NGSecureWeb® v. 2.00 Technical Documentation

Document Version 1.0

Date: 09/09/2002

1. Preface 3

2. Introduction 4

3. Installation procedure 7

3.1 Windows installation 7

3.2 UNIX installation 9

4. Configuration 14

4.1 Long URL protection 16

4.2 Traversal Directory protection 16

4.3 Long Headers protection 16

4.4 Forbidden Words protection 16

4.5 Shellcode protection 17

4.6 Non Printable Characters protection 17

4.7 Method protection 17

4.8 Configuration considerations 18

5. Maintenance 19

6. FAQ's / Troubleshooting 20

6.1 Apache® HTTP Server 20

6.2 Iplanet / Netscape® Enterprise Server 21

6.3 Microsoft® Internet Information Services (IIS) 22

1. Preface

Scope:

This document describes the installation procedure, configuration, maintenance and troubleshooting of **NGSecureWeb©**.

Who should read this document:

This document was written to help system administrators task operating **NGSecureWeb©**.

It assumes you have read the **NGSecureWeb©** commercial documentation available from:

http://www.ngsec.com/ngproducts/ngsw/docs/NGSecureWeb-commercial.pdf

It also assumes that you have a basic understanding and working knowledge of the following:

- System and network security
- System and network administration
- UNIX or Windows operating systems
- Internet protocols

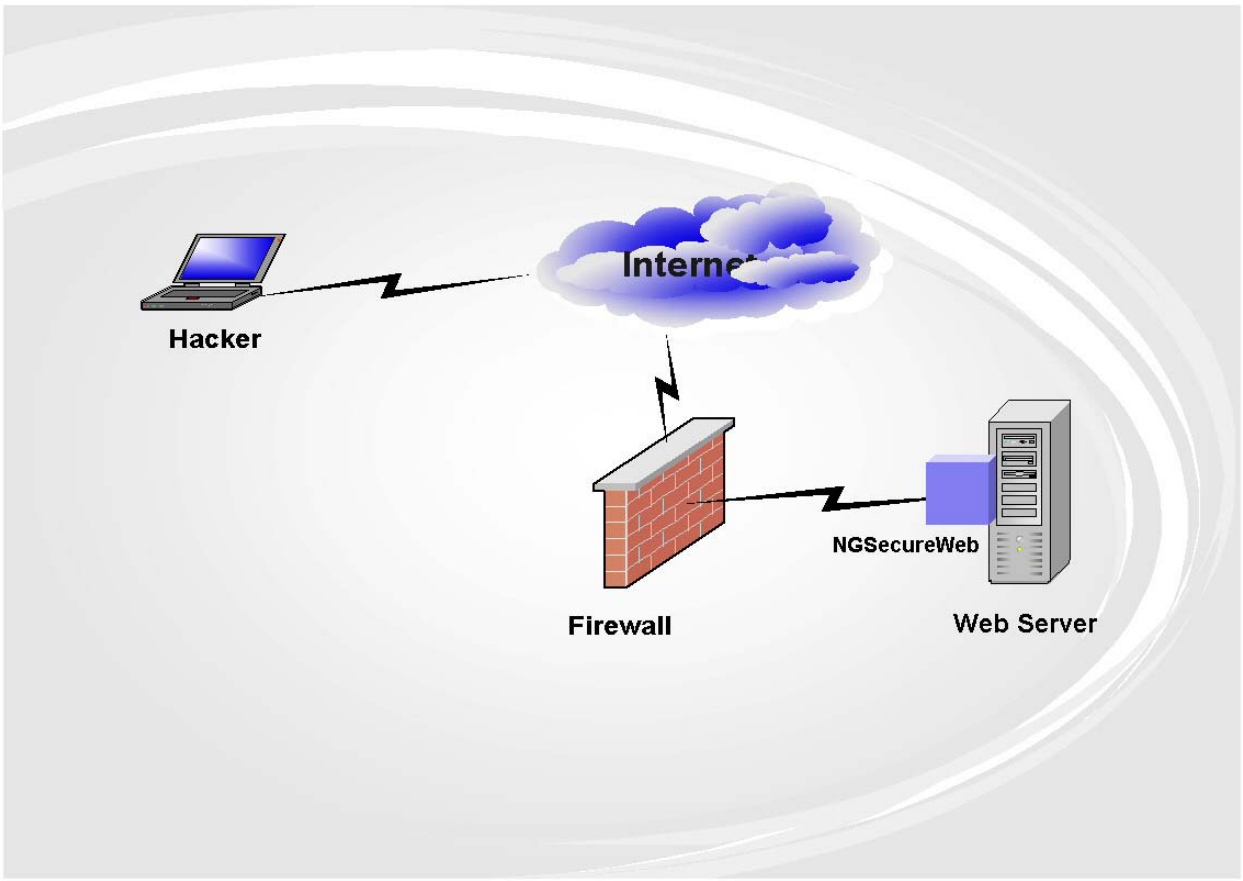
Please make sure you always have the latest version of this document by checking at:

http://www.ngsec.com/ngproducts/ngsw/docs/NGSecureWeb-technical.pdf

2. Introduction

NGSecureWeb® is the result of the fusion of two security technologies: Firewalls and IDSs, (Intrusion Detection Systems).

NGSecureWeb® filters all traffic from clients to the HTTP-server, looking for well-known attacks to web-servers and to its third party applications. When **NGSecureWeb®** detects a possible attack (acting as an **Application IDS**), it will refuse to forward it to the web server (acting as an **Application Firewall**).



NGSecureWeb® will protect your system from attacks that your firewall has already accepted. For example, your Web Server could be vulnerable to a buffer overflow (htr overflow in Microsoft IIS), your firewall will accept the connection to the Web Server, but NGSecureWeb® will detect the attempt of exploitation, deny and log the request.

NGSecureWeb® will protect your system from both **known and unknown vulnerabilities**, since its IDS engine has been designed to look for patterns of well-known attacks. **Future security flaws** in this web-server and its applications **will not be exploitable**.

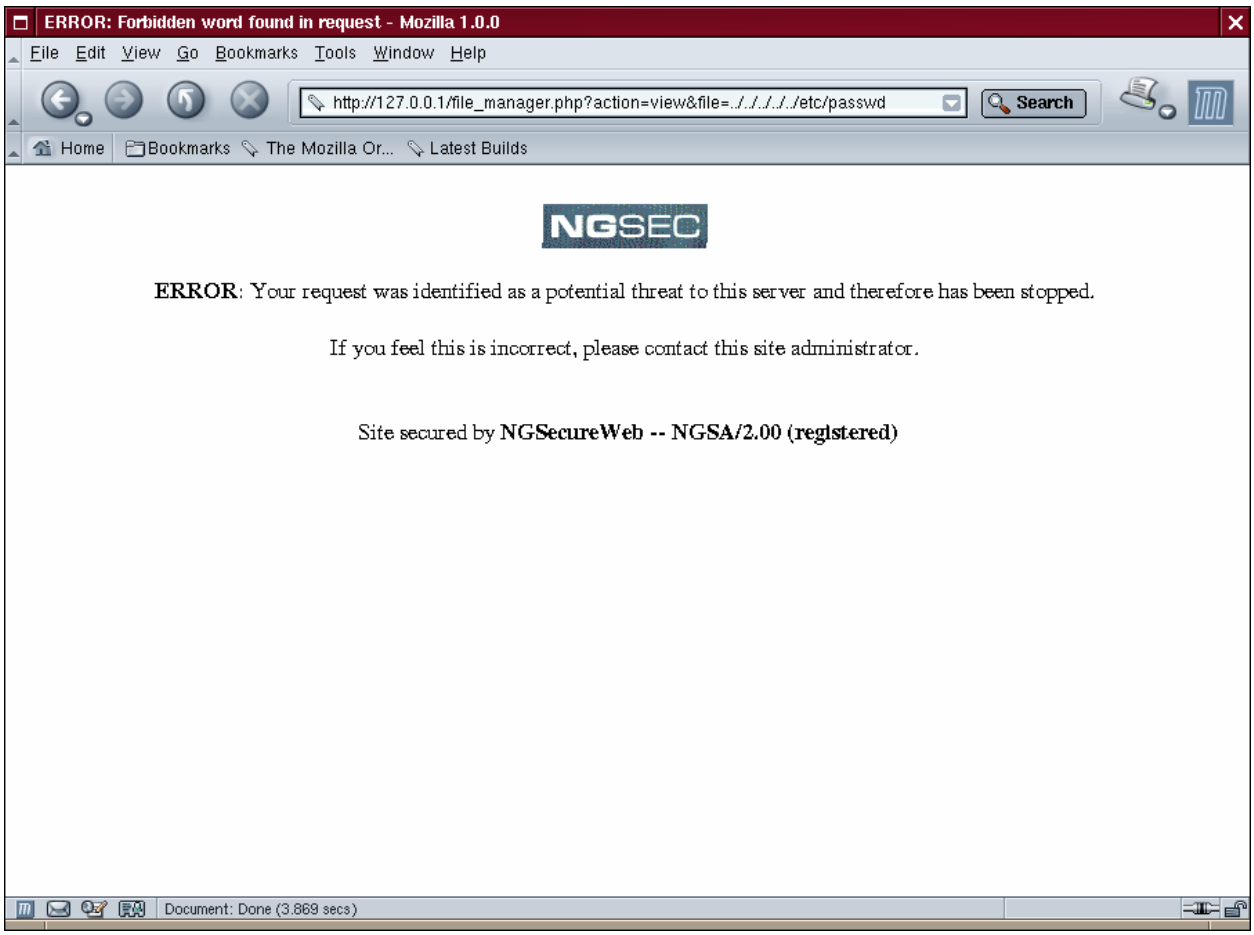
Currently, **NGSecureWeb® IDS engine** checks for the following attack patterns:

- **Directory traversal attacks:** During the past few years many CGI applications have suffered this kind of vulnerabilities, especially the ones involved in file managing. NGSecureWeb® Firewall engine will protect both for known and unknown vulnerabilities.
- **Forbidden Words:** NGSecureWeb® will search the entire request for forbidden words (defined by the Administrator). For example, it is not common to find the word "/bin/sh" in an HTTP request. NGSecureWeb® IDS engine detects these words and NGSecureWeb® Firewall engine blocks the request to the web-server.
- **Shellcode:** NGSecureWeb® IDS engine uses the newest techniques in shellcode recognition (even polymorphic ones).
- **Long Headers (buffer overflows):** NGSecureWeb® IDS engine will check the length of all HTTP headers looking for unusual values.
- **Long GET (buffer overflows):** NGSecureWeb® IDS engine will check the length of the GET arguments looking for unusual high values. These high values could be due of buffer overflow exploitation.
- **Long POST (buffer overflows):** NGSecureWeb® IDS engine will check the length of the URL arguments looking for unusual high values. These high values could be due of buffer overflow exploitation.
- **Long URL (buffer overflows):** NGSecureWeb® IDS engine will check the length of the URL looking for unusual high values. These high values could be due of buffer overflow exploitation.
- **Non printable characters**: NGSecureWeb® will filter every request looking for non-printable characters. This request could be an attempt of buffer overflow exploitation.
- **Method filtering:** NGSecureWeb® will filter and stop every request with a forbidden method. Common allowed methods are GET, HEAD and POST.

Currently **NGSecureWeb®** is available for:

- **Microsoft® Internet Information Services (IIS)**
- **Apache® HTTP Server**
- **Iplanet® / Netscape® Enterprise Server®**

Whenever NGSecureWeb® identifies, denies and logs a potential threat in a request, **the client will receive the following web page**:

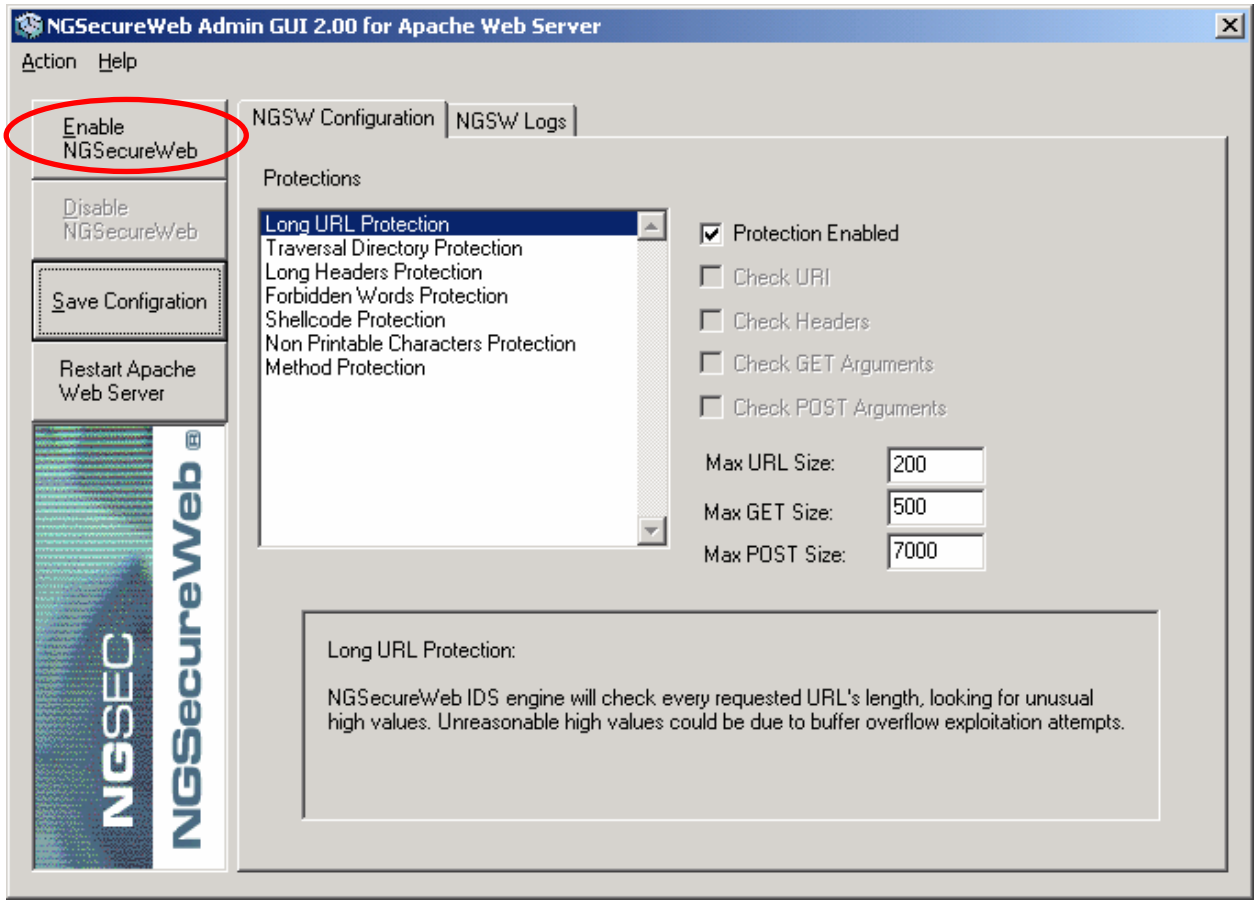


3. Installation procedure

Installation procedure differs between Windows and UNIX, so we will cover both separately.

3.1 Windows installation

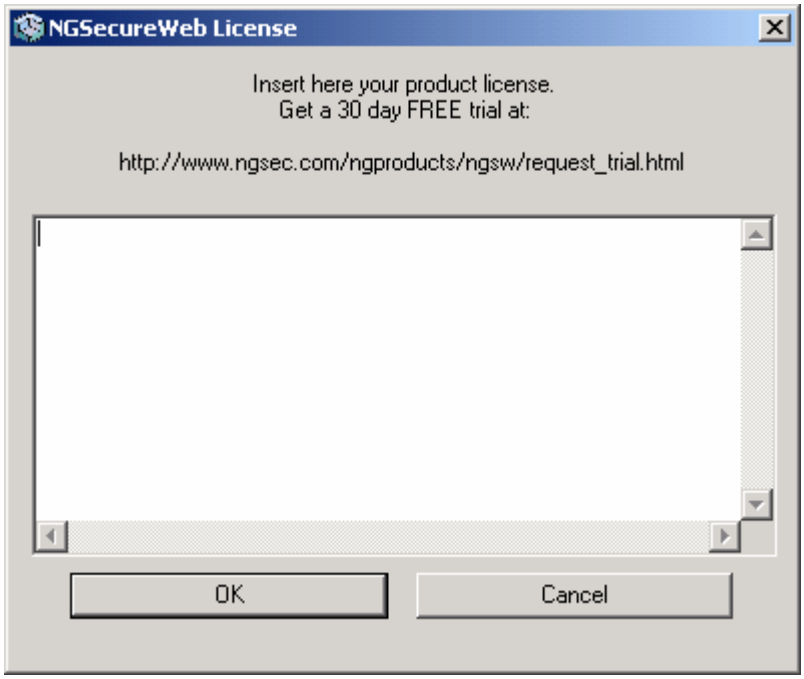
Windows installation is very straightforward. Once you have installed it, you will need to **run at least once the GUI and click the "Enable" button in order to properly activate NGSecureWeb®**.



Upon NGSecureWeb® GUI start, the program will check for a valid a license. If it fails to verify it's existence, it will pop up a window requesting for it.

Should you want to test the software, please obtain a 30-day FREE trial license from:

http://www.ngsec.com/ngproducts/ngsw/request_trial.html



Once you have obtained a valid license, NGSecureWeb® will activate normally. Should you want to make sure that everything is correct, please review NGSecureWeb® logs upon Web Server starting. If there is no complain about the license, everything is working properly.

Important: In order to have a successful uninstallation of NGSecureWeb®, you it must be first disabled by clicking the 'disable' button.

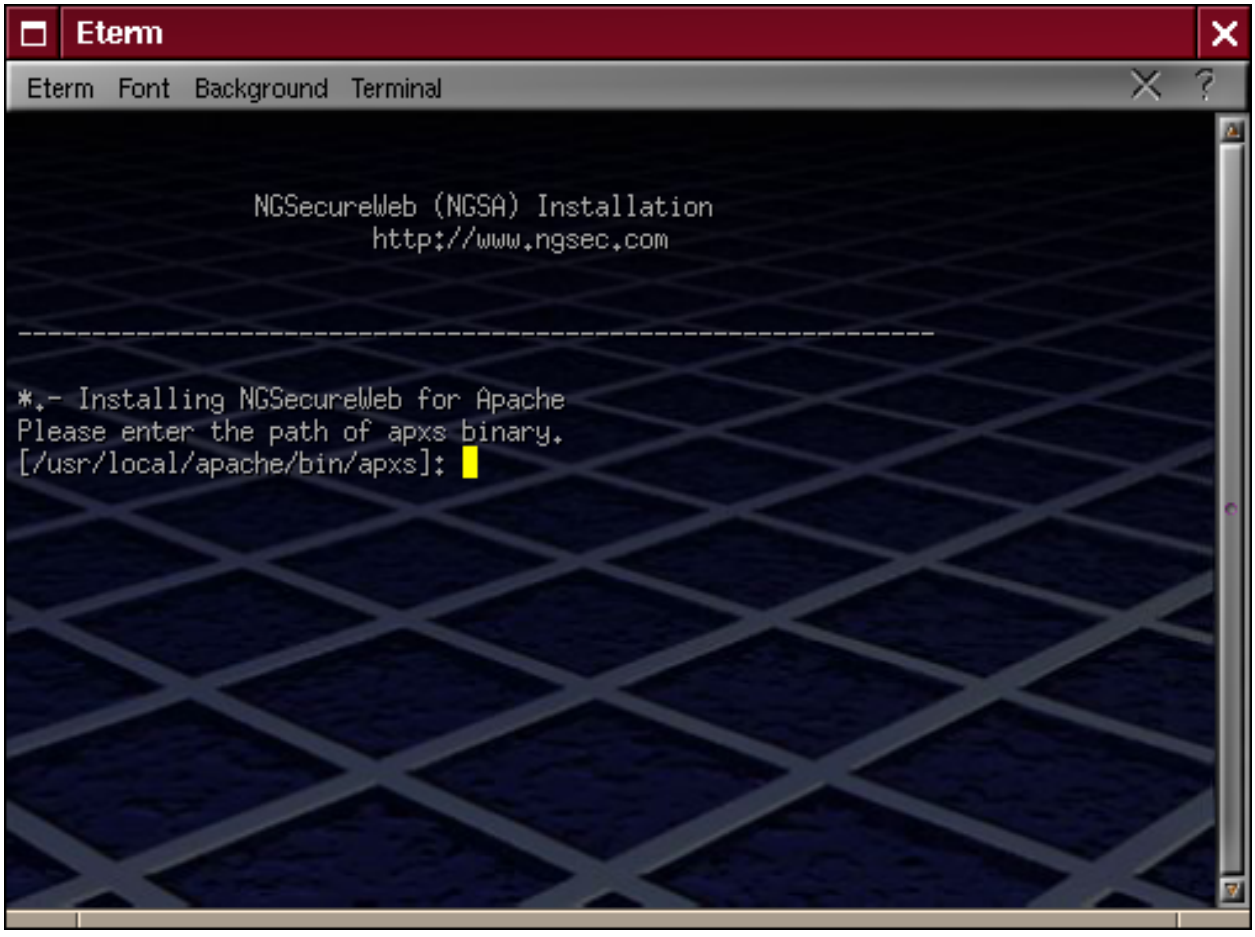
3.2 UNIX installation

Because most servers do not run X Windows, the UNIX installation is intentionally in text mode. However there is an Administration GUI for the X Windows, but the configuration can be accomplished in text mode too.

To begin the installation, please follow these simple steps:

- **gunzip mod_ngs<webserver>-<version>-<platform>.tgz**
- **tar –xvf mod_ngs<webserver>-<version>-<platform>.tar**
- **cd mod_ngs<webserver>-<version>-<platform>**
- **./setup**

On the first stage you will be prompted for a custom path of the Web Server.



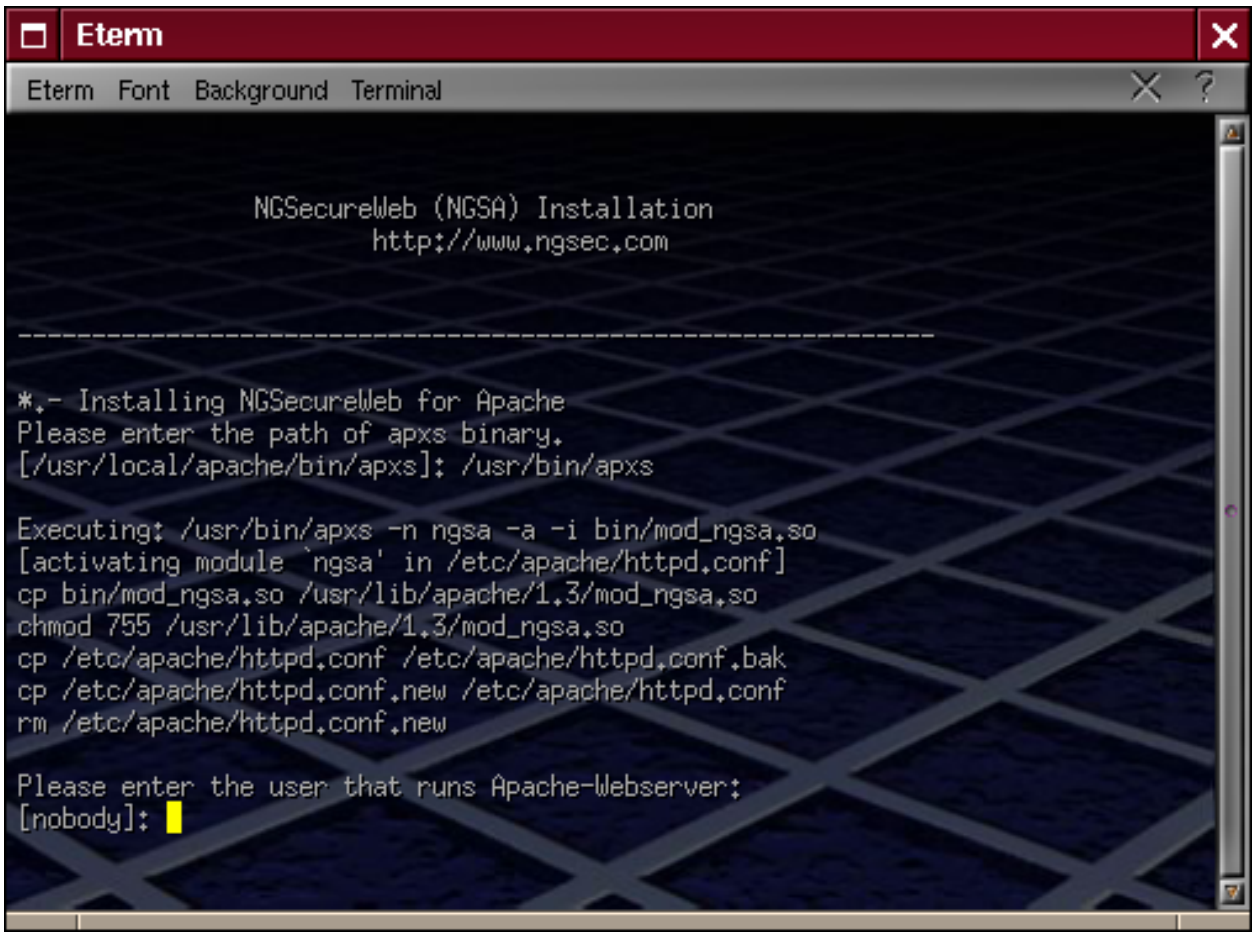
For instance, during the Apache® Web Server installation, you will be prompted for the path of the apxs binary. In order to find it, open another session and execute the following command as root:

 # find / -name apxs –print

This command will print the absolute path you must supply.

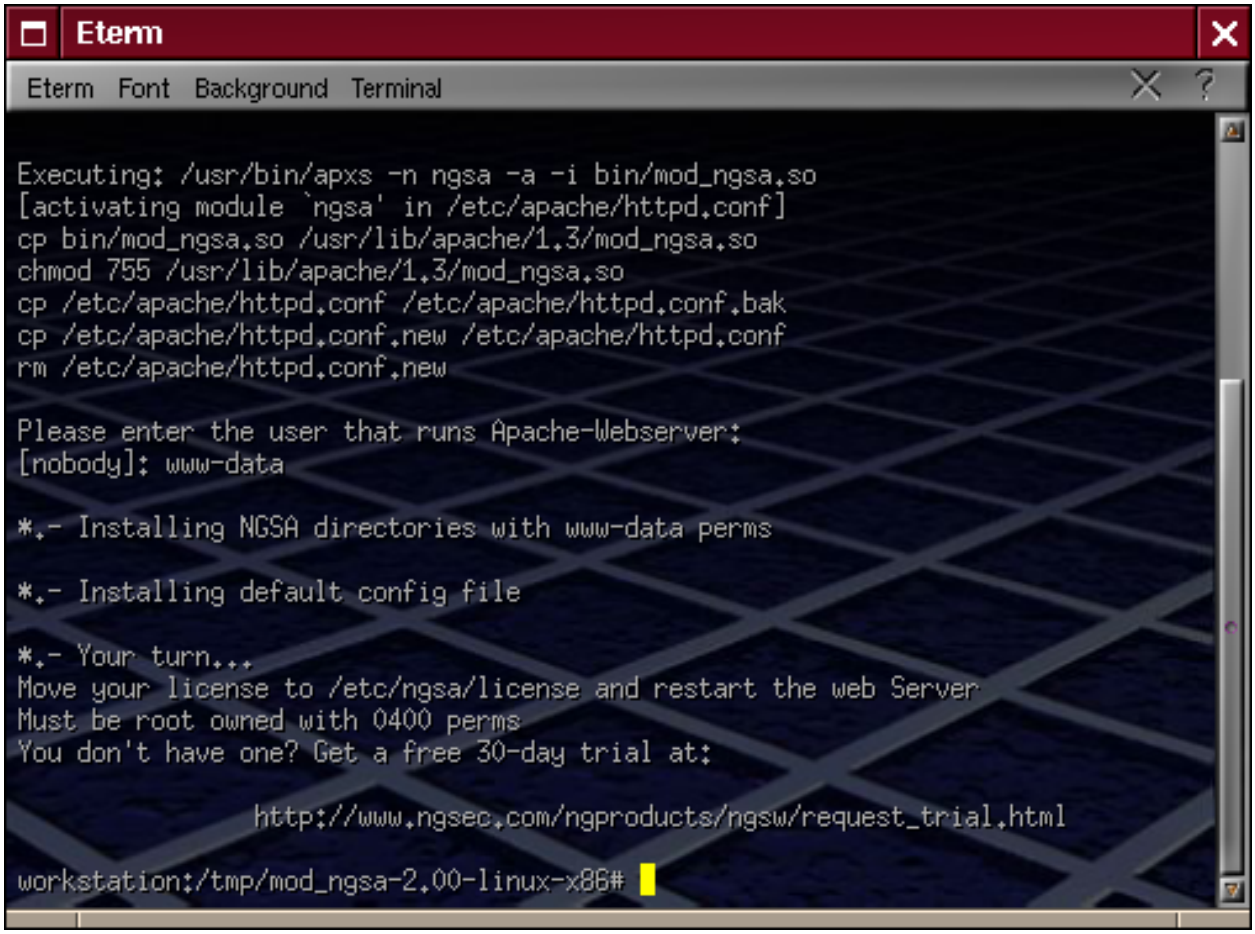
The next stage asks you for the user who runs the Web Server.

Most commonly, this user is: '**nobody**'.



Please refer to the documentation of your Web Server in order to verify that '**nobody**' is the user who runs your Web Server.

The final step is installing the binaries. The ngsw-admin (Adminsitration GUI) will be placed at **/usr/local/bin**. It does not require any extra library. As any other X Window program you can run it on a remote Xserver setting the DISPLAY to a correct value such as: **192.168.1.1:0**



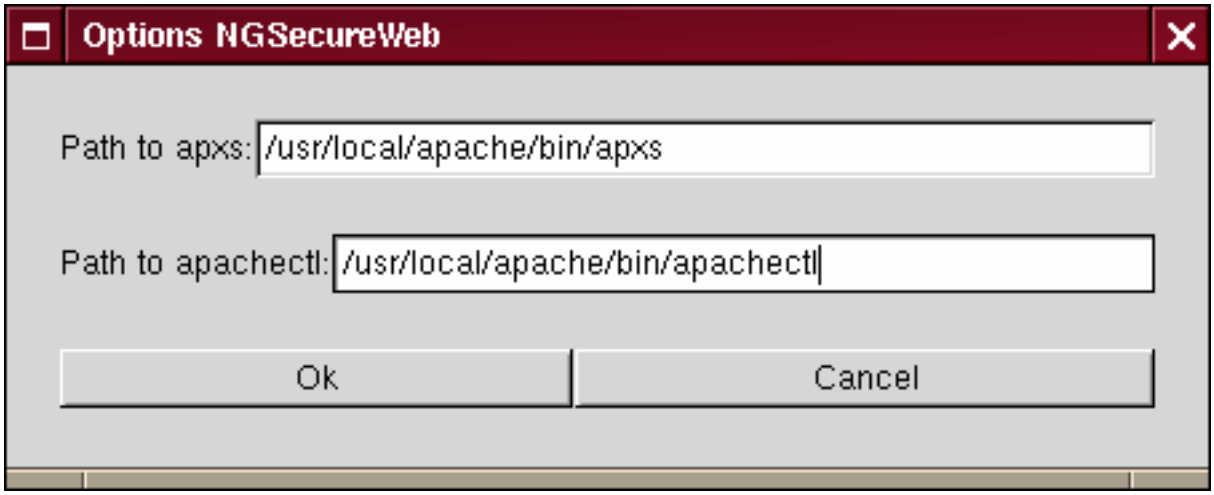
At this point **you have successfully installed NGSecureWeb®**.

Should you wish to continue using **text mode** the manual final steps are:

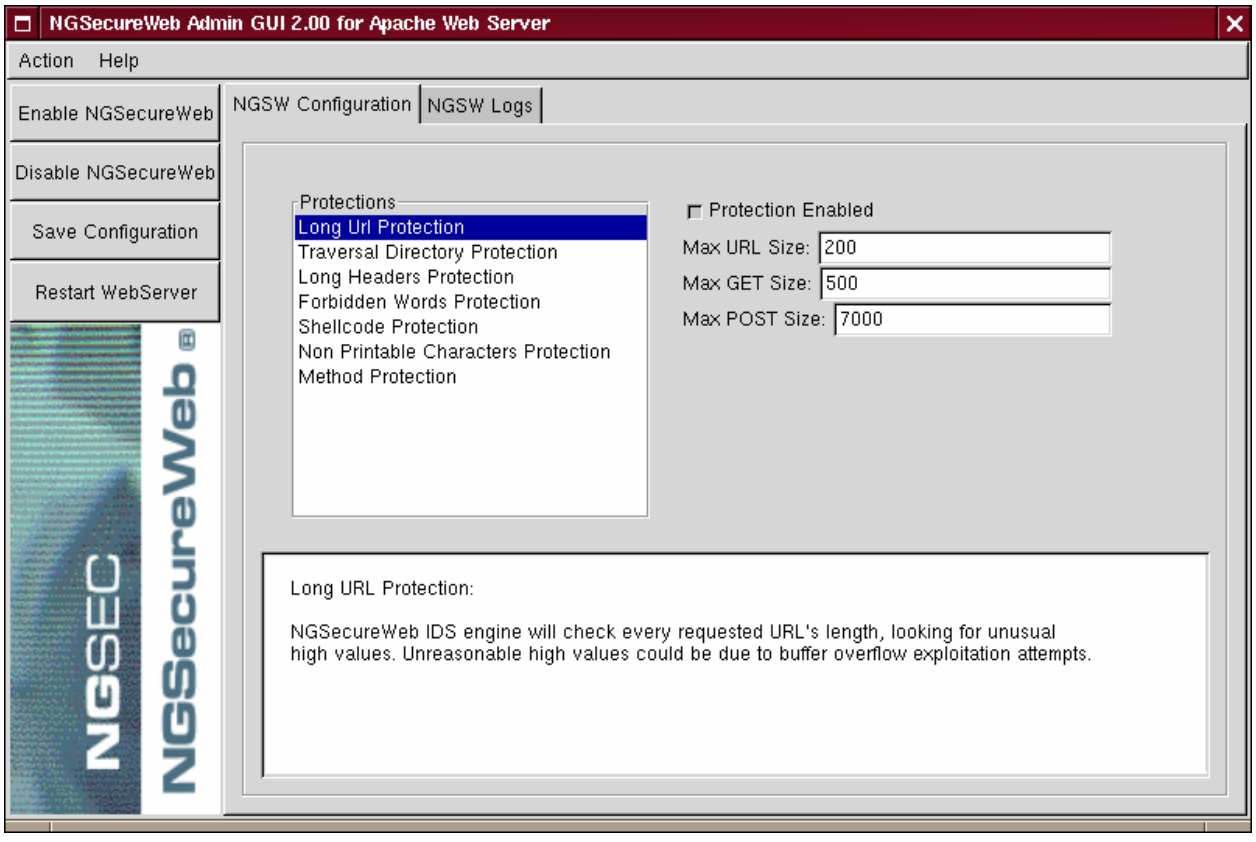
- Copy your license to **/etc/ngsa/license** or **/etc/ngsnes/license** depending on your Web Server's flavour.
- Check the config file **/etc/ngsa/ngsa.conf** or **/etc/ngsnes/ngsnes.conf** and configure with proper values (self explaining).
- Restart the Web Server.

If you wish to continue using a **user-friendly Administration GUI**, start the ngsw-admin located at **/usr/local/bin/ngsw-admin.**

Notice you will need to **configure the NGSecureWeb GUI** in the **menu Action -> Options.**
For instance: **NGSecureWeb®** for Apache® will have this options window.



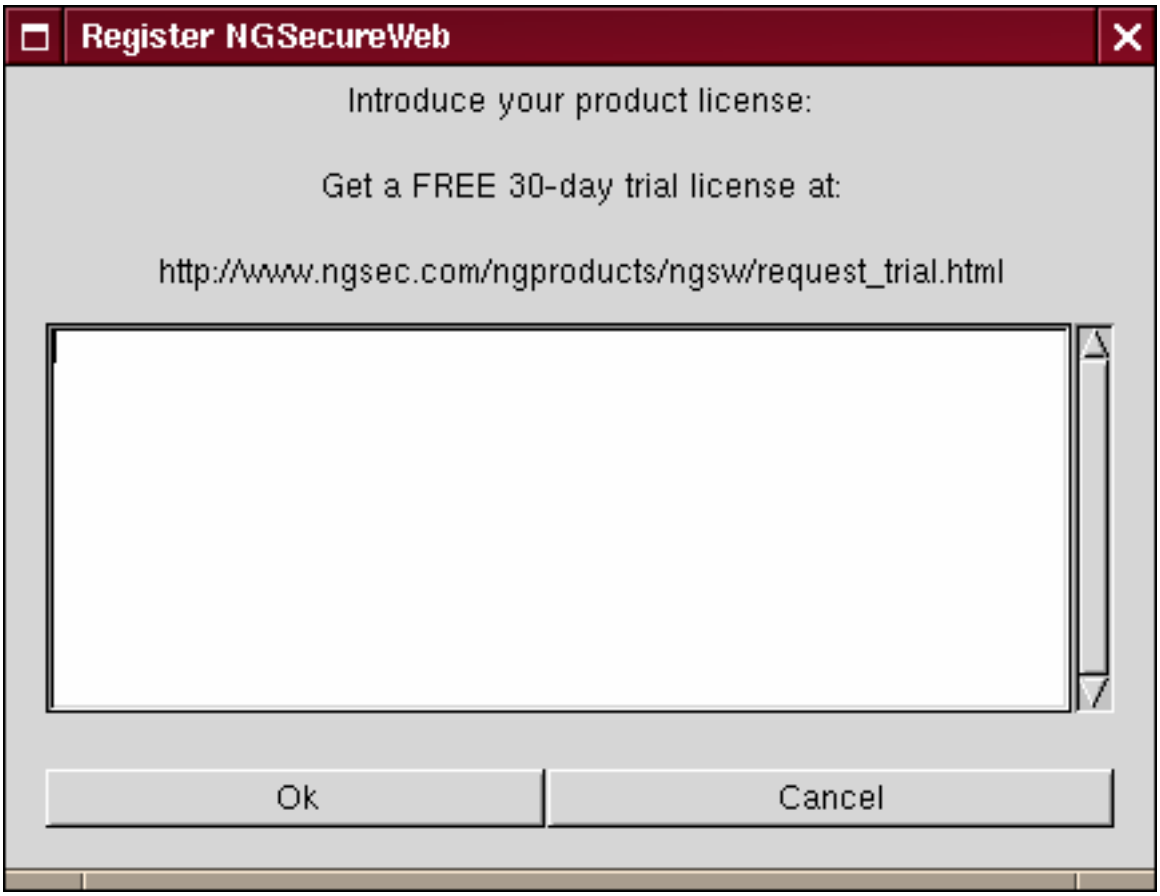
You will not have to configure this again because this values are saved at **$HOME/.ngswadminrc**



Upon NGSecureWeb® GUI start, the program will check for a valid a license. If it fails to verify it's existence, it will pop up a window requesting for it.

Should you want to test the software, please obtain a 30-day FREE trial license from:

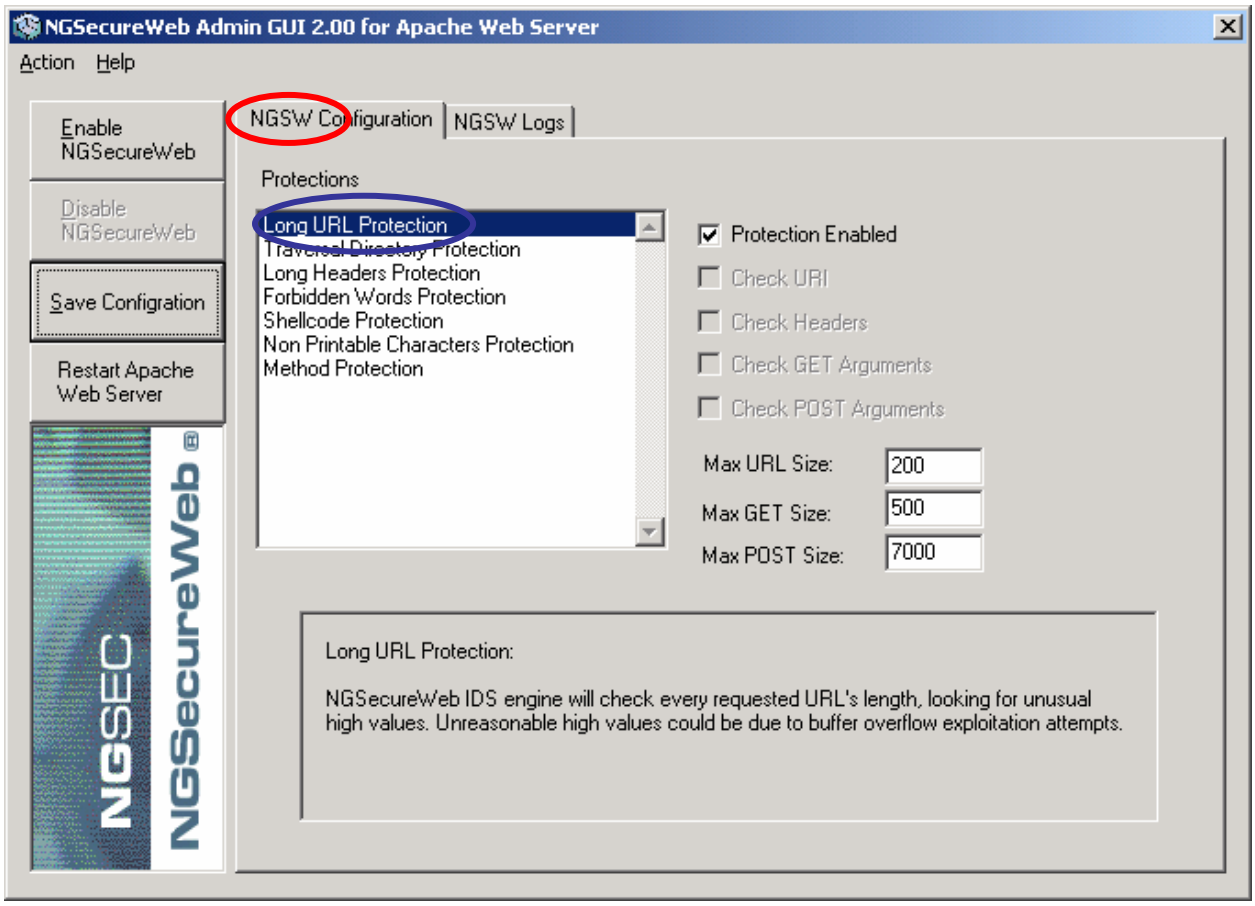
http://www.ngsec.com/ngproducts/ngsw/request_trial.html



Once you have obtained a valid license, NGSecureWeb® will activate normally. Should you want to make sure that everything is correct, please review NGSecureWeb® logs upon Web Server starting. If there is no complain about the license, everything is working properly.

4. Configuration

In order to configure NGSecureWeb® you will have to step into the "Configure" Tab. In it, you will find a List Box of available protections. Checking over each protection, you will see its own configuration options.



Each protection has one common option: '**Protection enabled**'. Once enabled, **NGSecureWeb®** will use this protection method while filtering the incoming HTTP requests.

In order to activate the changes on **NGSecureWeb®**, you will have to "**Save Configuration**" and "**Restart the Web Server**".

A fairly normal HTTP request could be:

```
POST /index.php?variable1=abc HTTP/1.0
Host: www.ngsec.com
Content-Length: 13

variable2=123
```

NGSecureWeb® considers Method: POST
NGSecureWeb® considers URL: /index.php
NGSecureWeb® considers GET arguments: variable1=abc
NGSecureWeb® considers POST arguments: variable2=123
NGSecureWeb® considers Header Key: “Host” and “Content-Length”
NGSecureWeb® considers Header Value: “www.ngsec.com” and “13”

4.1 Long URL protection

This protection checks for unusual size values of the request (URL, GET arguments and POST arguments).

For example: if you set a value of 100 in the URL max size, under Microsoft® IIS the **htr overflow** would not be exploitable.

You have to be careful with the values you supply.
Please check **4.8 Configuration considerations** for more information on this subject.

4.2 Traversal Directory protection

This protection checks for directory traversal attacks on some fields of the HTTP request.

For example: if you configure this protection to check GET arguments, the **newsdesk.cgi directory traversal attack** could not be exploited.

4.3 Long Headers protection

This protection checks for unusual size values of the request (Header Key and Header value).

For example: if you set a value of 100 in the Header value, under Microsoft® IIS the **.printer overflow** would not be exploitable.

Once again, be careful with the values you supply. Please check **4.8 Configuration considerations** for more information in this subject.

4.4 Forbidden Words protection

This protection checks for forbidden words (as defined by the administrator), on some fields of the HTTP request.

Some words are not usual in a normal HTTP request but very common on an exploit attempt, such as "**cmd.exe**".

For example: if you configure this protection to check for the word "**cmd.exe**" you will stop most IIS worms that uses the **Unicode Bug** to propagate.

Once again, be careful with the values you supply. Please check **4.8 Configuration considerations** for more information on this subject.

4.5 Shellcode protection

This protection checks for shellcodes on some fields of the HTTP request.

Shellcodes are not usual in a normal HTTP request but very common on an exploit attempt.

For example: if you configure this protection to check for shellcodes you will stop most IIS worms that uses **htr overflow** to propagate.

Note: "**Nop number**" is the number of NOP-like characters before raising an alert. This value should not be changed from its defaults.

Once again, be careful with the values you supply. Please check **4.8 Configuration considerations** for more information on this subject.

4.6 Non Printable Characters protection

This protection checks for non printable characters on some fields of the HTTP request.

Non printable characters are not usual in a normal HTTP request but very common on an exploit attempt.

For example: if you configure this protection to check for non printable characters you will stop most IIS worms that uses **htr overflow** to propagate.

Note: Under some languages such us Rusian, Chinesse, etc… you should disable this protection, because HTTP requests on this languages will raise and stop false positives.

Once again, be careful with the values you supply. Please check **4.8 Configuration considerations** for more information on this subject.

4.7 Method protection

This protection checks the HTTP method, allowing only the ones you configure.

Note: At least you should have the **HEAD** and **GET** methods enabled, in order for the Web Server to properly function.

Once again, be careful with the values you supply. Please check **4.8 Configuration considerations** for more information on this subject.

4.8 Configuration considerations

NGSecureWeb® will not work properly unless some options of some protections have normal values:

- **Long URL protection**:
  - Max URL size value should not be lower than 100.
  - Max GET size value should not be lower than 200.
  - Max POST size value should not be lower than 1000.

- **Long Headers Protection**:
  - Max Key size value should not be lower than 100.
  - Max Value size should not be lower than 400.

- **Forbidden Wirds Protection:**
  - Words should be as accurate as possible.
    A good word is "**/bin/sh**", and a bad word is "**sh**".

- **Shellcode Protection**:
  - Nop Number value should not be lower than 80.

- **Method Protection**:
  - At least the GET and HEAD methods should be allowed.

5. Maintenance

NGSecureWeb® does not require any kind of maintenance. However here are some tips that might be useful:

- **Keep track of the logs for NGSecureWeb Messages** such as license expiration, module deactivation, attacks…

- **Keep track of newer versions of NGSecureWeb®**. Maybe a newer version with newer capabilities will stop newer attacks.

- **Rotate the NGSecureWeb® logs** as often as they become big in size. Notice you do not even need to restart the Web Server.

6. FAQ's / Troubleshooting

6.1 Apache® HTTP Server

Here you will find the list of frequently asked questions and known issues related to **NGSecureWeb for Apache® HTTP Server**:

1. **Apache refuses to load the module:**
   This may be due to several causes:
   - Apache server has not been compiled with module "**so**" support.
     Solution: Recompile apache with: **./configure --enable-module=so ; make ; make install**.
   - Under some OSs (such as Solaris) Apache refuses to load a module unless it has been compiled with SHARED_CORE support.
     Solution: Recompile apache with: **./configure --enable-module=so --enable-rule=SHARED_CORE; make ; make install**.

2. **Apache loads the module but does not seem to work:**

   This may be due to several causes:

   - You don't have a license. Get one at:
     http://www.ngsec.com/ngproducts/ngsw/request_trial.html
   - Either your license has expired, nodename is incorrect, sysname is incorrect... Check NGSecureWeb logs (under UNIX **/etc/ngsa/ngsa.log**) for more information.

3. **Where does NGSecureWeb® for Apache log failures, attacks and blocked requests?**
   All errors go to NGSecureWeb® log file (under UNIX **/etc/ngsa/ngsa.log**).

4. **What happens when the 30 day trial is over? Will I have to restart Apache web server or uninstall NGSecureWeb®?**
   NGSecureWeb® will deactivate itself, and Apache web server will work normally. You won't even need to restart Apache.

5. **Does NGSecureWeb® works with mod_ssl? What is that message about -DEAPI?**
   Yes, NGSecureWeb® works fine with mod_ssl. Just ignore these warning messages when starting apache with ssl support.

6. **Does NGSecureWeb® works with Apache 2.0?**
   No, NGSecureWeb® does not currently work with Apache 2.0. We are working on this issue for future releases.

Please direct any further question or issue related to NGSA to: **ngsa@ngsec.com**

6.2 Iplanet / Netscape® Enterprise Server

Here you will find the list of frequently asked questions and known issues related to **NGSecureWeb® for Netscape® Enterprise Server**:

1. **Netscape® Enterprise Server loads the module but does not seem to work:**

   This may be due to several causes:

   - You don't have a license. Get one at: http://www.ngsec.com/ngproducts/ngsw/request_trial.html
   - Either your license has expired, nodename is incorrect, sysname is incorrect... Check NGSecureWeb® logs (under UNIX **/etc/ngsnes/ngsnes.log**) for more information.

2. **Where does NGSecureWeb® for Netscape® Enterprise Server log failures, attacks and blocked requests?**

   All errors go to NGSecureWeb® log file (under UNIX **/etc/ngsnes/ngsnes.log**).

3. **What happens when the 30 day trial is over? Will I have to restart Netscape® Enterprise Server or uninstall NGSecureWeb®?**

   NGSecureWeb® will deactivate itself, and Netscape® Enterprise Server will work normally.

   You won't even need to restart it.

Please direct any further question or issue related to NGSNES to: **ngsnes@ngsec.com**

6.3 Microsoft® Internet Information Services (IIS)

Here you will find the list of frequently asked questions and known issues related to **NGSecureWeb® for Microsoft® Internet Information Services (IIS)**:

1. **Microsoft® Internet Information Services loads the module but does not seem to work:**

   This may be due to several causes:

   - You don't have a license. Get one at: http://www.ngsec.com/ngproducts/ngsw/request_trial.html
   - Either your license has expired, nodename is incorrect, sysname is incorrect... Check NGSecureWeb® logs for more information.

2. **What happens when the 30 day trial is over? Will I have to restart Microsoft® Internet Information Services or uninstall NGSecureWeb®?**

   NGSecureWeb® will deactivate itself, and Microsoft® IIS will work normally.

   You won't even need to restart it.

Please direct any further question or issue related to NGSIIS to: **ngsiis@ngsec.com**

Microsoft, Microsoft Windows, Internet Information Services, Netscape, Netscape Enterprise Server, Iplanet, Solaris, and Sun are trademarks, registered trademarks, or service marks of third party corporations, in the United States and other countries.
© Copyright NGSEC [Next Generation Security Technologies], 2002. All rights reserved.