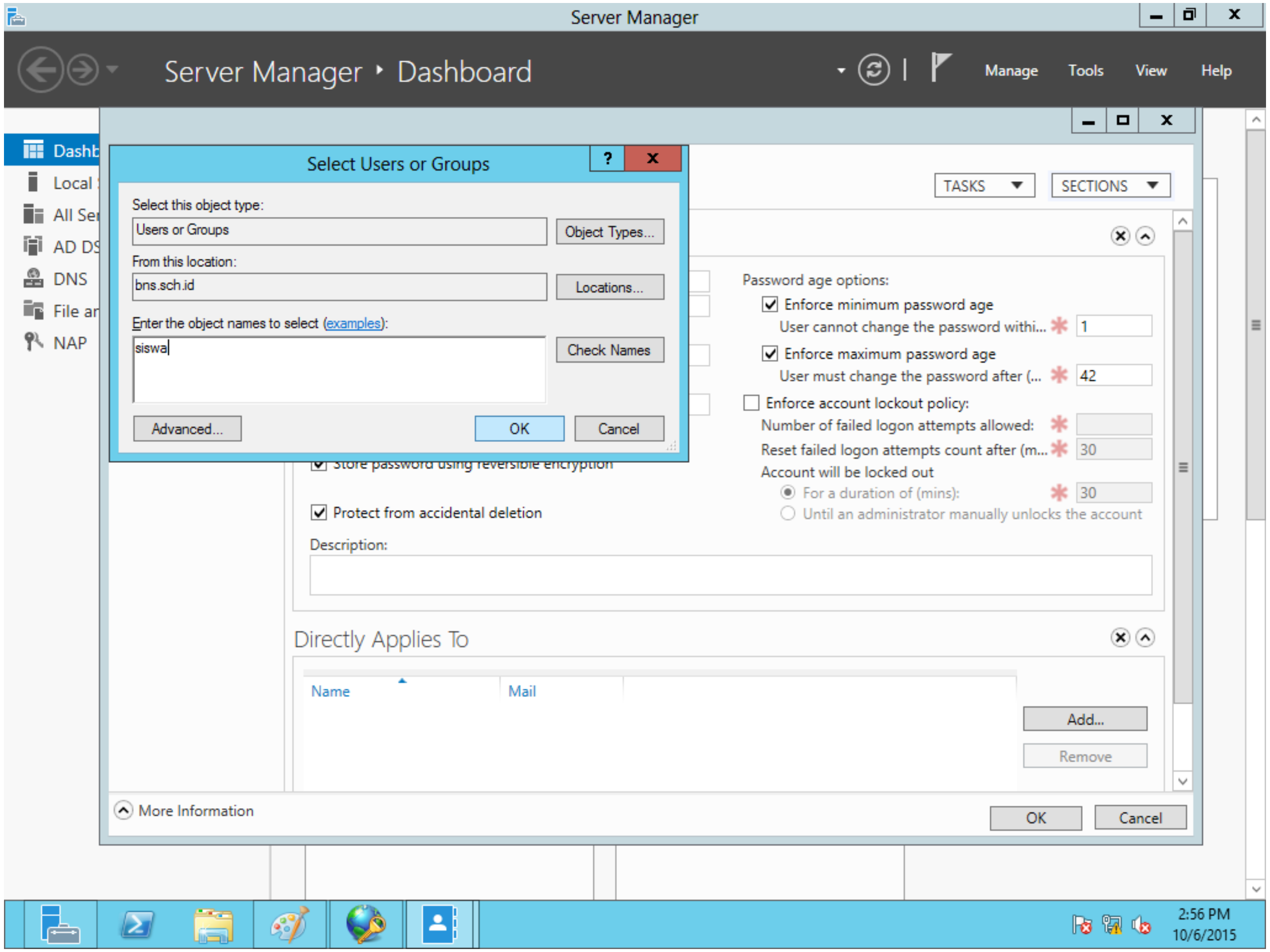
● For a duration of (mins): * 30

○ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail

Konfigurasi Password Container



Select Users or Groups

Select this object type:
Users or Groups [Object Types...]

From this location:
bns.sch.id [Locations...]

Enter the object names to select (examples):
siswa [Check Names]

[Advanced...] [OK] [Cancel]

Password age options:
☑ Enforce minimum password age
User cannot change the password withi... * 1
☑ Enforce maximum password age
User must change the password after (... * 42
□ Enforce account lockout policy:
Number of failed logon attempts allowed: *
Reset failed logon attempts count after (m... * 30
Account will be locked out
● For a duration of (mins): * 30
○ Until an administrator manually unlocks the account

☑ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

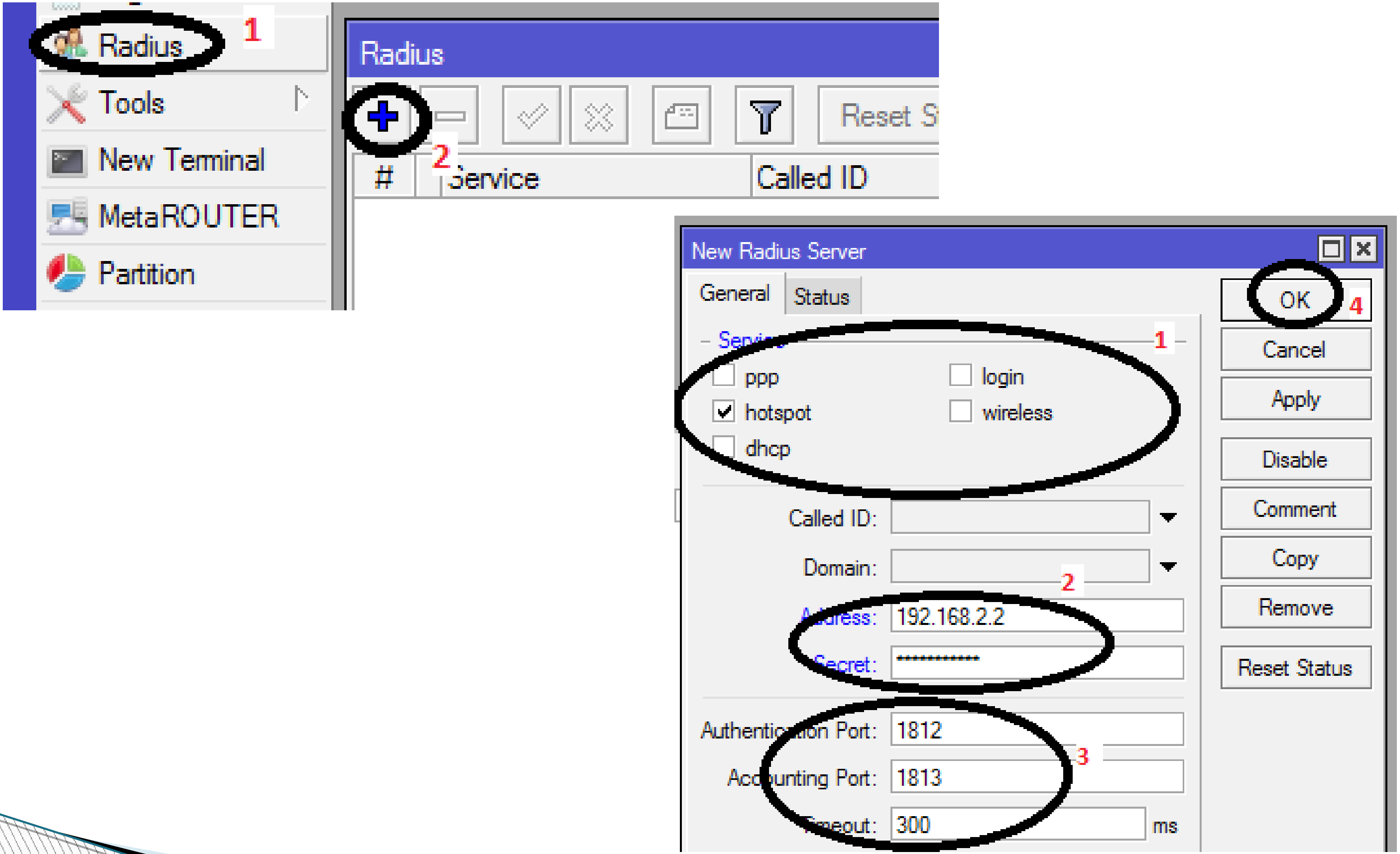
Directly Applies To

Name	Mail

[Add...] [Remove]

More Information [OK] [Cancel]

Set Radius di MikroTik (1)



Service:

- ☐ ppp
- ☐ login
- ☑ hotspot
- ☐ wireless
- ☐ dhcp

Called ID:

Domain:

Address: 192.168.2.2

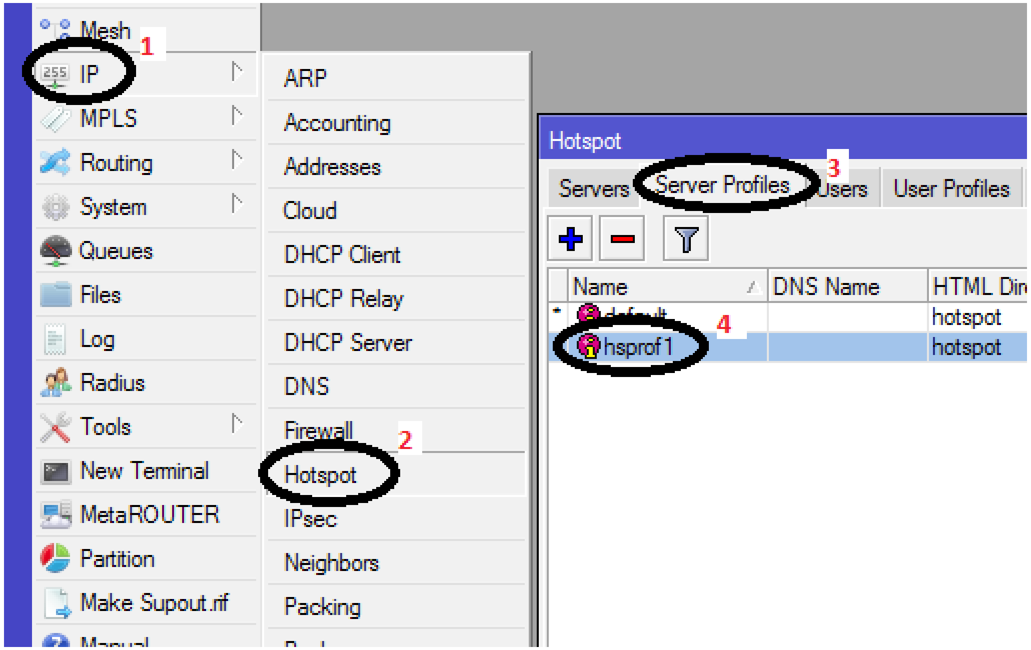
Secret: ************

Authentication Port: 1812

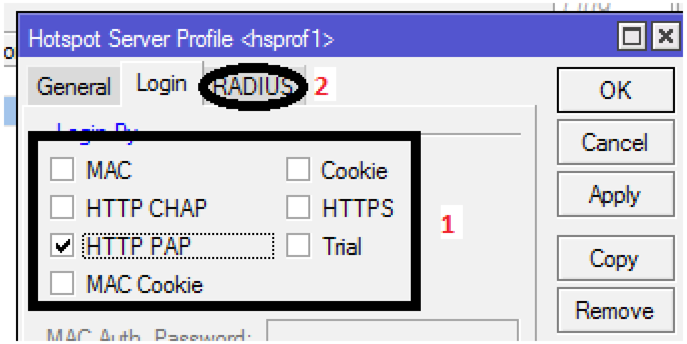
Accounting Port: 1813

Timeout: 300 ms

Set Radius di MikroTik (2)



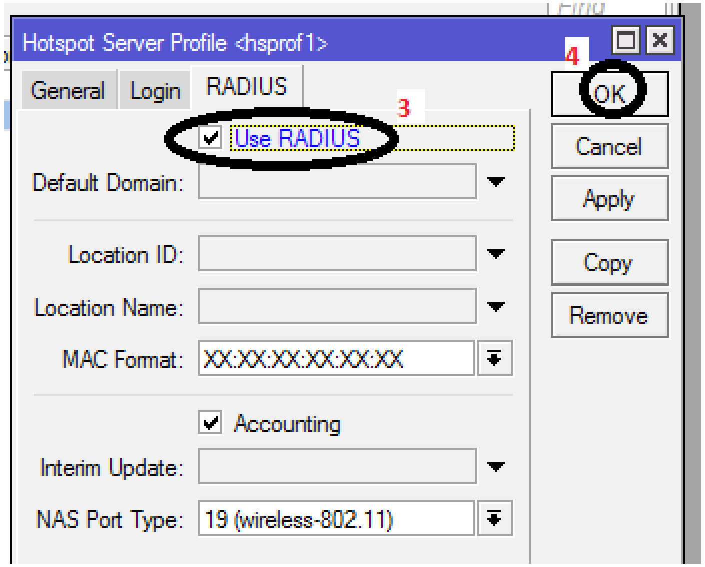
Name	DNS Name	HTML Dir
default		hotspot
hsprof1		hotspot



Login By

- □ MAC
- □ Cookie
- □ HTTP CHAP
- □ HTTPS
- ☑ HTTP PAP
- □ Trial
- □ MAC Cookie

MAC Auth. Password:



☑ Use RADIUS

Default Domain:

Location ID:

Location Name:

MAC Format: XX:XX:XX:XX:XX:XX

☑ Accounting

Interim Update:

NAS Port Type: 19 (wireless-802.11)

Info tambahan integrasi radius server

- password container dapat menjadi standar pengaturan pasword grup atau user
- Bandwidth manajemen di hotspot tetap berfungsi meskipun user berasal dari radius nya win2012

Blokir web terjadwal (1)

SET NTP CLIENT

- /system ntp client
- set enabled=yes primary-ntp=119.82.243.189 secondary-ntp=203.114.224.252

SET FIREWALL

- /ip firewall filter
- add action=drop chain=forward comment=blok content=facebook.com
- out-interface=ether1-internet src-address=192.168.2.70-192.168.3.200

Blokir web terjadwal (2)

SET SCRIPT

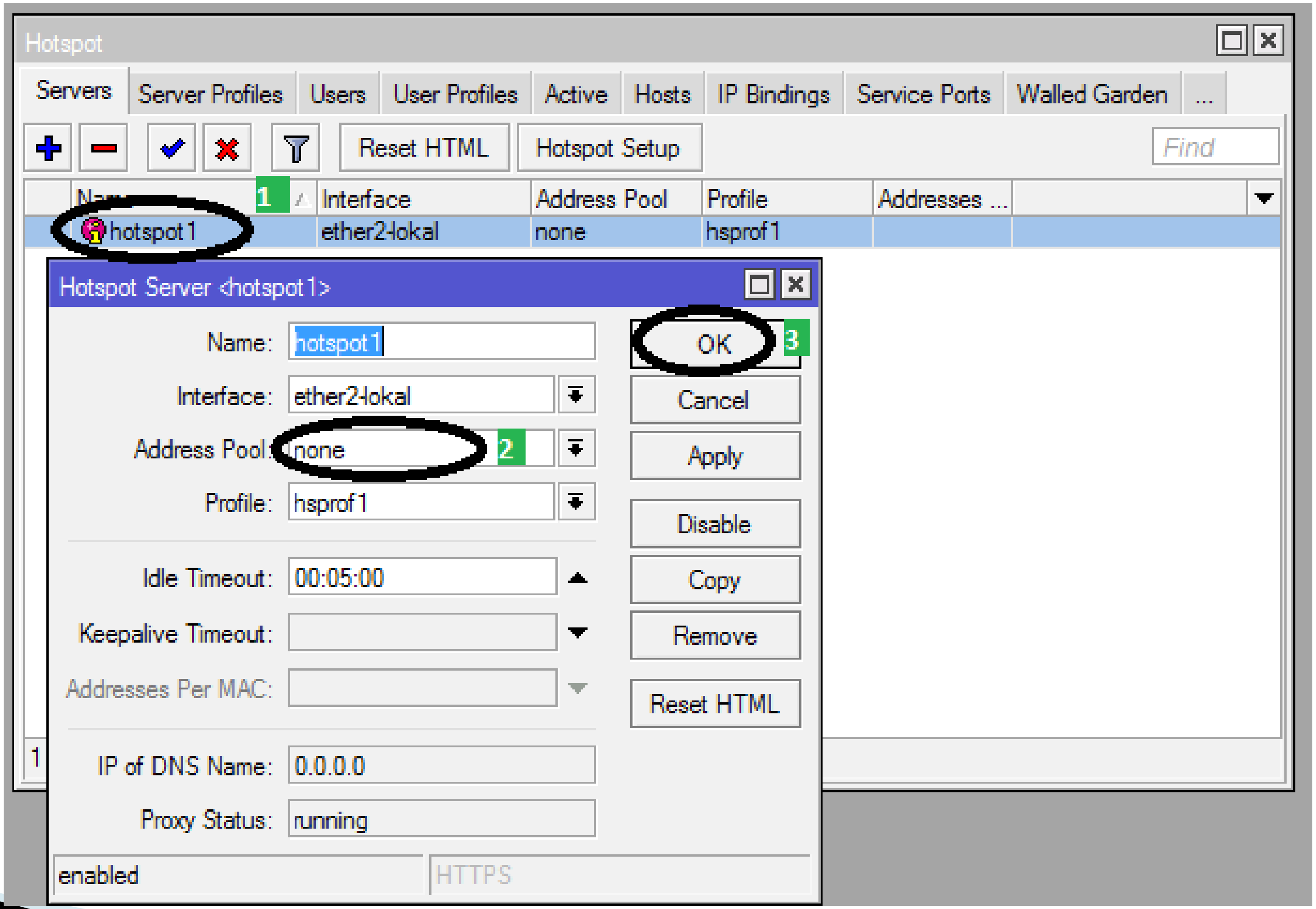
- add name=allow policy=read,write,policy,test,sniff source="/ip firewall filter set [/ip firewall filter find comment="blok"] disabled=yes"
- add name=denied policy=read,write,policy,test,sniff source="/ip firewall filter set [/ip firewall filter find comment="blok"] disabled=no"

Blokir web terjadwal (3)

SET SCHEDULER

- /system scheduler
- add interval=1d name=07.00 on-event=denied policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive start-date=sep/17/2015 start-time=07:00:00
- add interval=1d name=12.00 on-event=allow policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive start-date=sep/17/2015 start-time=12:00:00
- add interval=1d name=13.00 on-event=denied policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive start-date=sep/17/2015 start-time=13:00:00
- add interval=1d name=15.45 on-event=allow policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive start-date=sep/17/2015 start-time=15:45:00

Force DHCP (1)



Name	Interface	Address Pool	Profile	Addresses ...
hotspot1	ether2-lokal	none	hsprof1	

Name: hotspot1

Interface: ether2-lokal

Address Pool: none

Profile: hsprof1

Idle Timeout: 00:05:00

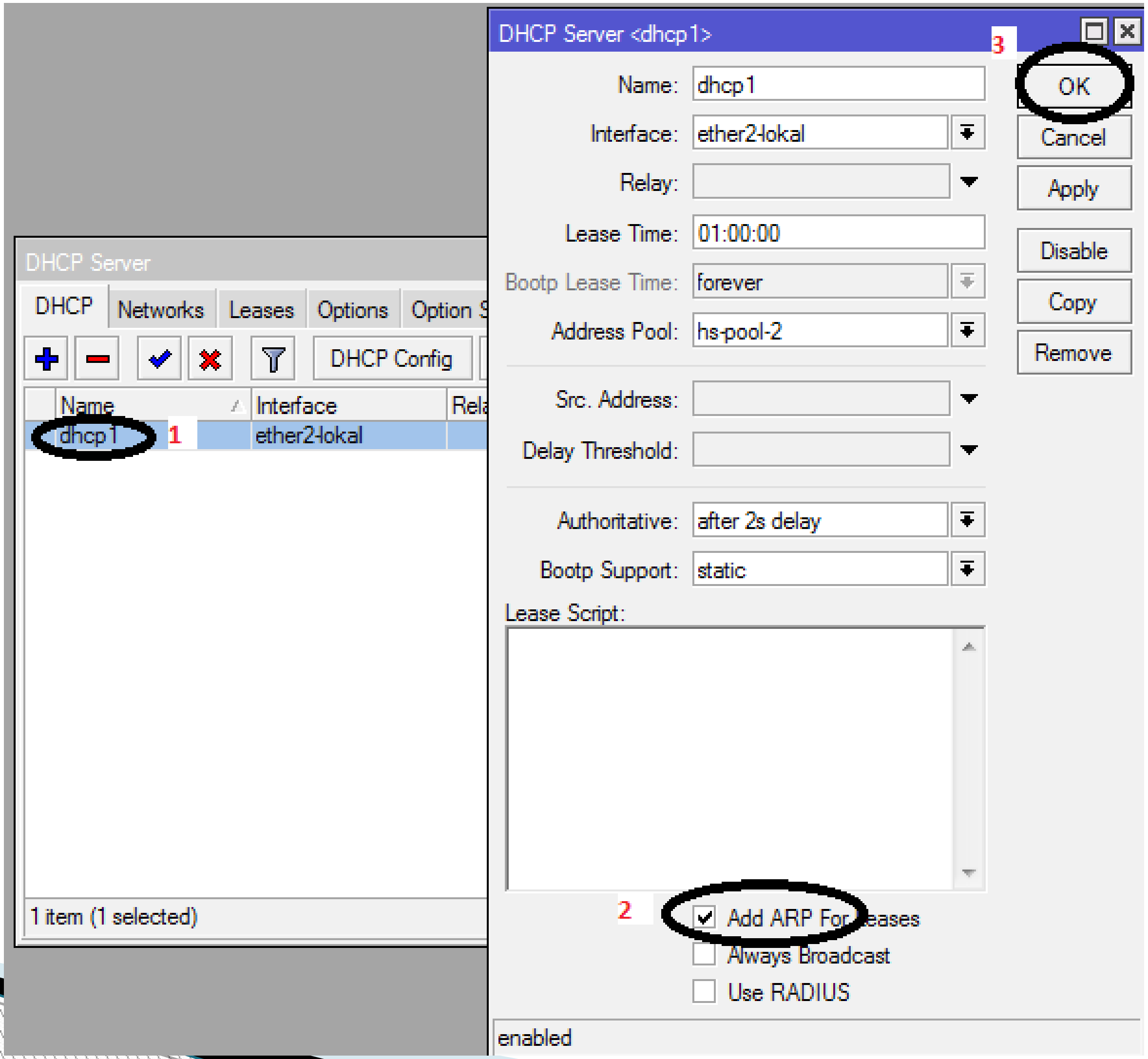
Keepalive Timeout:

Addresses Per MAC:

IP of DNS Name: 0.0.0.0

Proxy Status: running

Force DHCP (2)



DHCP Server

DHCP | Networks | Leases | Options | Option S

DHCP Config

Name	Interface	Rela
dhcp1	ether2-lokal	

1

1 item (1 selected)

DHCP Server <dhcp1>

3

Name: dhcp1

Interface: ether2-lokal

Relay:

Lease Time: 01:00:00

Bootp Lease Time: forever

Address Pool: hs-pool-2

Src. Address:

Delay Threshold:

Authoritative: after 2s delay

Bootp Support: static

Lease Script:

2

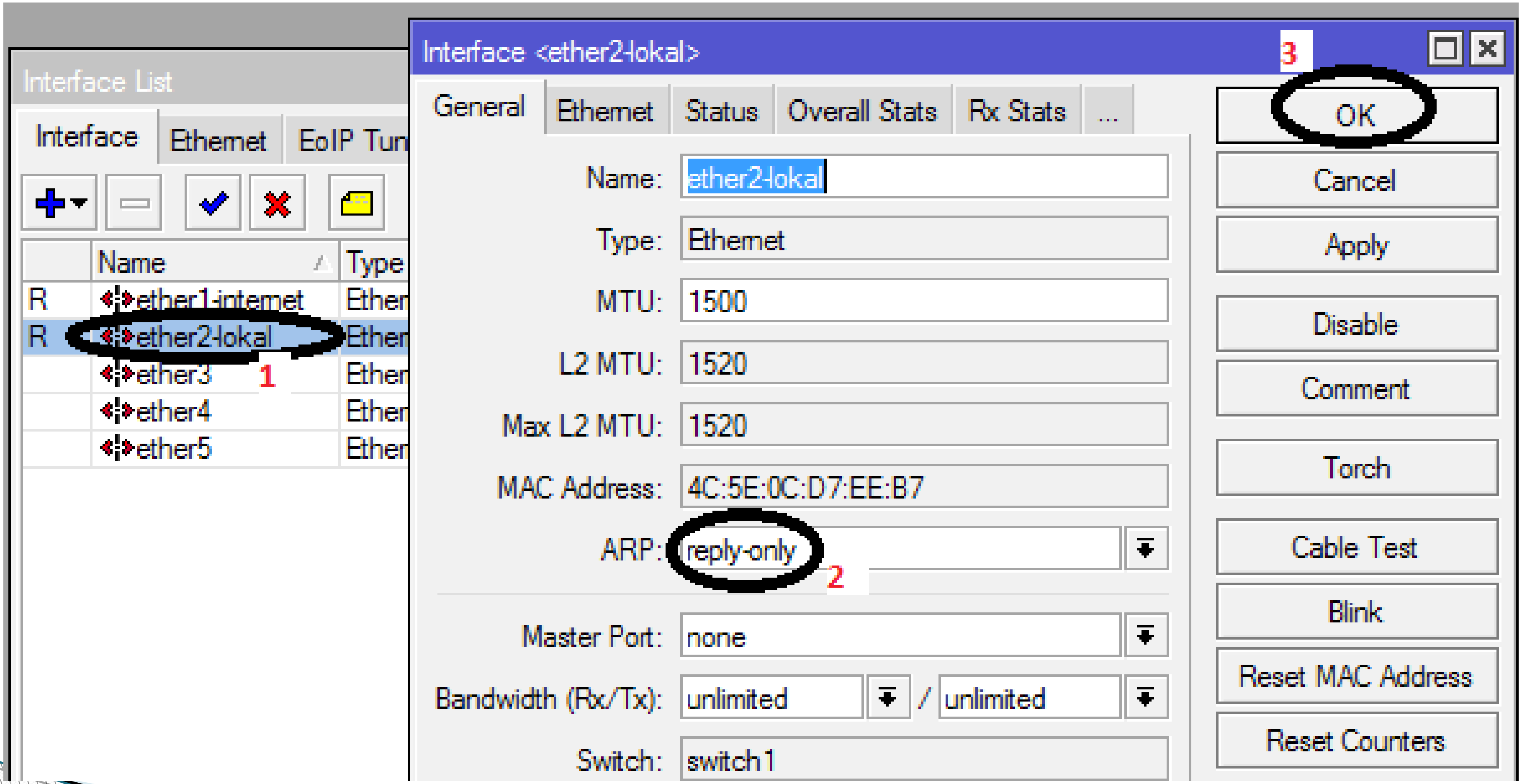
☑ Add ARP For Leases

□ Always Broadcast

□ Use RADIUS

enabled

Force DHCP (3)



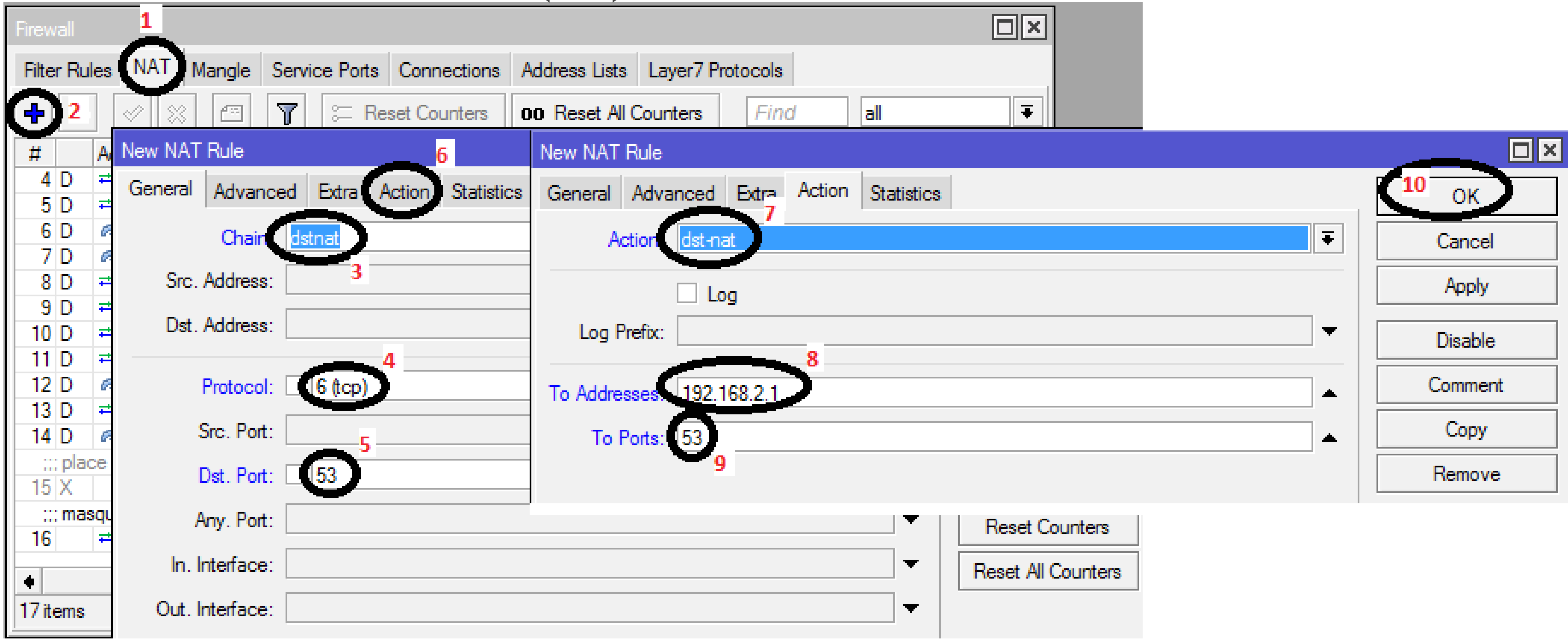
	Name	Type
R	ether1-internet	Ether
R	ether2-lokal	Ether
	ether3	Ether
	ether4	Ether
	ether5	Ether

Name:	ether2-lokal
Type:	Ethernet
MTU:	1500
L2 MTU:	1520
Max L2 MTU:	1520
MAC Address:	4C:5E:0C:D7:EE:B7
ARP:	reply-only
Master Port:	none
Bandwidth (Rx/Tx):	unlimited / unlimited
Switch:	switch1

Force DHCP

- /ip hotspot set hotspot1 address-pool=none
- /ip dhcp-server set add-arp=yes numbers=dhcp1
- /interface ethernet set ether2-lokal arp=reply-only

Force DNS (1)



1 NAT

2 +

3 Chain: dstnat

4 Protocol: 6 (tcp)

5 Dst. Port: 53

6 Action

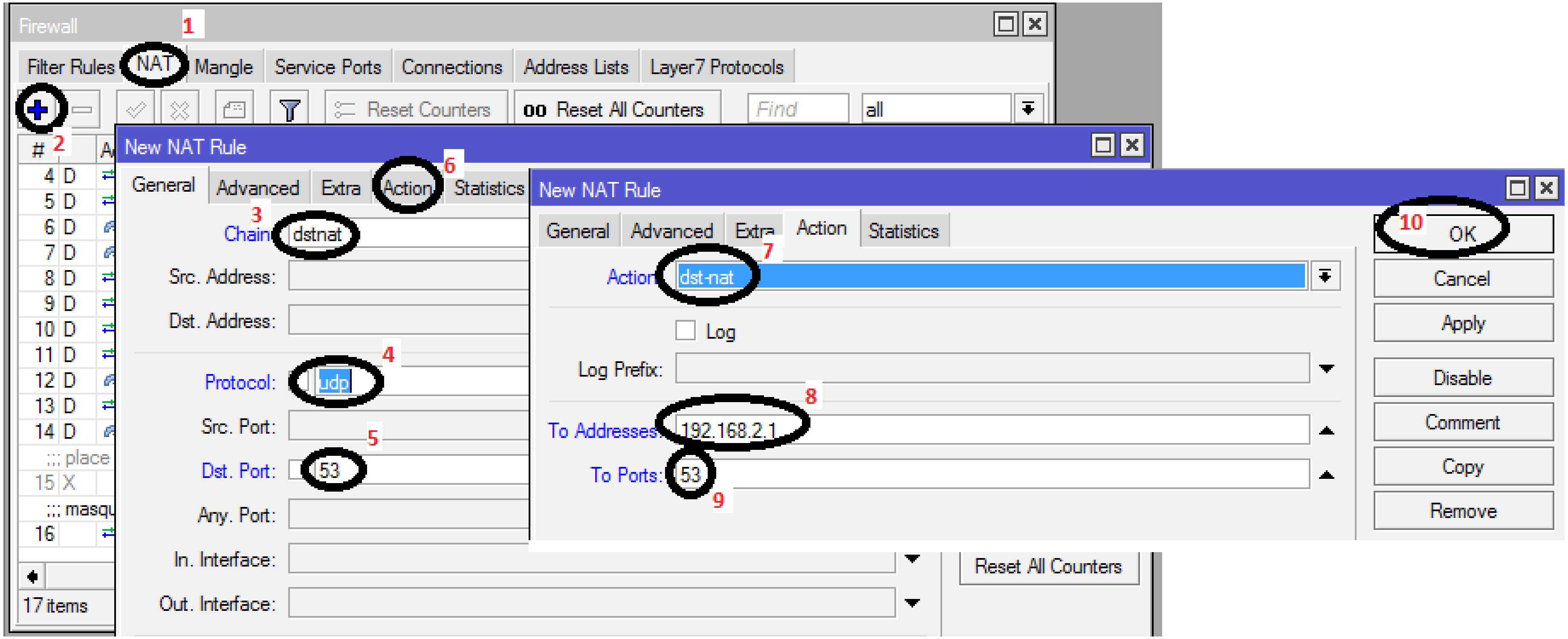
7 Action: dst-nat

8 To Addresses: 192.168.2.1

9 To Ports: 53

10 OK

Force DNS (2)



Firewall

New NAT Rule

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: udp

Src. Port:

Dst. Port: 53

Any. Port:

In. Interface:

Out. Interface:

New NAT Rule

Action: dst-nat

☐ Log

Log Prefix:

To Addresses: 192.168.2.1

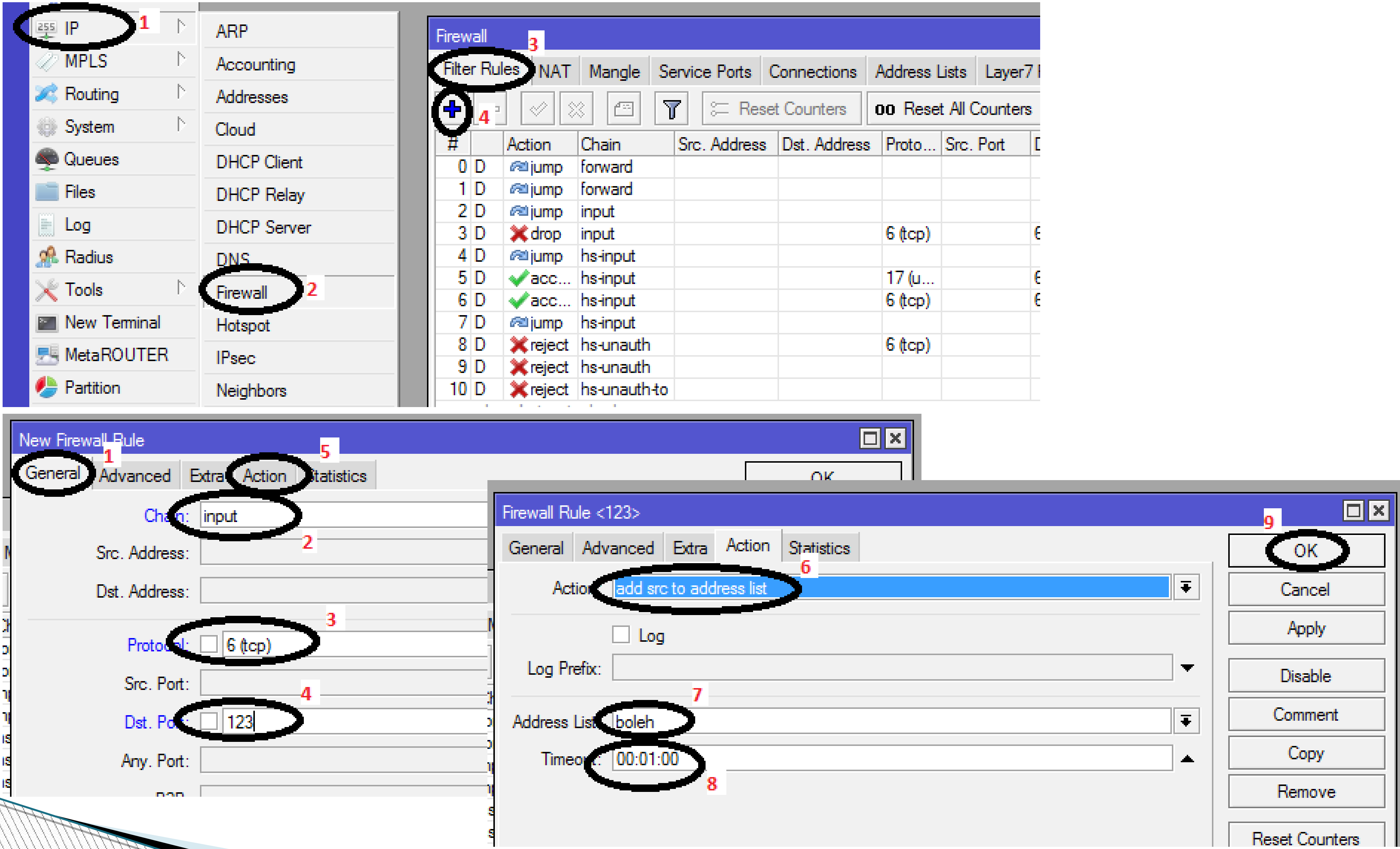
To Ports: 53

17 items

Force DNS

```
/ip firewall nat
add chain=dstnat protocol=tcp dst-port=53 action=dst-nat to-addresses=192.168.2.1 to-ports=53
add chain=dstnat protocol=udp dst-port=53  action=dst-nat to-addresses=192.168.2.1 to-ports=53
```

Port knocking (1)



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	D
0	D	jump	forward					
1	D	jump	forward					
2	D	jump	input					
3	D	✗ drop	input			6 (tcp)		6
4	D	jump	hs-input					
5	D	✓ acc...	hs-input			17 (u...		6
6	D	✓ acc...	hs-input			6 (tcp)		6
7	D	jump	hs-input					
8	D	✗ reject	hs-unauth			6 (tcp)		
9	D	✗ reject	hs-unauth					
10	D	✗ reject	hs-unauth-to					

Chain: input
2

Src. Address:

Dst. Address:

Protocol: □ 6 (tcp)
3

Src. Port:

Dst. Port: □ 123
4

Any. Port:

Action: add src to address list
6

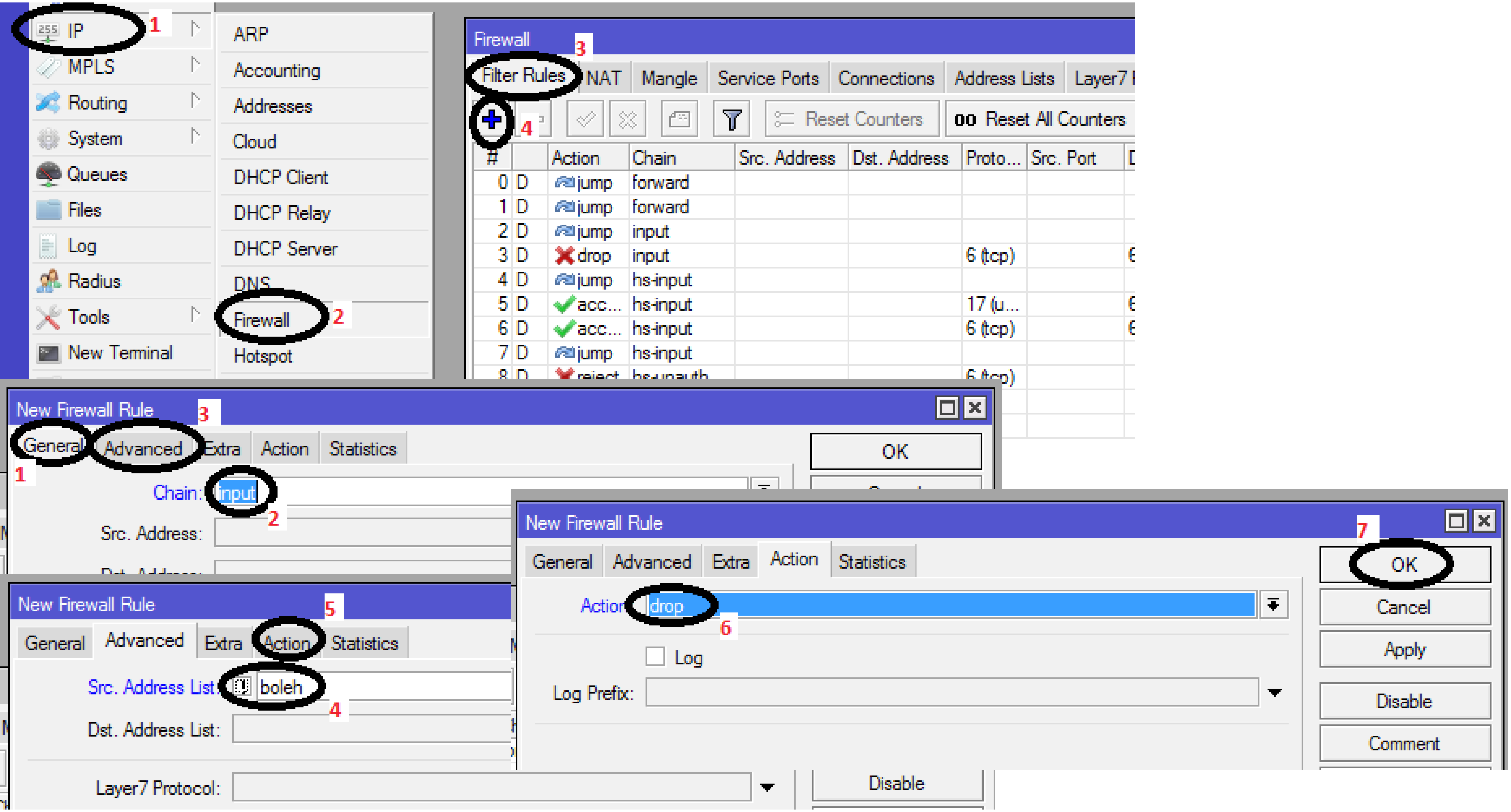
□ Log

Log Prefix:

Address List: boleh
7

Timeout: 00:01:00
8

Port knocking (2)



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	D	jump	forward				
1	D	jump	forward				
2	D	jump	input				
3	D	drop	input			6 (tcp)	
4	D	jump	hs-input				
5	D	acc...	hs-input			17 (u...	
6	D	acc...	hs-input			6 (tcp)	
7	D	jump	hs-input				
8	D	reject	hs-unauth			6 (tcp)	

Chain: input

Src. Address:

Dst. Address:

Src. Address List: boleh

Dst. Address List:

Layer7 Protocol:

Action: drop

□ Log

Log Prefix:

Port knocking

```
/ip firewall filter
add chain=input protocol=tcp dst-port=123 action=add-src-to-address-list address-list=boleh address-list-timeout=10m
add chain=input src-address-list=!boleh action=drop
```

1. ID-networkers, Mas Dedi khususnya (training gratis untuk guru SMK)
2. Pak Ziad Sobri (proses menjadi mikrotik academy)
3. Mas Supono (Materi mikrotiknya)
4. www.forummikrotik.com (materi mikrotiknya)
5. Wiki.mikrotik.com (panduannya)
6. SMK Bintang Nusantara School, (menyediakan tempat dan perangkat untuk latihan)

TERIMA KASIH