

Deployment of NetOp Netfilter Business using Active Directory Group Policies

This guide describes how to use group policies to activate NetOp Netfilter for selected users while, optionally, leaving other users unfiltered in a Windows 2000 environment using Active Directory for user management.

NetOp Netfilter operates as a proxy server. To activate Netfilter for a user, this user's browsers must be configured to use Netfilter as proxy when accessing the web. The steps outlined below will do this for Microsoft Internet Explorer.

Create Groups

1. Open *Active Directory Users and Computers*, which is available from the Start menu:

Start > Programs > Administrative Tools > Active Directory Users and Computers

This program is shown in Figure 1.

2. Locate the domain containing the users that must have their Internet traffic filtered. If users from several domains must be filtered, you may repeat the steps below for each domain.

3. Create, in this domain, two groups of users: *FilteredUsers* and *UnfilteredUsers*.

A group is created by right-clicking on the container and choosing *New > Group* in the pop-up menu (see Figure 2). The group type should be *Security* and the scope *Domain local*.

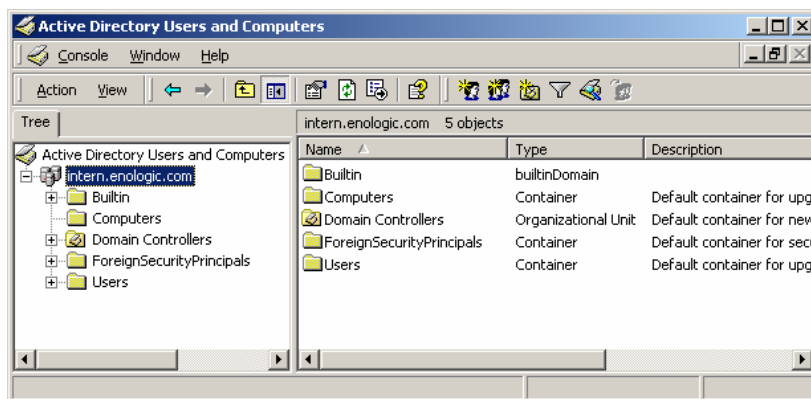


Figure 1: Active Directory Users and Computers.

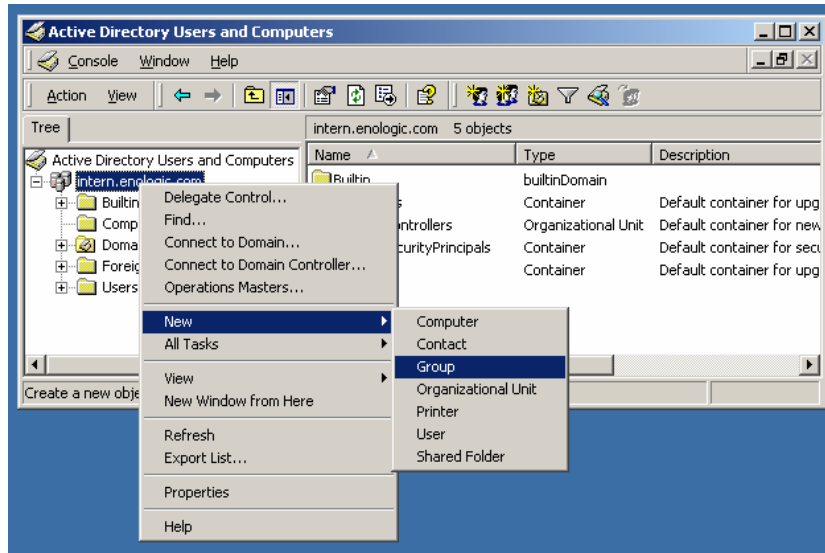


Figure 2: Creating a new group.

Add Users to Groups

4. Add all users that are to use the Netfilter proxy to *FilteredUsers* and all other users to *UnfilteredUsers*. You can add users to a group by

- double-clicking on the group and choosing the members on the *Members* tab in the group properties window,
- double-clicking on the person to add a choosing the group on the *Member of* tab in the user properties window, or
- choosing the users, right-clicking on one of them and choosing *Add members to a group*.

Create “Netfilter On” Group Policy

5. Open the properties window for the domain by right-clicking on the domain and choosing *Properties*. Go to the *Group Policy* tab, shown in Figure 3.

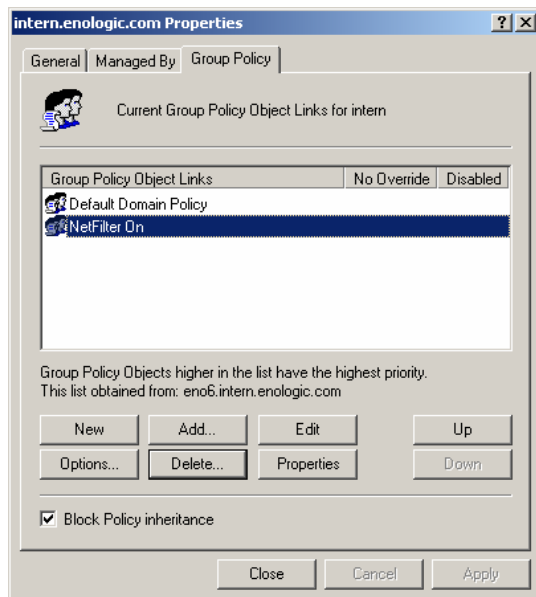


Figure 3: Creating a group policy.

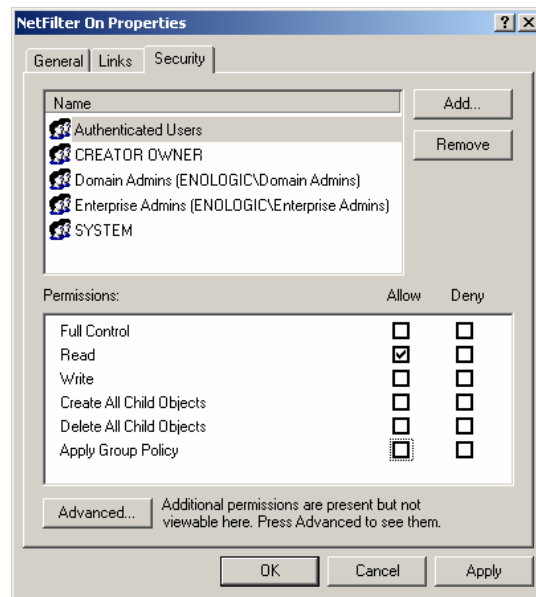


Figure 4: Group policy properties.

- 6a. Click *New* to add a new group policy and name it *Netfilter On*.
- 6b. Open the properties window for this policy by clicking on the *Properties* button. In the properties window, go to the *Security* tab, shown in Figure 4. Choose the group *Authenticated Users* and remove the checkmark in the *Allow* column for *Apply Group Policy*.
- 6c. Click *Add* to add a new group. The window shown in Figure 5 will appear. Choose the group *FilteredUsers* and press *Add*, then *OK*.
- 6d. Back on the *Security* page, check the *Allow* checkbox for *Apply Group Policy*, as shown in Figure 6. Choose *OK*.

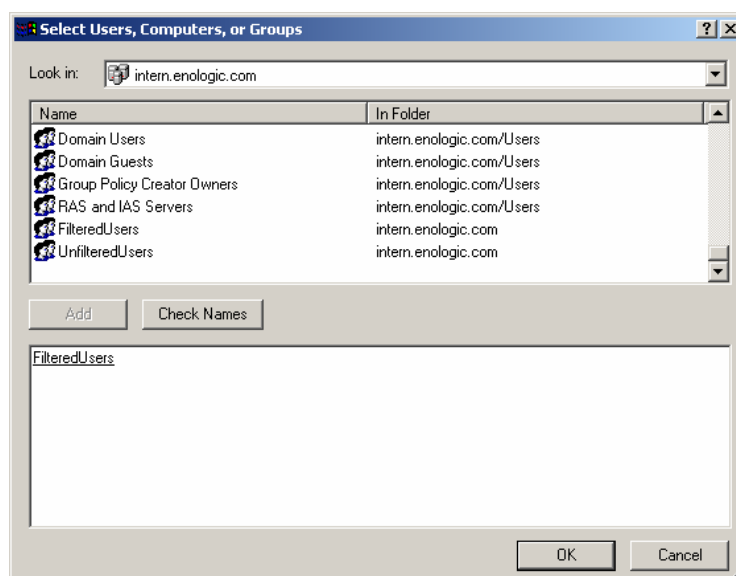


Figure 5: Adding a group to the group policy access control list.

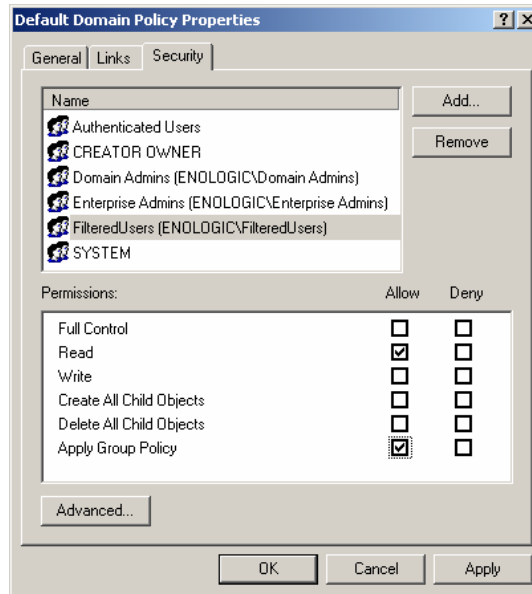


Figure 6: Configuring group policy to be applied to the FilteredUsers group.

Create “Netfilter Off” Group Policy

7a. Click *New* to add a new group policy and name it *Netfilter Off*.

7b. Open the properties window for this policy by clicking on the *Properties* button. In the properties window, go to the *Security* tab. Choose the group *Authenticated Users* and remove the checkmark in the *Allow* column for *Apply Group Policy*.

7c. Click *Add* to add a new group. Choose the group *UnfilteredUsers* and press *Add*, then *OK*.

7d. Back on the *Security* page, check the *Allow* checkbox for *Apply Group Policy*. Choose *OK*.

Configure “Netfilter On” Group Policy

8a. Double-click on the *Netfilter On* policy. This will open the Group Policy snap-in, shown in Figure 7.

8b. Go to *User Configuration > Windows Settings > Internet Explorer Maintenance > Connection* and double-click on *Proxy Settings*.

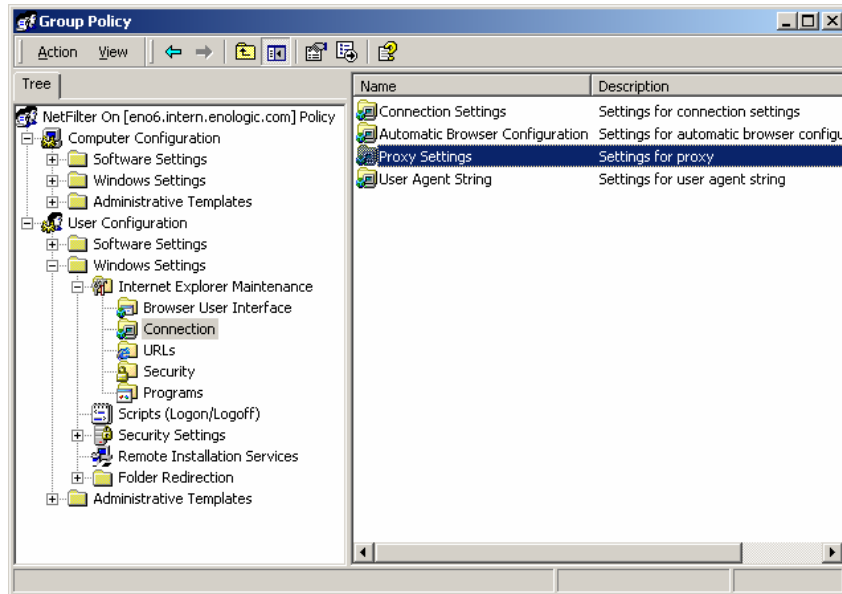


Figure 7: Group policy proxy settings.

8c. Check *Enable proxy settings* and enter the address and port of the Netfilter proxy in the HTTP fields as shown in Figure 8. Uncheck *Use the same proxy server for all addresses*. If you use one or more proxies for the other types of traffic, the addresses and ports of these should be entered in the other fields. Configure *Exceptions* as desired. Note that if *Do not use proxy server for local (intranet) addresses* is checked, web pages on your intranet will not be filtered. Choose *OK* to return to the Group Policy window.

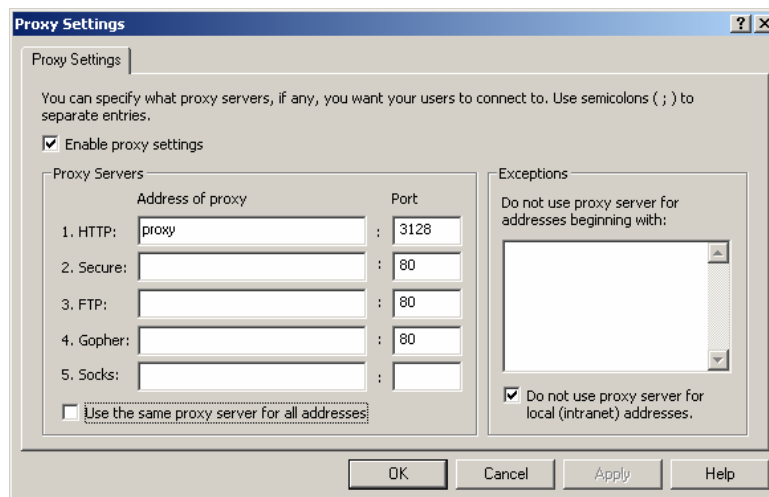


Figure 8: Configuring proxy settings for Internet Explorer.

8d. If you use automatic browser configuration on your network, you should disable this for the users in the *FilteredUsers* group. Do this by double-clicking on *Automatic Browser Configuration* and unchecking *Automatically detect configuration settings* and *Enable Automatic Configuration*.

8e. To prevent users from modifying proxy settings (and thereby avoiding filtering), go to *User Configuration > Administrative Templates > Windows Components > Internet Explorer*.

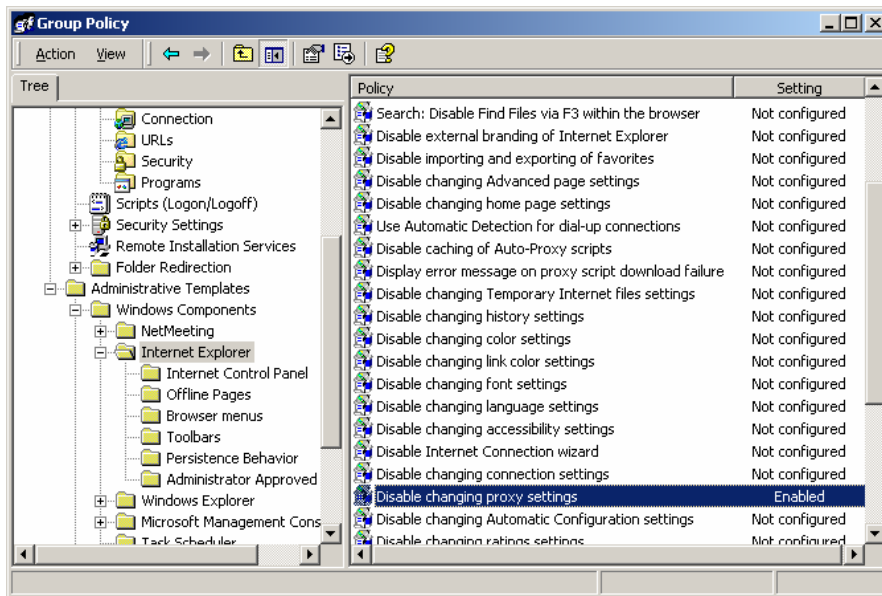


Figure 9: Internet Explorer user interface policy.

Double-click on *Disable changing proxy settings* and set the value to *Enabled*, as shown in Figure 9. You may want to do the same for *Disable changing Automatic Configuration settings*, *Disable changing connection settings*, and/or *Disable Internet Connection wizard*.

8f. Go to *User Configuration > Administrative Templates*. Right-click on *Administrative Templates* and choose *Add/Remove Templates*, as shown in Figure 10. This will result in the window shown in Figure 11 being opened. Choose *Add* and open the file *enologic.adm*, which is located in the *Scripts* subdirectory in the directory that NetOp Netfilter was installed to. Then choose *Close* to return to the group policy window.

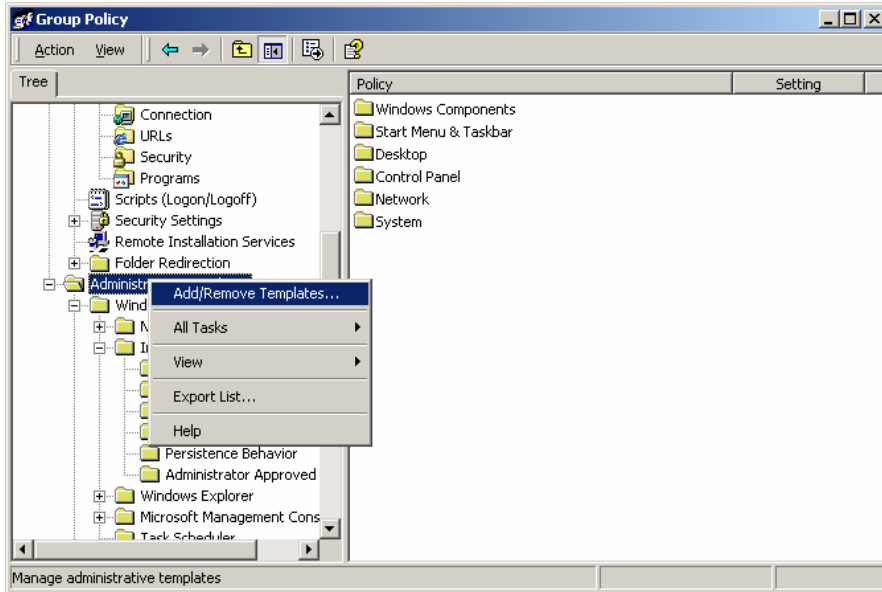


Figure 10: Adding custom administrative template.

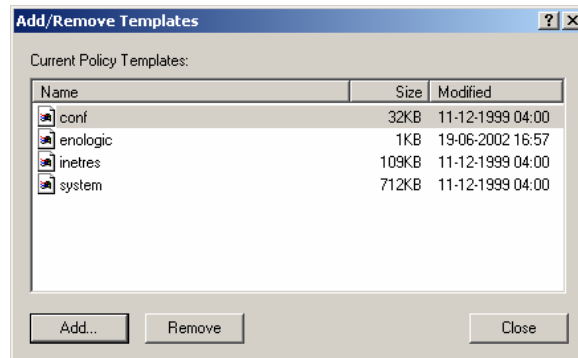


Figure 11: Add/Remove Templates dialog.

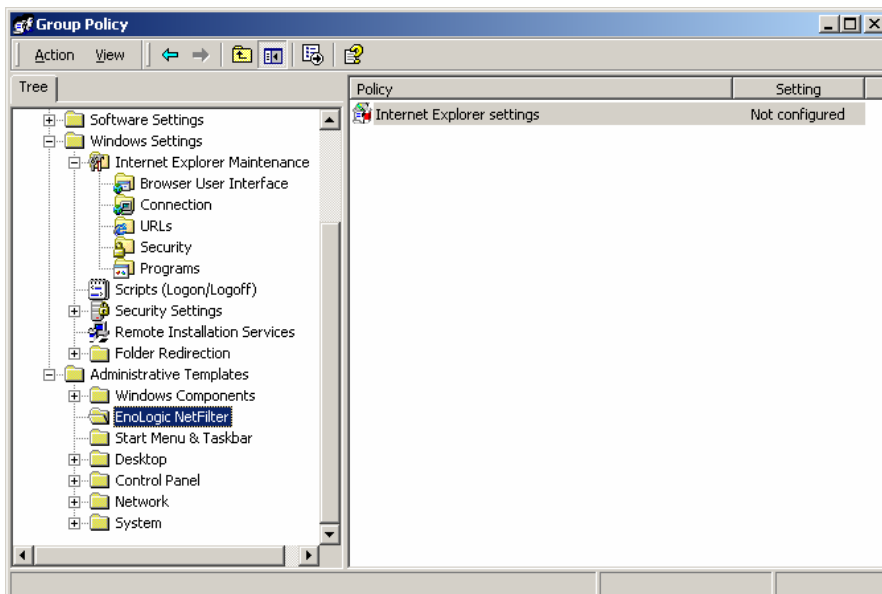


Figure 12: NetOp Netfilter administrative template.

8g. In the group policy window, the entry *User Configuration > Administrative Templates > NetOp Netfilter* has now appeared. Left-click, then right-click on *NetOp Netfilter* and make sure that the option *View > View Policies Only* is not checked. Then double-click on *Internet Explorer settings* and enable the policy, as shown in Figure 13. Press *OK* to accept the default settings. (*Use HTTP 1.1 through proxy connections* should be checked for the best performance. It is recommended to use the default values for the *Max. connections...* entries, but increasing the values may decrease the delays experienced when surfing through the proxy. However, if the values are too high, requests from the browser will be lost and the users will experience missing images on the web pages.)

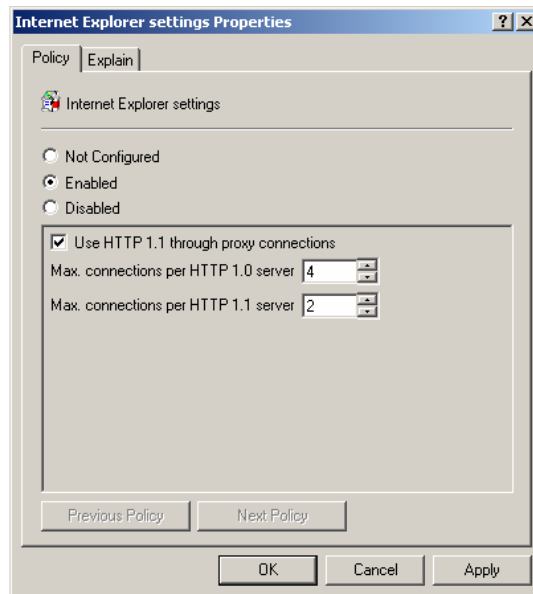


Figure 13: "Internet Explorer settings" policy.

8h. Close the Group Policy snap-in.

Configure "Netfilter Off" Group Policy

9a. Double-click on the *Netfilter Off* policy. This will open the Group Policy snap-in.

9b. Go to *User Configuration > Windows Settings > Internet Explorer Maintenance > Connection* and double-click on *Proxy Settings*.

9c. Configure the proxy settings as desired, giving either direct access to the Internet (when *Enable proxy settings* is not checked), or access through a proxy server.

9d. If you use automatic browser configuration on your network, you may need to enable this for the users in the *UnfilteredUsers* group. Do this by double-clicking on *Automatic Browser Configuration* and checking *Automatically detect configuration settings* and/or *Enable Automatic Configuration* and fill out the other information as desired.

9e. To undo the changes done in step 8e to prevent users from modifying proxy settings (if a user is moved from the *FilteredUsers* group to the *UnfilteredUsers*

group), go to *User Configuration > Administrative Templates > Windows Components > Internet Explorer*.

Double-click on *Disable changing proxy settings* and set the value to *Disabled*. You may want to do the same for *Disable changing Automatic Configuration settings*, *Disable changing connection settings*, and/or *Disable Internet Connection wizard*. Close the Group Policy window.

Finish

10. Close the domain properties window and the *Active Directory Users and Computers* window. The users you added to the *FilteredUsers* group will now use the Netfilter proxy when accessing the web (they may have to login again before the new policy is applied).

If a user in the *FilteredUsers* group must have unfiltered access to the Internet, simply remove him from the *FilteredUsers* group and add him to the *UnfilteredUsers* group, instead. Please note that just removing him from the *FilteredUsers* group may not be sufficient to change whether he uses the Netfilter proxy – he must be added to the *UnfilteredUsers* group for the proxy settings to be changed. Similarly, you can remove a user from the *UnfilteredUsers* group and add him to the *FilteredUsers* group to activate filtering for this user.