

Chapter Twelve (b): General Information on Site Lists for Guardian

Summary of Chapter:

- General Information on Site Lists and how Site Lists are connected to User Groups.
- How to check if individual URLs are being categorised correctly by the 'User Groups' you have created.

What you need:

- Knowledge of Admin user account and valid password for your CachePilot.
- A UTM PoP code. CachePilot users please contact Equinet for a quote.

Software Revision Required:

- Applicable to software revision 5.2.0 > CachePilots



Site Lists are part of 'Web access rules' which are applied when editing or adding 'User Groups' in the User Accounts / Groups section.

Site Lists:

- Log on to the CachePilot as shown in Chapter One (b).
- From the left-hand side of the screen, select 'Web', then 'Filtering' and then 'Site lists'. (All links are highlighted below).

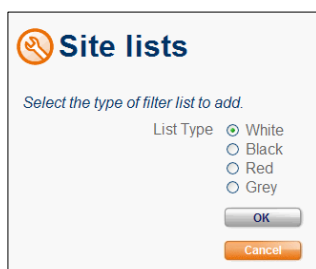



- The default Site Lists are highlighted left.

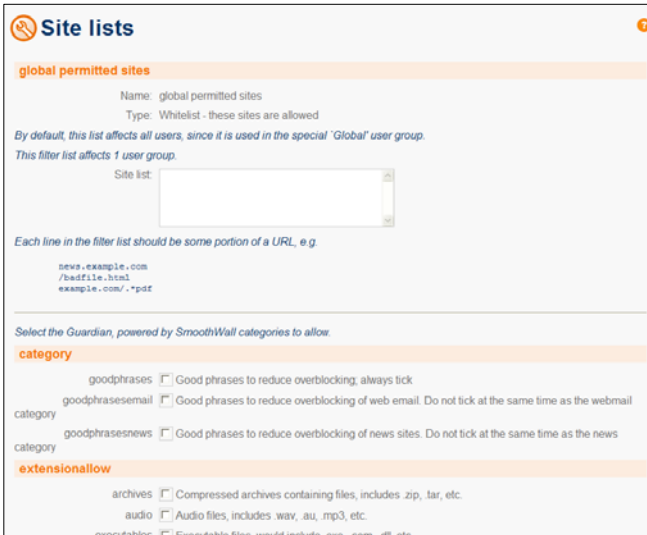


These Site Lists are blank as default, until you edit them.

- To edit any Site Lists, select the Site List you want and then select the 'Edit' button.
- In addition to the default Site Lists, you can create your own. Select the 'Add' button and you will be presented with the below screen:



 Here is more information about the different site lists you can create:



Site lists

global permitted sites

Name: global permitted sites
Type: Whitelist - these sites are allowed

*By default, this list affects all users, since it is used in the special 'Global' user group.
This filter list affects 1 user group.*

Site list:

Each line in the filter list should be some portion of a URL, e.g.

```
news.example.com
/badfile.html
example.com/*.pdf
```

Select the Guardian, powered by SmoothWall categories to allow.

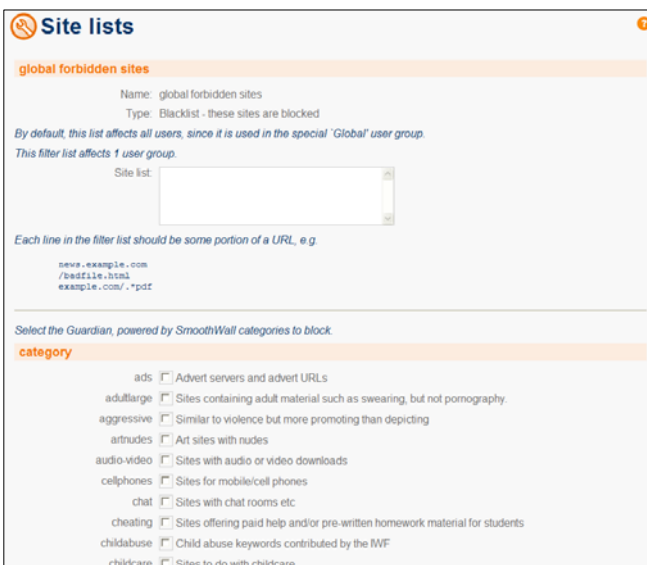
category

goodphrases Good phrases to reduce overblocking, always tick
goodphrasesemail Good phrases to reduce overblocking of web email. Do not tick at the same time as the webmail category
goodphrasenews Good phrases to reduce overblocking of news sites. Do not tick at the same time as the news category

extensionallow

archives Compressed archives containing files, includes zip, tar, etc.
audio Audio files, includes wav, au, mp3, etc.
overridables Executable files would include exe, com, dll etc.

White – Whitelists can override blacklists and redlists. They will only allow the sites which have been entered into the 'Site List:' text box and exceptions which are provided by Guardian.



Site lists

global forbidden sites

Name: global forbidden sites
Type: Blacklist - these sites are blocked

*By default, this list affects all users, since it is used in the special 'Global' user group.
This filter list affects 1 user group.*

Site list:

Each line in the filter list should be some portion of a URL, e.g.

```
news.example.com
/badfile.html
example.com/*.pdf
```

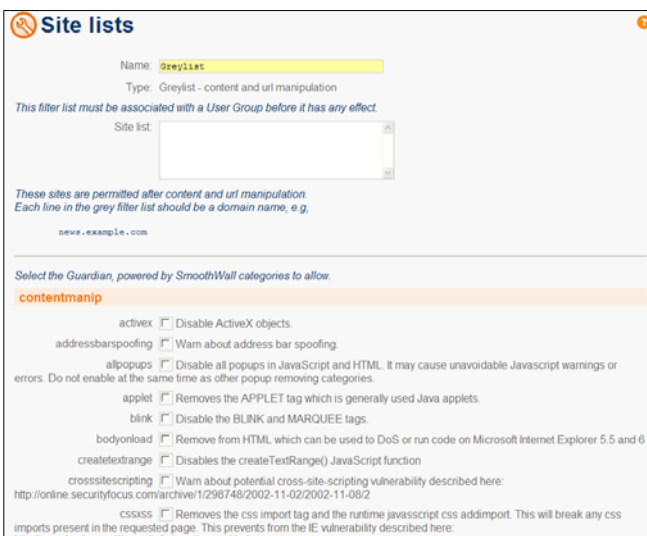
Select the Guardian, powered by SmoothWall categories to block.

category

ads Advert servers and advert URLs
adultlarge Sites containing adult material such as swearing, but not pornography
aggressive Similar to violence but more promoting than depicting
artnudes Art sites with nudes
audio-video Sites with audio or video downloads
cellphones Sites for mobile/cell phones
chat Sites with chat rooms etc
cheating Sites offering paid help and/or pre-written homework material for students
childabuse Child abuse keywords contributed by the IWF
childcare Sites to do with childcare

Black – Blacklists block specific sites. They will block sites entered into the 'Site List:' text box and selected categories of sites, which are provided by Guardian.

Red – Redlists are similar to blacklists. They are block lists which can be used for more severe URLs than the standard blacklists. A suitable error.cgi script can be setup to react to red list block messages and if necessary send an email when triggered. (This is also true of all block messages). In a Redlist you can only enter URL's into the text box provided.



Site lists

Name: **greylist**

Type: Greylist - content and url manipulation

This filter list must be associated with a User Group before it has any effect.

Site list:

*These sites are permitted after content and url manipulation.
Each line in the grey filter list should be a domain name, e.g.*

```
news.example.com
```

Select the Guardian, powered by SmoothWall categories to allow.

contentmanip

activex Disable ActiveX objects
addressbarspoofing Warn about address bar spoofing
alpopups Disable all popups in JavaScript and HTML. It may cause unavoidable Javascript warnings or errors. Do not enable at the same time as other popup removing categories.
applet Removes the APPLET tag which is generally used Java applets.
blink Disable the BLINK and MARQUEE tags
bodyload Remove from HTML which can be used to DoS or run code on Microsoft Internet Explorer 5.5 and 6
createtextrange Disables the createTextRange() JavaScript function
crosssitescripting Warn about potential cross-site-scripting vulnerability described here: <http://online.securityfocus.com/archive/1/298748/2002-11-02/2002-11-08/2>
cssxss Removes the css import tag and the runtime javascript css addimport. This will break any css imports present in the requested page. This prevents from the IE vulnerability described here: http://www.beuker.nl/03secvuln/iecss_import.html

Grey – Greylists allow access to URLs like Whitelists. Guardian adds additional category options for the manipulation of content and URLs. These include the 'force safe search' category, which will manipulate URLs sent to various search engines (Google, Singingfish, Ilse, KEL, Lycos, Alltheweb, Yahoo, Hotbot, Wisenut) so that 'safe searching' is activated.



Be careful not to exceed the character size limit of 10,000 characters for each of the Site Lists text box, in which you can enter URLs.

Site Lists & User Groups:



User Groups use Site Lists to implement browsing controls. Listed below are standard User Groups with the Site Lists they contain. As default the Site Lists are blank and have no URLs or categories selected.

Controlled:

Allow Permitted sites

Filters for Anonymous user (this group applies if the firewall does not require users to log in before using the web proxy):

This contains no Site Lists as default.

Global: this group applies to all users

Allow Global Permitted sites

Block Global Forbidden sites

Allow Global manipulated sites

Limited:

Block and report restricted sites

Block forbidden sites during work hours

Open:

This contains no Site Lists as default.

Guardian:

Guardian differs from Smartfilter and Netsweeper in that it uses a number of filtering techniques that are all resident on the CachePilot. Therefore no additional servers are required locally or remotely to hold lists or undertake checks. The administrator of the local CachePilot defines which users may view which categories - so local flexible controls are available – which is often a key requirement. The technology uses a combination of URL list checking – against a somewhat smaller list than Smartfilter or Netsweeper – but, significantly, also employs additional real-time content checking, which Smartfilter or Netsweeper do not currently provide.



Tip!

For further information on Smartfilter or Netsweeper please see Chapter 12 and 13.

For further information on Guardian please see other sections of Chapter 12.

Test URL-Filtering:

Log on to the CachePilot as shown in Chapter One (b).

From the left-hand side of the screen, select 'Web', then 'Filtering' and then 'Test URL'. (All links are highlighted below).



In the drop down list select a User you wish to test.


In the text box enter a URL you wish to test. You must manually enter the syntax 'http://' or 'https://' or 'ftp://' etc before the 'www.sitename.com'.

Select 'OK'.

The CachePilot will then display the filter results after going through a process of checking the following:

- Timeband controls
- Global filtering controls
- Blacklist/Whitelist controls depending on the User Group.

In the below example,

 **Test URL filtering**

*Traffic matching these firewalls will use the **Filters for anonymous user** group rules:*

- Trusted/Local 'web proxy'
- DMZ/Internet 'web'
- DMZ/Local 'web proxy'
- Controlled/Local 'web proxy'

Users do not have to give a username and password. Leave the username below **blank** for this test.

Username:

URL to test:

Filter results

Browser gave us user: bob
Local user found.
Using NetPilot VPN group: bob's group
This user lookup cached: Nov 13 16:58:30

Guardian blocked the request;
Reason: Banned Regular Expression URL found.
Block One

The user is 'bob' who is in the User Group 'bobs_group' which contains the Site List 'Block One'.

All Global and individual Whitelists are applied first.

Then all Global and individual Blacklist are applied.


In the User Group 'bob's group' the URL was matched in a Blacklist (block_one).

The final decision was to block the request.

The test results will show the Site List matched.

In the example below, the user is anonymous and the URL has not been blocked in the Global Rules or the 'Filters for anonymous user' Group, therefore, it has been allowed.

No individual User Groups are applied as the user is anonymous and the CachePilot does not know which User Group the anonymous user belongs to. Therefore, it applies the User Group 'Filters for anonymous users'.

 **Test URL filtering**

*Traffic matching these firewalls will use the **Filters for anonymous user** group rules:*

- Trusted/Local 'web proxy'
- DMZ/Internet 'web'
- DMZ/Local 'web proxy'
- Controlled/Local 'web proxy'

Users do not have to give a username and password. Leave the username below **blank** for this test.

Username:

URL to test:

Filter results

Browser gave us user: -
Local group found.
Using NetPilot VPN group: anonymous
This user lookup cached: Nov 13 16:19:13

Guardian allowed the request.



When URL filtering is applied to Users' browsing, 'Whitelists' are always implemented first, then 'Blacklists'. If users are accessing the Internet anonymously, without having to authenticate with the unit, 'Filters for anonymous user' will be applied with the Global Groups.



For more information on Sites Lists please see the other sections of Chapter 12.