



MYSURFGUARD

Administration Manual

Version 1.2

OPEN SOURCE COMPETENCY CENTRE (OSCC) MAMPU

Level 3, APT E302-E304
Enterprise Building, Persiaran APEC
63000 Cyberjaya
Selangor
Tel: (6)03-8319 1200
Fax: (6)03-8319 3206
E-mail: helpdesk@oscc.org.my
<http://opensource.mampu.gov.my>

Table of Contents

Introduction.....	1
System Requirement.....	3
Hardware.....	3
Software	3
Log-in to MySurfGuard.....	4
Webmin.....	5
Webmin Configuration	6
DansGuardian.....	8
From Webmin page.....	9
MAINTENANCE.....	10
Network connections.....	10
Log files.....	10
Services.....	10
Package update/patch.....	10
Disk Space.....	11
Password change.....	11
Service update.....	11

Illustration Index

Illustration 1: Login to Webmin.....	4
Illustration 2: Webmin Interface.....	5
Illustration 3: Webmin Modules.....	6
Illustration 4: Insert your Webmin Module that you already install from your computer.....	7
Illustration 5: View/Edit Groups in DansGuardian.....	9

Introduction

A content filter is a software program that either blocks or allows access to Internet content depending on whether or not the content meets a set of criteria. These criteria depend on the filtering rules available in the software. Some filter look for keywords or phrases while others are based on lists of an Internet sites.

This document specifies the system requirements and installation instructions to set up MySurfGuard, an open source software (OSS) content filtering solution. MySurfGuard is a suite of OSS products which comprises of CentOS 5 Linux, Squid, DansGuardian and Webmin. Filtering capability is provided by DansGuardian which uses multiple methods for filtering, such as:

1. URL and domain filtering
2. Content phrase filtering
3. Platform for Internet Content Selection (PICS) filtering
4. Multipurpose Internet Mail Extensions (MIME) filtering
5. File extension filtering
6. POST limiting

The URL and domain filtering which is filtering by web address has configurable domain, user and source IP exception lists and is able to handle huge lists of internet sites.

The content phrase filtering will check for pages that contain profanities and phrases often associated with pornography and other undesirable content. PICS is a technical specification that enable users to easily find appropriate content or avoid content that they consider inappropriate or unwanted. The specification ease the creation of, and access to, labeling schemes associated with content selection and filtering mechanisms. MIME filtering controls

what headers are passed from your browser to websites. The Mime Filtering rule definitions are implemented using the threepartscheme of rules Global or Default, Allow, and Deny. File extension filtering blocks unwanted file extension, for example unknown .exe files which is possible to execute virus in the PC. The POST filtering block or limit web upload.

MySurfGuard can be configured according to the organization's needs thus giving the system administrator flexibility and total control over what to filter. The additional features of Webadmin software tool enables the system administrator to produce easy to read logs and to easily generate reports/statistics.

System Requirement

Below is minimum requirement needed to install MySurfGuard:

Hardware

- **Model:** Pentium IV
- **Memory:** 512MB RAM
- **Storage:** 10GB HD
- **Network Interface Card:** 1 or 2

Software

- **Operating System:** CentOS 5
- **Web Caching Proxy:** Squid
- **Web Content Filtering:** DansGuardian
- **Web Based Administration Tool:** Webmin

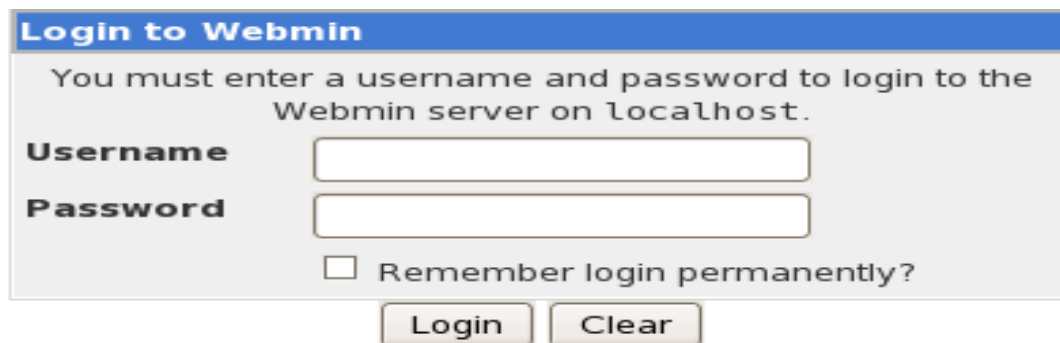
Log-in to MySurfGuard

Open your web browser to login to the MySurfGuard. It will prompt for username and password. Then click on the Login button. Example as below:

Mail URL: <https://localhost:10000>

Username: root

Password: [use your rott password]



The image shows a web browser window titled "Login to Webmin". The main text inside the window says "You must enter a username and password to login to the Webmin server on localhost." Below this text are two input fields: "Username" and "Password". Under the "Password" field is a checkbox labeled "Remember login permanently?". At the bottom of the form are two buttons: "Login" and "Clear".

Illustration 1: Login to Webmin

Webmin

Webmin is a web-based interface for system administration for Unix. Using any modern web browser, you can setup user accounts, Apache, DNS, file sharing and much more. Webmin removes the need to manually edit Unix configuration files like `/etc/passwd`, and lets you manage a system from the console or remotely.

For more info, check website at <http://www.webmin.com/>

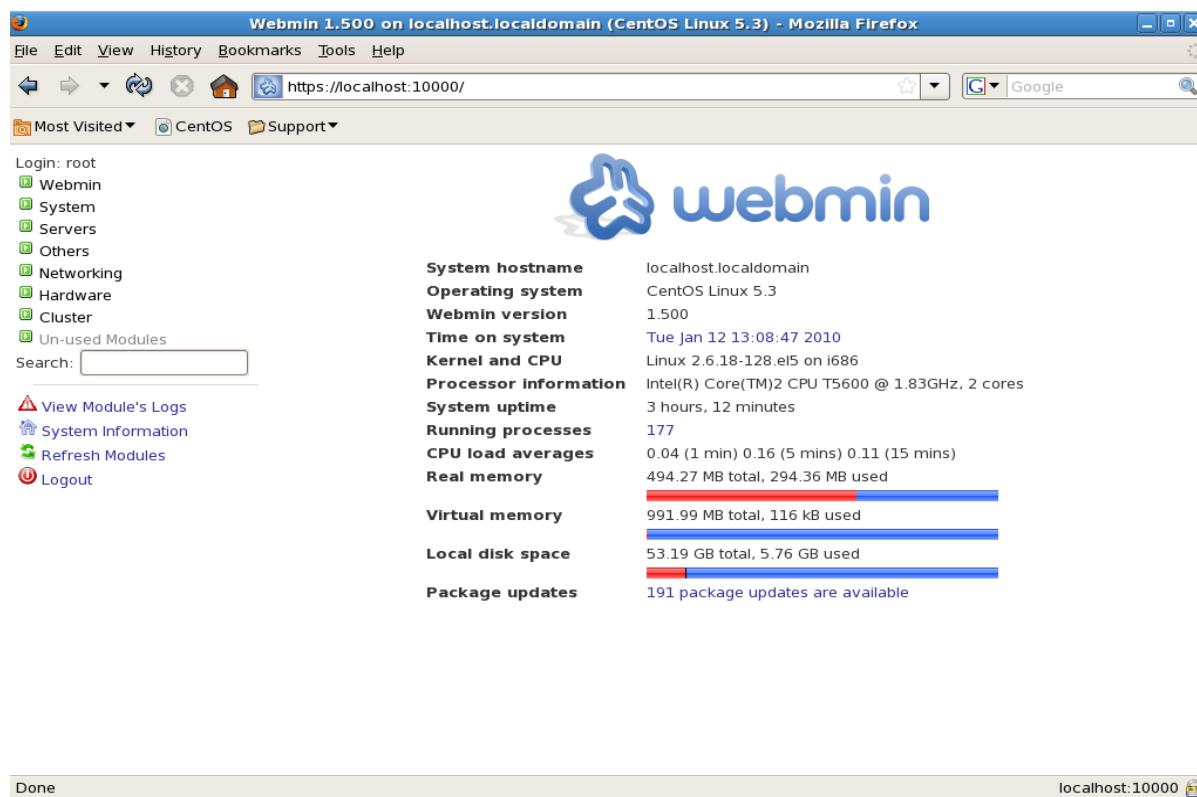


Illustration 2: Webmin Interface

Webmin Configuration

To administer DansGuardian from Webmin, you have to install DansGuardian Webmin module

1. Download module from repos <http://repos.oscc.org.my/centos/5/i386/CentOS/dg-0.5.10-pr4.wbm>
2. Go to your Webmin page at your browser
3. From the left side menu choose Webmin → Webmin Configuration
4. From Webmin Configuration menu, choose Webmin Module icon

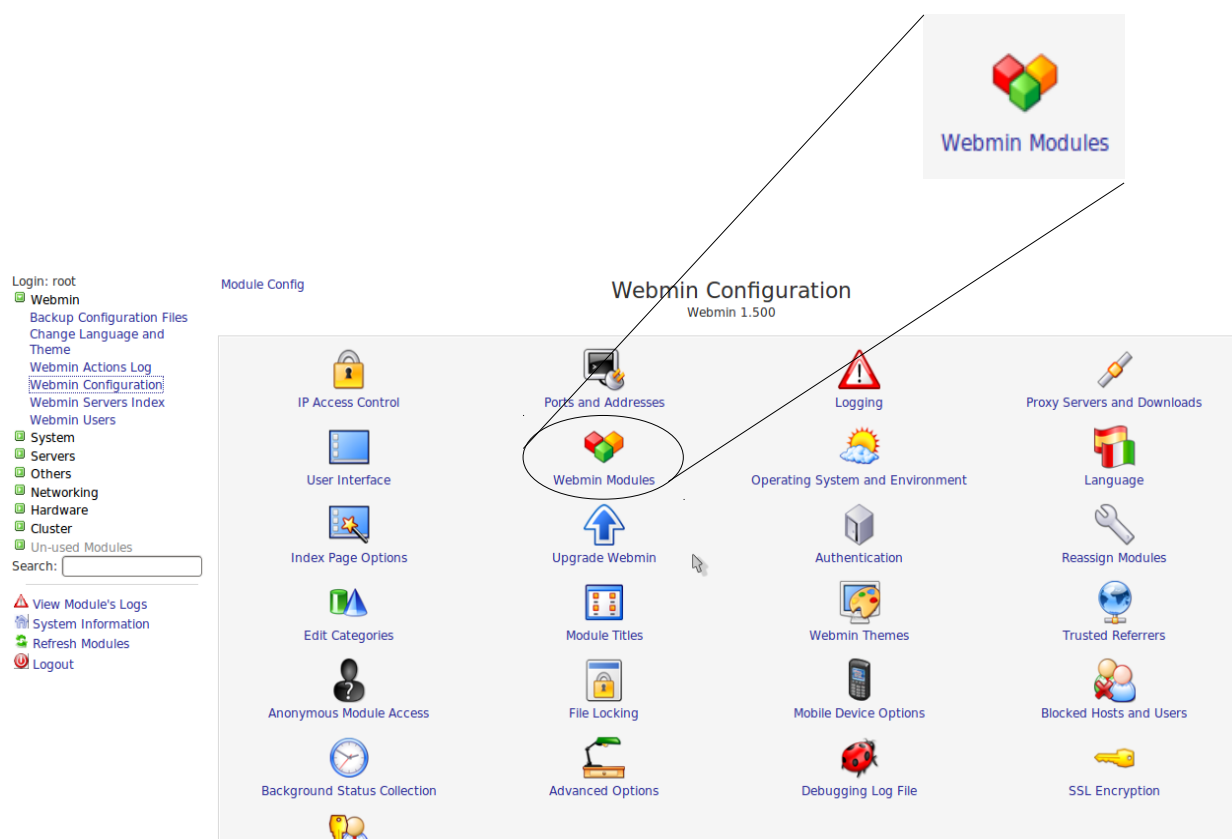


Illustration 3: Webmin Modules

5. Select install from uploaded file. Click browser button and find the downloaded webmin module from your computer

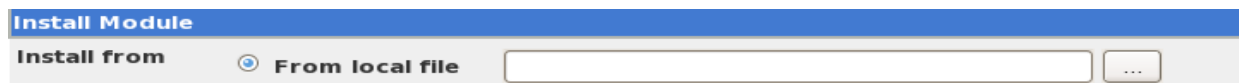


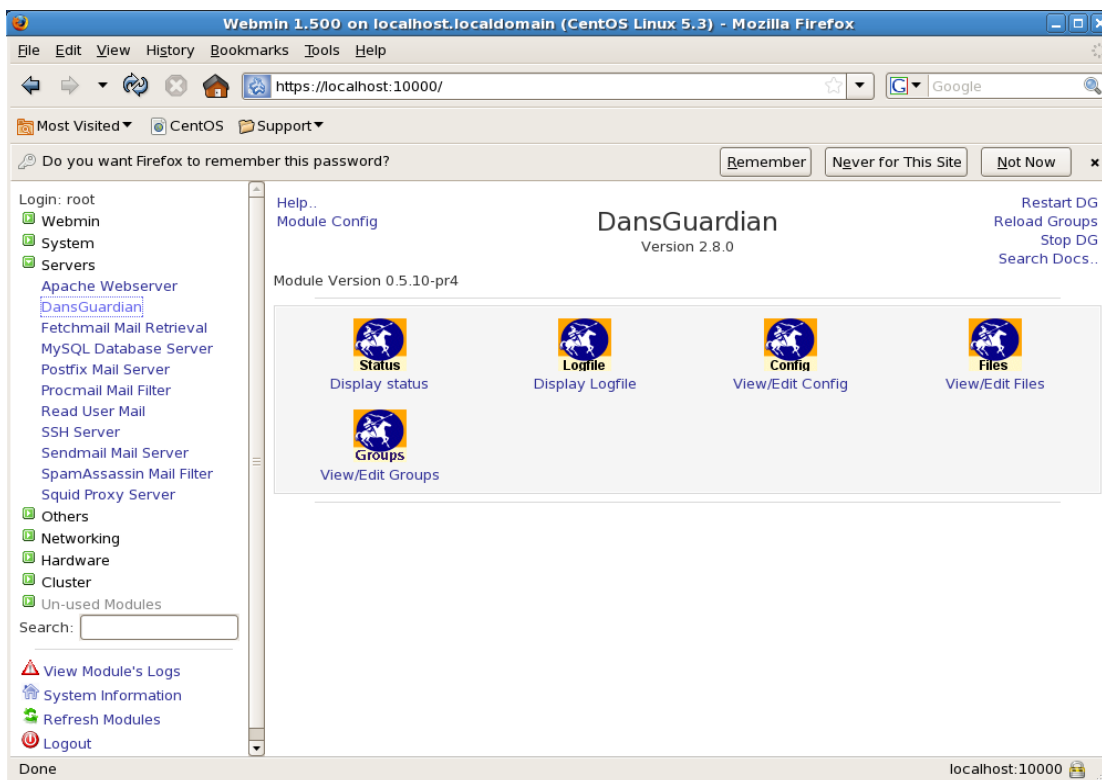
Illustration 4: Insert your Webmin Module that you already install from your computer

DansGuardian

DansGuardian is an award winning Open Source web content filter which currently runs on Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX, and Solaris. It filters the actual content of pages based on many methods including phrase matching, PICS filtering and URL filtering. It does not purely filter based on a banned list of sites like lesser totally commercial filters.

DansGuardian is designed to be completely flexible and allows you to tailor the filtering to your exact needs. It can be as draconian or as unobstructive as you want. The default settings are geared towards what a primary school might want but DansGuardian puts you in control of what you want to block.

For more info. Check website at <http://dansguardian.org>



From Webmin page

1. Go to Servers and Click DansGuardian
2. When DansGuardian page appears, choose View/Edit Groups
3. It will appear all settings

[Module Index](#)

View/Edit Groups

DG version: 2.8.0

Number of groups: 1

[Edit Group f1](#)

Group settings for f1

Naughtyness limit: 50

Bypass time limit: 0

Bypass key:

/etc/dansguardian/bannedphraselist	edit
/etc/dansguardian/exceptionphraselist	edit
/etc/dansguardian/weightedphraselist	edit
/etc/dansguardian/bannedsitelist	edit
/etc/dansguardian/greysitelist	edit
/etc/dansguardian/exceptionsitelist	edit
/etc/dansguardian/bannedurllist	edit
/etc/dansguardian/greyurllist	edit
/etc/dansguardian/exceptionurllist	edit
/etc/dansguardian/bannedregexpurllist	edit
/etc/dansguardian/bannedextensionlist	edit
/etc/dansguardian/bannedmimetyplist	edit
/etc/dansguardian/pics	edit
/etc/dansguardian/contentregexplist	edit

Illustration 5: View/Edit Groups in DansGuardian

MAINTENANCE

The following should be checked on a regular basis:

Network connections

The administrator should verify the server is reachable from the public network to avoid service interruption. Network monitoring is beyond the scope of these manual.

Log files

With the log files, it is possible to identify and monitor hardware and software problems on the servers. The log files should be checked at least once a week. All log files in /var/log/ directory.

Services

Used to start, stop or cancel a service on a local or remote computer. It is also a tool to set up recovery actions to take place if a service should fail. Should be checked in case of service failure.

e.g:

```
[root@localhost ~]#/etc/init.d/[SERVICE_NAME] start
[root@localhost ~]#/etc/init.d/[SERVICE_NAME] stop
[root@localhost ~]#/etc/init.d/[SERVICE_NAME] status
```

Package update/patch

Check that the latest package update/patches has been installed on the servers. It should be checked and done at least once a month.

Disk Space

to verify that there is always enough space on the most mission critical servers. It should be done at least once a week. Use *df -lh* command.

Password change

Password should be changed periodically, at least every three months.

Service update

Check for services update for the main components in MySurfGuard such as DansGuardian and Squid.