Lesson 13: Configuring NPS Policies

MOAC 70-411: Administering Windows Server 2012
Overview

- Exam Objective 4.2: Configure NPS Policies
- Managing NPS Policies
Managing NPS Policies

Lesson 13: Configuring NPS Policies
<table>
<thead>
<tr>
<th>Network Policy Server (NPS) Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Request</strong></td>
</tr>
<tr>
<td>• Specifies which RADIUS servers perform authentication, authorization, and accounting</td>
</tr>
<tr>
<td><strong>Network</strong></td>
</tr>
<tr>
<td>• Specifies who is authorized to connect to the network and circumstances under which they can or cannot connect</td>
</tr>
<tr>
<td><strong>Health</strong></td>
</tr>
<tr>
<td>• Establishes system health validators (SHVs) and other settings that define client computer configuration requirements for NAP-capable computers</td>
</tr>
</tbody>
</table>
NPS Policies

Connection Request Policies
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP or 802.1X, you must configure PEAP authentication in connection request policy.

Configure Connection Request Policies
Learn more

Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Configure Network Policies
Learn more

Health Policies
Health policies allow you to designate the configuration required for NAP capable client computers to access the network. Deploy health policy by configuring system Health Validators, creating a health policy, and then attaching the health policy to the Health Policies condition in network policy.

Configure Health Policies
Learn more
Configuring Connection Request Policies

Connection request policies are based on a range of factors such as:

• The time of day and day of the week
• The realm name in the connection request
• The type of connection requested
• The IP address of the RADIUS client
Configuring Connection Request Policies

When you create a connection request policy, you define these parameters:

- **Type of network access server** such as remote access server (VPN dial-up)
- **Condition** that specifies who or what can connect to the network based on one or more RADIUS attributes
- **Settings** that are applied to an incoming RADIUS message such as authentication, accounting, and attribute manipulation
Configuring Connection Request Policies

Connection request policy conditions:

• Are one or more RADIUS attributes that are compared to the attributes of the incoming RADIUS Access-Request message.

• If there are multiple conditions, all of the conditions in the connection request message and in the connection request policy must match in order for the policy to be enforced by NPS.
Create a Connection Request Policy

Defining the policy name
Create a Connection Request Policy

Specify Conditions

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

Conditions:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
</table>

Condition description:

Add...  Edit...  Remove

Specifying conditions

© 2013 John Wiley & Sons, Inc.
Create a Connection
Request Policy

Selecting a condition

Access Client IPv6 Address
The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access from the RADIUS client.

Framed Protocol
The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.

Service Type
The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.

Tunnel Type
The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions restrict the policy to only clients that are online during a specified day and time, with the ability to restrict different days to different times.

Add  Cancel
Create a Connection
Request Policy

Selecting a tunnel type
Create a Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

- Authenticate requests on this server
- Forward requests to the following remote RADIUS server group for authentication
  - (not configured)
- Accept users without validating credentials

Specifying Connection Request Forwarding page

© 2013 John Wiley & Sons, Inc.
Create a Connection
Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match the policy. For EAP authentication, you must configure an EAP type. If you deploy EAP with 802.1x or VPN, you must configure Protected EAP.

- Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1x connections with NAP, you must configure PEAP authentication here.

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

EAP Types:

- Add
- Edit
- Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAPv2)
- 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 (EAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Specifying Authentication Methods page
Create a Connection Request Policy

Configuring Settings page
Create a Connection Request Policy

New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

**Connection Policy Name**

**Policy conditions:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Type</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
</tbody>
</table>

**Policy settings:**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Provider</td>
<td>Local Computer</td>
</tr>
</tbody>
</table>

To close this wizard, click Finish.
Create a Connection Request Policy

Configuring Connection Request Policy properties
Configuring Network Policies

An NPS network policy evaluates remote connections based on these three components:

• Conditions
• Constraints
• Settings
Configuring Network Policies

When a user attempts to connect to a remote access server, this process occurs:

1. User attempts to initiate a remote access connection.
2. Remote access server checks the conditions in the first configured NPS network policy.
3. If the conditions of this NPS network policy do not match, the remote access server checks the next configured NPS network policies. It keeps checking each policy until it finds a match or reaches the last policy.
4. When the remote access server finds an NPS network policy with conditions that match the incoming connection attempt, the remote access server checks any constraints that have been configured for the policy.
Configuring Network Policies

When a user attempts to connect to a remote access server, this process occurs (continued):

5. Once the remote access server finds an NPS network policy with conditions that match the incoming connection attempt, the remote access server checks any constraints (such as time of day or minimum encryption level) that have been configured for the policy.

6. If the connection attempt does not match any configured constraints, the remote access server denies the connection.

7. If the connection attempt matches both the conditions and the constraints of a particular NPS network policy, the remote access server will allow or deny the connection, based on the Access Permissions configured for that policy.
Create a Network Policy

Starting the New Network Policy Wizard
Create a 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:
<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
</table>

Condition description:

Specifyconditions
Create a Network Policy

Selecting conditions

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 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.

© 2013 John Wiley & Sons, Inc.
Create a Network Policy

Adding Windows groups
Create a Network Policy

Specifying access permissions
Create a 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:

- 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

Configuring authentication methods
Create a 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:

- Idle Timeout
- Session Timeout
- Dial 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

Configuring constraints
Create a 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
  - Multihomed 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed Protocol</td>
<td>PPP</td>
</tr>
<tr>
<td>Service Type</td>
<td>Framed</td>
</tr>
</tbody>
</table>

Add... Edit... Remove...
Create a Network Policy

Completing New Network Policy

You have successfully created the following network policy:

**Policy Name**

**Policy conditions:**
- Condition: Windows Groups
  - Value: CONTOSO\Domain Users

**Policy settings:**
- Condition: Authentication Method
  - Value: MS-CHAP v1 OR MS-CHAP v2 (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.
Create a Network Policy

Configuring Network Policy properties
Multilink and Bandwidth Allocation

• ISDN includes multiple channels, which allow simultaneous voice and data communications.

• With multilink and Bandwidth Allocation Protocol (BAP) settings, you can specify:
  o Whether multiple connections form a single connection to increase bandwidth
  o How BAP determines when these extra lines are dropped
Multilink and Bandwidth Allocation

Configuring Multilink and BAP settings

© 2013 John Wiley & Sons, Inc.
IP Filters

Allow you to control which packets are allowed through the network connection based on IP address.

To configuration:
1. Click the Input Filters or Output Filters for IPv4 or IPv6.
2. Specify to permit or not permit packets.
3. Click the New button to specify the source network or destination network.
IP Filters

Configuring an IPv4 Inbound filter
Encryption Options

- **Basic Encryption (MPPE 40-Bit)**: For dial-up and PPTP-based VPN connections, MPPE is used with a 40-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.

- **Strong Encryption (MPPE 56-Bit)**: For dial-up and PPTP VPN connections, MPPE is used with a 56-bit key. For L2TP/IPsec VPN connections, 56-bit DES encryption is used.

- **Strongest Encryption (MPPE 128-Bit)**: For dial-up and PPTP VPN connections, MPPE is used with a 128-bit key. For L2TP/IPsec VPN connections, 168-bit Triple DES encryption is used.

- **No Encryption**: This option allows unencrypted connections that match the remote access policy conditions. Clear this option to require encryption.
Encryption Settings

Configuring encryption settings

The encryption settings are supported by computers running Microsoft Routing and Remote Access Server.

If you use different network access servers for dialup or VPN connections, ensure that the encryption settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

- Basic encryption (MPPE 40-bit)
- Strong encryption (MPPE 56-bit)
- Strongest encryption (MPPE 128-bit)
- No encryption
IP Addressing

IP settings include these options:

• Server Must Supply An IP Address
• Client May Request An IP Address
• Server Settings Determine IP Address Assignment (the default setting)
• Assign A Static IP Address
Configuring IP assignment settings
Managing NPS Templates

NPS template types available in Templates Management:

• Shared Secrets
• RADIUS Clients
• Remote RADIUS Servers
• IP Filters
• Health Policies
• Remediation Server Groups
Managing NPS Templates

Configuring templates in NPS

Templates Configuration

Select an item below to create, configure, and manage templates. All templates can be exported to or imported from other NPS servers. To import or export templates, right-click Templates Management and select a command.

Configure NPS Templates

In Templates Management, you create and modify NPS templates. NPS templates allow you to create and save NPS component configurations for reuse later. The templates are not applied to the NPS server configuration until you select the templates in the appropriate location in the NPS console.

After you create a template, you can apply the NPS component configuration in the NPS console by selecting the template. For example, you can create an IP Filters template, and then apply the same IP Filters configuration to multiple network policies by simply selecting the template.
Managing NPS Templates

Creating a new IP filter template
Managing NPS Templates

Applying the template
Exporting and Importing the NPS Configuration Including NPS Policies

Use the `netsh` command to export the entire NPS configuration from one NPS server for import on another NPS server.

NPS configuration includes:

• RADIUS clients and servers
• Network policy
• Connection request policy
• Registry
• Logging configuration
Lesson Summary

• An NPS policy is a set of permissions or restrictions that are used by remote access authenticating servers that determine who, when, and how a client can connect to a network.

• With remote access policies, connections can be authorized or denied based on user attributes, group membership, and so on.

• Connection request policies are policies that establish sets of conditions and settings that specify which RADIUS servers perform the authentication, authorization, and accounting of connection requests received by the NPS server from RADIUS clients.

• Network policies establish sets of conditions, constraints, and settings that specify who is authorized to connect to the network and the circumstances under which they can or cannot connect.

• With multilink and Bandwidth Allocation Protocol (BAP) settings, you can specify whether multiple connections form a single connection to increase bandwidth. In addition, you can specify how BAP determines when these extra lines are dropped.
Lesson Summary

- The IP filters allow you to control which packets are allowed through the network connection based on IP address.
- The Encryption settings enable you to specify the supported encryption used with network connections.
- The last setting in the Routing and Remote Access is IP settings, which specify how IP addresses are assigned.
- Network Policy Server templates enable you to create configuration elements that can be reused on the local NPS server and can be exported to other NPS servers.
- You can export the entire NPS configuration, including RADIUS clients and servers, network policy, connection request policy, registry, and logging configuration from one NPS server for import on another NPS server by using the `netsh` command.
Copyright 2013 John Wiley & Sons, Inc.
All rights reserved. Reproduction or translation of this work beyond that
named in Section 117 of the 1976 United States Copyright Act without the
express written consent of the copyright owner is unlawful. Requests for
further information should be addressed to the Permissions Department, John
Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own
use only and not for distribution or resale. The Publisher assumes no
responsibility for errors, omissions, or damages, caused by the use of these
programs or from the use of the information contained herein.