3. Windows Firewall configuration – Active Directory

3.1 Management console (GPMC)

To configure the firewall for multiple computers, it is advisable to define the required settings by means of a group policy.

The following example shows how to define a domain-wide setting using the Microsoft Group Policy Management Console (GPMC) tool. GPO settings can be made at the local (L), site (S), domain (D), and organizational unit (OU) levels. Subsequent settings always overwrite the previously defined values. The hierarchy is L, S, D, OU.

If the Microsoft Group Policy Management Console has not been installed on your system, you can download it for free from Microsoft. The following example shows how to change the firewall settings for all systems in the domain. It is strongly recommended to previously test this measure in a test environment or to implement the settings only in a dedicated test OU *(organizational unit)* in the Active Directory.

The remote server management tools including the GPMC can be downloaded from the Microsoft website for the Windows client operating systems.

Windows server operating systems (2008 and higher) already include the GPMC, but it might be necessary to install it subsequently via the Server Manager.

3.2 Starting GPMC

Open the Windows Run dialog (Windows key+R) and type *gpmc.msc*.

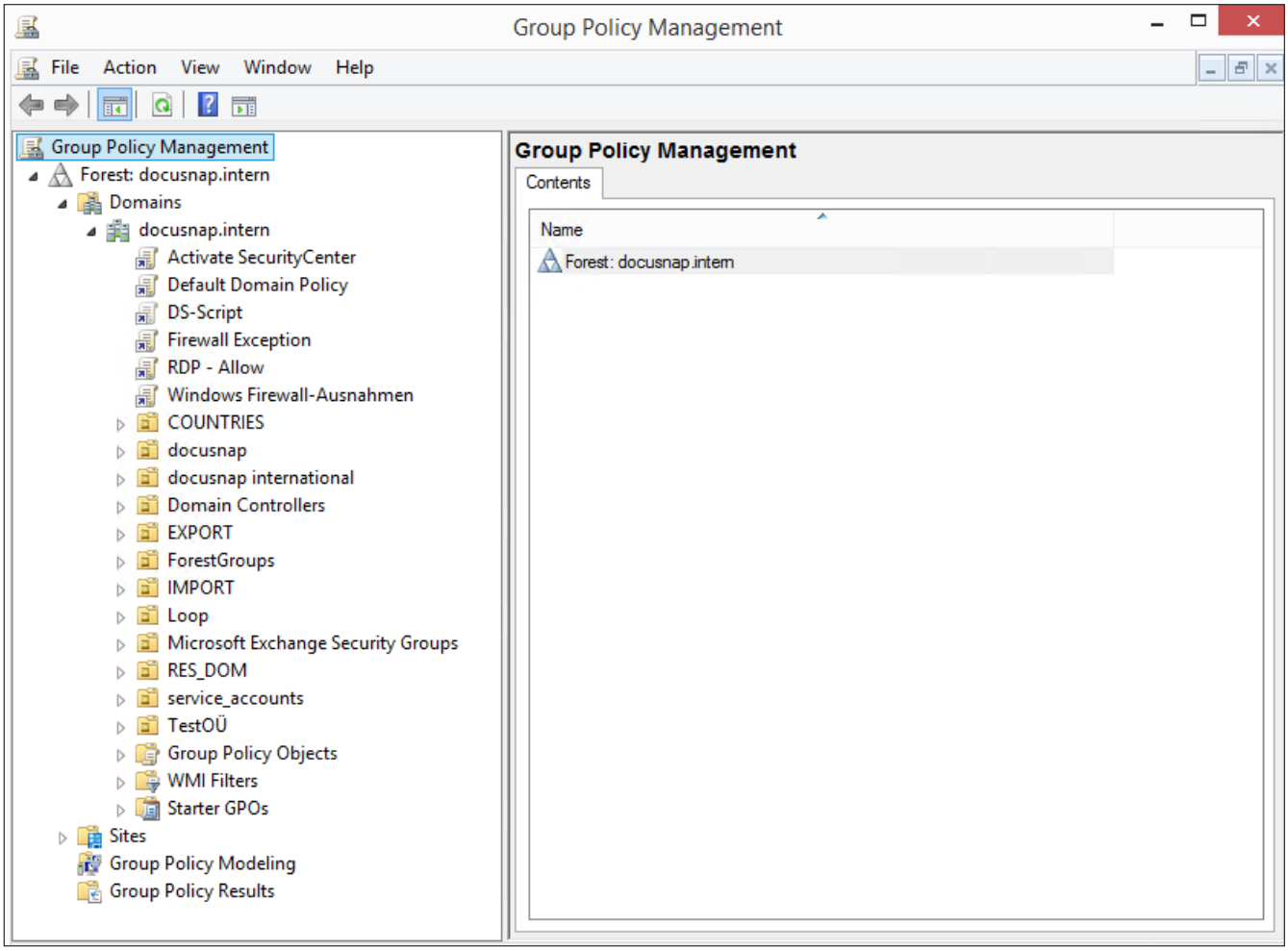

Fig. 1 - Group Policy Management

3.3 Creating a Group Policy Object

Right-click the desired *domain* or *OU* and select the *Create a GPO in this domain, and Link it here* option.

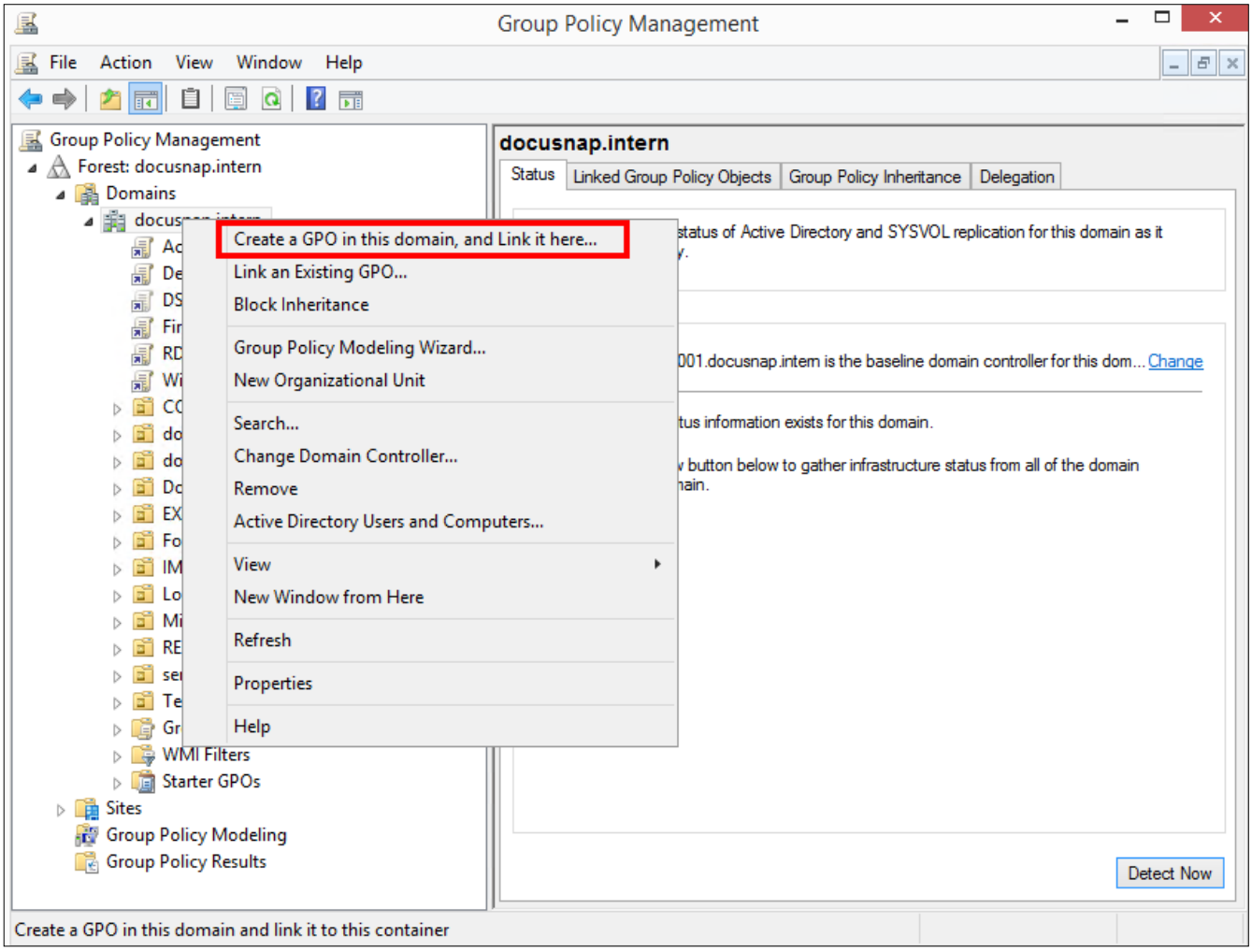

Fig. 2 - Create a GPO in this domain, and Link it here... option

Enter a descriptive name for the GPO.

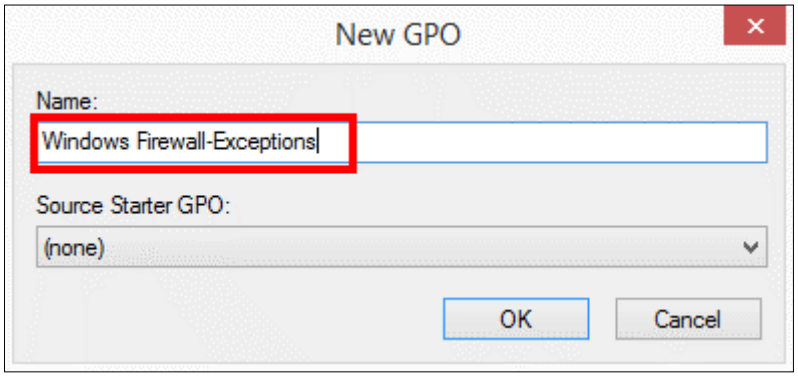

Fig. 3 - New GPO dialog

3.4 Editing a Group Policy Object

Right-click the previously created group policy object to select it and select *Edit*.

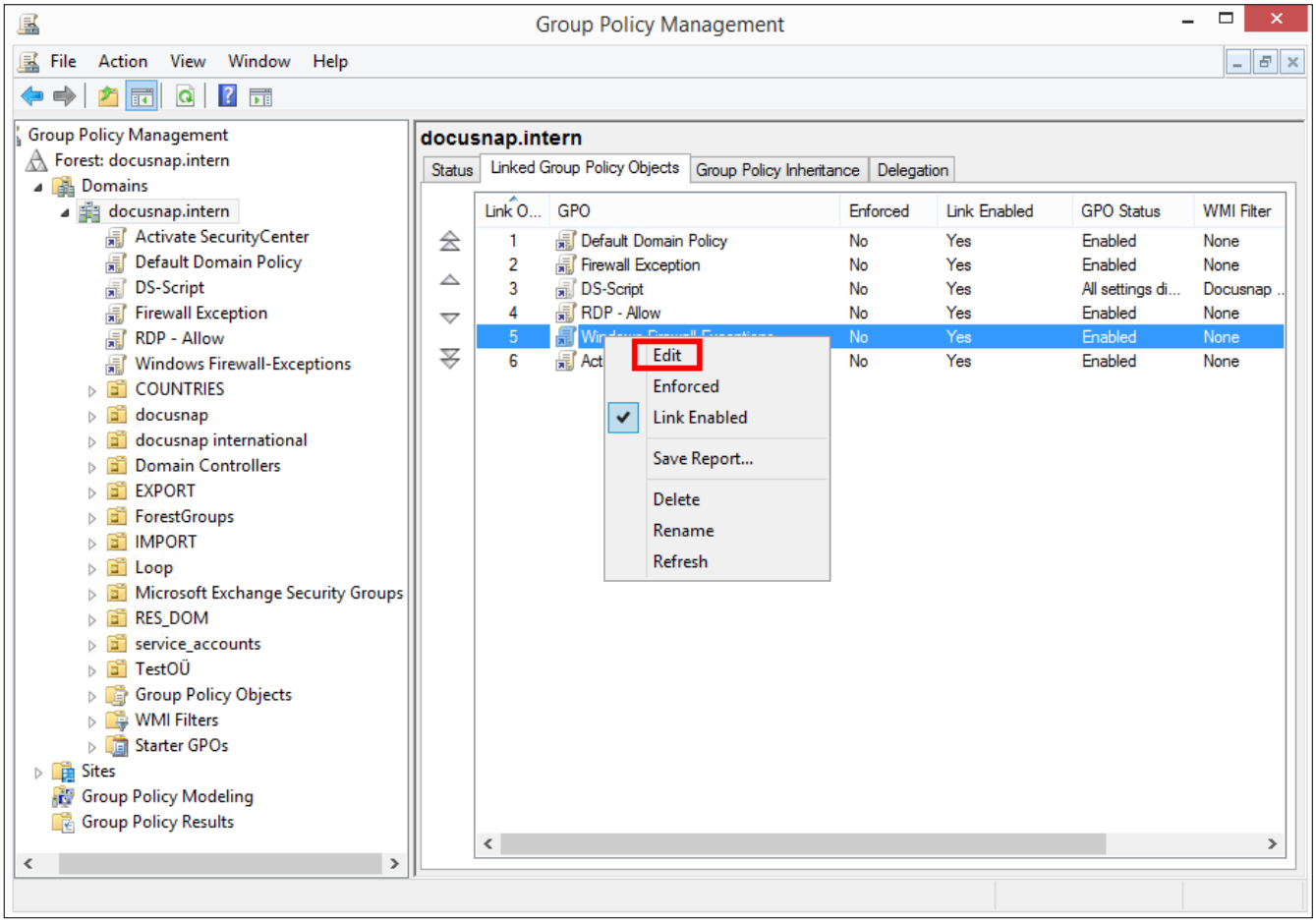

Fig. 4 - Editing a group policy object

The Group Policy Management Editor window opens:

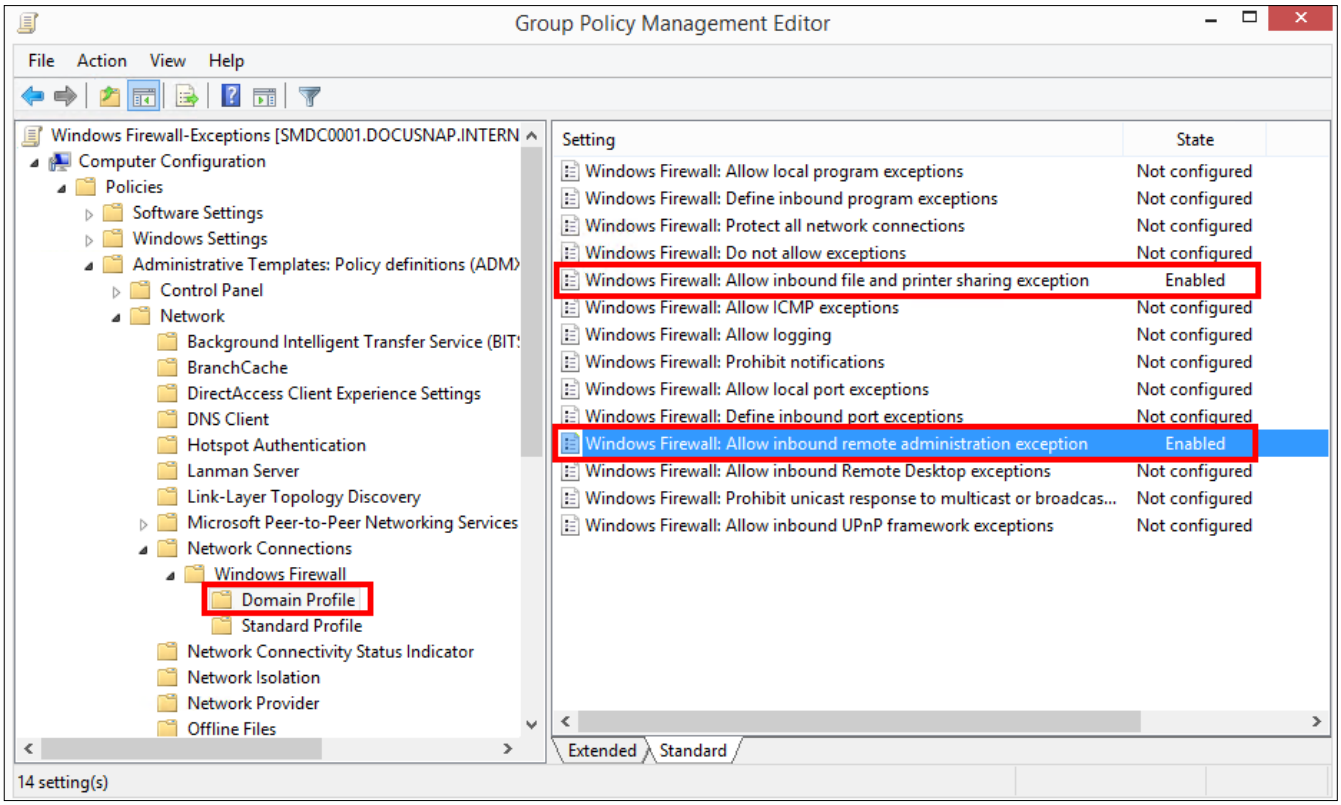

Fig. 5 - Group Policy Management Editor window

The group policies to be configured are in the following path:

- Computer Configuration
  - Policies
    - Administrative Templates
      - Network
        - Network Connections
          - Windows Firewall
            - Domain Profile

Click **Change settings** to edit the apps and features listed here. This is only possible if you have adequate rights. Windows 10 manages three different types of networks: Domain, Private, and Public. You need to define the firewall exceptions separately for each type. Define the following exceptions for the network types in use by setting the corresponding checkmarks in the **Allowed apps and features** list.

- File and Printer Sharing
- Windows Management Instrumentation (WMI)

Click the **OK** button to apply the new settings. The firewall settings thus defined allow Docusnap to scan the computer.

LIST OF FIGURES

VERSION HISTORY

Date	Description
01/03/2017	HowTo Creation
10/24/2018	Screenshots updated and modified content to Windows 10

