



MYSURFGUARD

Installation 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 |
|------------------------|----|
| ARCHITECTURE | |
| SYSTEM REQUIREMENT | 4 |
| Hardware | |
| Software | 4 |
| DEPENDENCIES | 5 |
| OSS TECHNOLOGIES | 6 |
| CentOS 5 | 6 |
| Squid | 7 |
| DansGuardian | 8 |
| Webmin | 9 |
| INSTALLATION STEPS | 10 |
| MYSURFGUARD DEPLOYMENT | 12 |
| MAINTENANCE | 15 |
| Network connections | 15 |
| Log files | 15 |
| Services | |
| Package update/patch | 15 |
| Disk Space | 16 |
| Password change | 16 |
| Service update. | 16 |



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.



ARCHITECTURE

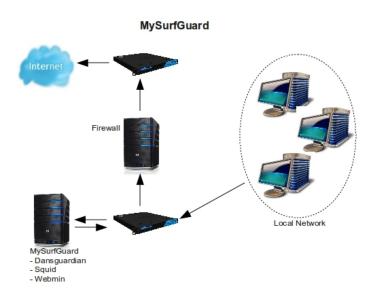


Illustration 1: MySurfGuard Diagram



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



DEPENDENCIES

Dependencies Resolved

| Package | Arch | Version | Repository | Size |
|---|---------|----------------------|-------------|-------|
| ======================================= | | | | |
| Installing: | | | | |
| mysurfguard | noarch | 1.2-1.oscc | oscc-repos2 | 2.4 k |
| Installing for depende | encies: | | | |
| dansguardian | i386 | 2.8.0.6-1.2 | oscc-repos2 | 279 k |
| oscc-tracking | noarch | 0.0.2-1.oscc | oscc-repos2 | 29 k |
| perl-Archive-Zip | noarch | 1.16-2 | oscc-repos2 | 72 k |
| perl-Compress-Zlib | i386 | 1.42-1.fc6 | base | 52 k |
| perl-HTML-Tagset | noarch | 3.10-2.1.1 | base | 15 k |
| perl-Net-IP | noarch | 1.25-2.fc6 | base | 31 k |
| perl-URI | noarch | 1.35-3 | base | 116 k |
| sarg | i386 | 2.2.3.1-1.e15.rf | oscc-repos2 | 563 k |
| squid | i386 | 7:2.6.STABLE21-3.el5 | base | 1.3 M |
| webmin | noarch | 1.500-1 | oscc-repos2 | 15 M |

Transaction Summary

Install 11 Package(s)
Update 0 Package(s)
Remove 0 Package(s)

Total download size: 18 M



OSS TECHNOLOGIES

CentOS 5

CentOS is an Enterprise class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS is perfect for servers and cluster nodes where newer software is not a requirement. CentOS preferred software updating tool is based on yum, although support for use of an uptodate variant exist. Each may be used to download and install both additional packages and their dependencies, and also to obtain and apply periodic and special (security) updates from repositories on the CentOS Mirror Network.

This following steps show how to install CentOS 5.

- Place the DVD/CDROM in your DVD/CDROM drive and boot your system from the DVD/CDROM. If the DVD/CDROM drive is found and the driver loaded, the installer will present you with the option to perform a media check on the DVD/CDROM. This will take some time, and you may option to skip over this step.
- 2. Welcome screen will be appear and click 'Next' to proceed.
- 3. Language selection Select the language and it will become the default language for the operating system once it is installed. Selecting the appropriate language also helps target your timezone configuration later in the installation. The installation program tries to define the appropriate time zone based on what you specify on this screen. Once you select the appropriate language, click 'Next' to continue.
- 4. Keyboard Layout Selection Select the correct layout type for the keyboard you would prefer to use for the installation and as the system default. Click 'Next' to continue installation.

MEMEM

5. Setup your disk partitioning, the first three option will perform automatic partitioning while 'Create customs layout' will perform manual partition.

6. For Network configuration, the installation program will automatically detects any network devices and its hostname. You can edit its configuration or just click 'Next' to continue.

7. Set your time zone by selecting the city closest to your computer's physical location. Select 'System Clock uses UTC' if your system is set to UTC.

8. Set root password. This is the most important steps because root account is used for system administration.

9. You can customize software selection of your system or do it after installation.

10. A screen preparing the installation will be appear. For your reference, a complete log of your installation can be found in /root/install.log once you reboot your system.

11. This step is when the installation program installing all the packages. How quickly this happens depends on the number of packages you have selected and your computer's speed.

12. Now your installation is complete. The installation program prompts you to prepare your system for reboot.

13. Then, start your CentOS Linux system in run level 5 (graphical run level), the Setup Agent is presented, which guides you through the CentOS Linux configuration. Using this tool, you can set up your system time and date, install software and more.

For more info about CentOS, check website at http://www.centos.org/

Squid

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces

MySurfGuard v1.2

MIMPU

bandwidth and improves response times by caching and reusing frequently-requested web

pages. Squid has extensive access controls and makes a great server accelerator. It runs on

most available operating systems, including Windows and is licensed under the GNU GPL.

For more info, check website at http://www.squid-cache.org/

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/



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/



INSTALLATION STEPS

- 1. Open terminal or console.
- 2. Install OSCC Repository

```
[root@localhost ~]# wget -c
http://repos.oscc.org.my/centos/5/os/i386/CentOS/oscc-repos-0.0.1-
1.noarch.rpm
[root@localhost ~]# rpm -Uvh oscc-repos-0.0.1-1.noarch.rpm
```

3. Install package MySurfGuard

```
[root@localhost ~]# yum install mysurfguard
```

4. Open your web browser and go to https://localhost.localdomain:10000/

Username: root

Password: USE_YOUR_ROOT_PASSWORD

- 5. To administer DansGuardian from Webmin, you have to install DansGuardian Webmin module
 - 5.1. Download the module from http://repos.oscc.org.my/centos/5/os/i386/CentOS/dg0.5.10 pr4.wbm
 - 5.2. Go to your Webmin page at your browser
 - 5.3. From the left side menu choose Webmin → Webmin Configuration
 - 5.4. From Webmin Configuration menu, choose Webmin Module icon
 - 5.5. Select install from uploaded file. Click Browse button and find the downloaded webmin module from your computer.



- 5.6. Select Install Module
- 5.7. You can monitor the Dansguardian module from Servers → Dansguadian
- 6. Post installation the following module configuration examples should be tailored to suite your installation:
- Full path to DG etc directory: /etc/dansguardian/
- Full path to filename for DG configuration: /etc/dansguardian/dansguardian.conf
- Full path to filename for AVPlugin configuration: /etc/dansguardian/virusscanner.conf
- Full path to DG pid file: /var/run/dansguardian.pid
- Full path to DG binary: /usr/sbin/dansguardian
- Full path to DG log directory: /var/log/dansguardian
- Full path to DG log file: /var/log/dansguardian/access.log
- Full path to public HTML directory: /var/www/html
- Build-in Restart method: Graceful
- Command to restart DG: /etc/init.d/dansguardian restart
- Command to start DG: /etc/init.d/dansguardian start
- Command to stop DG: /etc/init.d/dansguardian stop



MYSURFGUARD DEPLOYMENT

There are 2 options on how to deploy MySurfGuard solution to the users. First, by setting the Internet browser to use a proxy server. Secondly, by setting up a transparent proxy.

Web Browser Setting

- 1 Setting for Mozilla Firefox 2.0.0.6
 - 1.1 Go to Edit and select Preferences.
 - 1.2 Select Advanced
 - 1.3 Select Network tab and click on Settings button.
 - 1.4 Select Manual proxy configuration, then enable Use this proxy server for all protocol
 - 1.5 Enter the http proxy and port. http proxy is the ip of your proxy server and port is DansGuardian port number.
- 2 Setting for Internet Explorer 6
 - 2.1 Go to Tools and select Internet Options.
 - 2.2 Select Connections tab and click on LAN settings.
 - 2.3 Enable the Use a proxy server for your LAN in the Proxy Server box.
 - 2.4 Enter the IP address of the proxy server in the Address box and the port number in the port box.

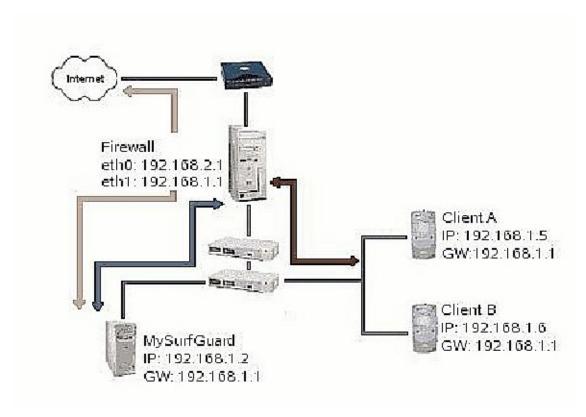
Transparent Proxy Setting

The ultimate goal of setting up content filtering is to have everybody use it, without being able to get around it. One way to do this is to block all out going web (port 80) requests, and only allow them from the proxy server. This will force every user to specify a port in their browser configuration as explained above. The second method is to set up a transparent



proxy. The advantage of transparent proxy over the first option is, it doesn't need any users intervention or for them to even aware of it.

Below is an example on how to set up a transparent proxy;



From the diagram, web requests by client A and B is redirected by the firewall to the MySurfGuard

server. In order to achieve this, squid must first be configured as both an httpd accelerator and a proxy

server.

1. Edit the following lines in /etc/squid/squid.conf

http_port 3128 transparent



2. You also may want to edit /etc/sysctl.conf

```
net.ipv4.ip_forward = 1

net.ipv4.conf.default.send_redirects = 0

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.eth0.send_redirects = 0

net.ipv4.conf.eth1.send_redirects = 0
```

3. After finish editing the /etc/sysctl.conf, load it with sysctl p command

Firewall setting

For this example, we are using IPTABLE. Please change your configuration to your respective firewall use. Redirection of clients web requests is handle by the firewall, in these example it is assumed that the firewall is running on a Linux box and using iptables.

Run these command or edit iptables configuration at /etc/sysconfig/iptables
 #iptables t mangle A PREROUTING j ACCEPT p tcp dport 80 s 192.168.1.2
 #iptables t mangle A PREROUTING j MARK setmark 3 p tcp dport 80

2. Run these command on the console

#ip rule add fwmark 3 table 2

#ip route add default via 192.168.1.2 dev eth1 table 2

Basically what the command above do is to mark (#3) any packets going to port 80 except the packets from mySurfGuard server. These specially marked packets will be routed through a special routing table (table 2), and eventually send to mySurfGuard server for processing.



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.