Security Considerations for the iPlanet Enterprise Web Server on Solaris

Edmundo Farinas

February 03, 2002

Abstract

When installing or configuring a software product, it is common to find isolated sources of information for securing such software. For the iPlanet Web Server there's not a single place where to find a set of measures that need to be taken into account to have a secured service before opening it to the public.

A set of recommended actions have been compiled and explained in this document, presented as a guide covering the most common areas where an iPlanet Web Server need to be hardened or carefully configured.

Assumptions

The following document assumes you'll secure an iPlanet Web Server (iWS) Enterprise Edition version 6.0 SP2 on a Sun SPARC server running Solaris version 2.6, 7 or 8 and that any of the configuration changes it suggest won't be performed directly over an operational system. It also assumes your computer have at least the recommended hardware configuration in order to run the iWS Enterprise Edition version 6.0 SP2. Check the web server release notes for more detail at http://docs.iplanet.com/docs/manuals/enterprise/60sp2/rn60sp2.html .

NOTE: Some of the changes suggested in this document could not suit your web site needs. Although some of the steps included here are also valid for previous versions of iWS (4.x and above) with minor modifications and most of them can be applied for the Standard Edition, tests have not been performed. Certain suggested changes can also be applied in previously installed non-secured iWS installations but further study will be needed before performing such actions. **No matter in which scenario you are, remember to perform and test a full backup of your system before making any change.**

Introduction

Every day new software products come to life with more and more features and due to the complexity involved in the software hardening process, it is very common to see default installations or configurations that could lead an organization to security breaches.

To ensure the "least privilege principle" any software need to be reduced to its minimal expression when installing or configuring its features. The iPlanet Web Server software is not an exception.

Performing the following recommended actions will help you prevent the most common security issues when installing or configuring the iPlanet Web Server software.

Locking down the underlying operating system

Securing an iPlanet Web Server is highly associated with the security of the operating system it is installed in top of (which is valid for most web servers and other services). This document needs to be used in conjunction with any guide for securing the operating system regardless the Solaris version your server has. Excellent guides can be found at the Sun Blueprints Program [1] or the Compass Security web site [2]

Having the latest security updates

From the security perspective, it is always recommended that you install the iWS version 6.0 from the original media but it may not include the latest security patches. In case your media has not the latest patches, obtain them directly and only from the iPlanet web site http://www.iplanet.com/downloads/patches/ . Those patches should be applied before you start configuring the web server software (and of course, after it has been completely installed) or you can incur in the risk of losing any previous configuration.

Choosing users, groups, ports and other parameters before installing

In order to keep your installation simple and add an additional level of security, it is very important to use a unique user and group created for web services purposes. The web server processes will run with these **userid** and **groupid** privileges and that's one the best ways to control its scope and to know what the web server will be capable of in case it gets compromised. You should prevent login access to such **userid** as a regular user so in order to perform common tasks on its behalf, the Unix `su` has to be used.

For every web server instance or virtual server (iWS Enterprise Server allows you to create multiple instances and/or virtual servers) you create, you may need to use a different **TCP port** to allow regular communication from the users' browsers. In this guide we'll use just one instance, but at least the same security considerations should be taken into account when creating additional instances.

iPlanet uses a separate web server for administering the iWS product, so an extra port should also be assigned to such server in order to function. Then, at least two ports are required, one for the "real" web server and another for the Administrative Server.

From the security point of view, choosing high TCP ports (greater than 1023) for both services, will help you hide certain internal details from the "external" users. This will also allow a non-root user to start/stop the servers (which could be a good approach for operator actions with minimal capabilities). One good practice is NOT to use the default suggested ports by the setup program at installation time, which is 8888 for the Administration Server and 80 for the user web server.

In case you follow this approach you will need to make-up you server to make it look like most of the common Internet accessible web server. Port Address Translation or PAT is one way to do it and this feature is usually available in most of the firewalls, routers and other current network devices. Then, your regular end user will access the server as if it were using the default HTTP or HTTPS port (TCP 80 or 433) but the service will be really running at any other port (the one you chose). Refer to your network equipment documentation for further details.

Installation Options

When installing the iWS software you'll need to run the `./setup` binary and it will prompt for the installation type you want to use. When prompted, choose "Typical" or "Custom" installation (both are identical) but never choose "Express". Express will assume most of the installation input required and that's not what we want to do.

The following options will be showed:

```
1. Server Core
2. Java Runtime Environment
3. Java Support
4. Search and Indexing Support
5. SNMP Support
```

The "Server Core" is the only needed but you have to select "Java Support" because it is required by the Administration Server in order to work properly. "Java Runtime Environment" (JRE) Support need to be selected unless you have a JRE previously installed.

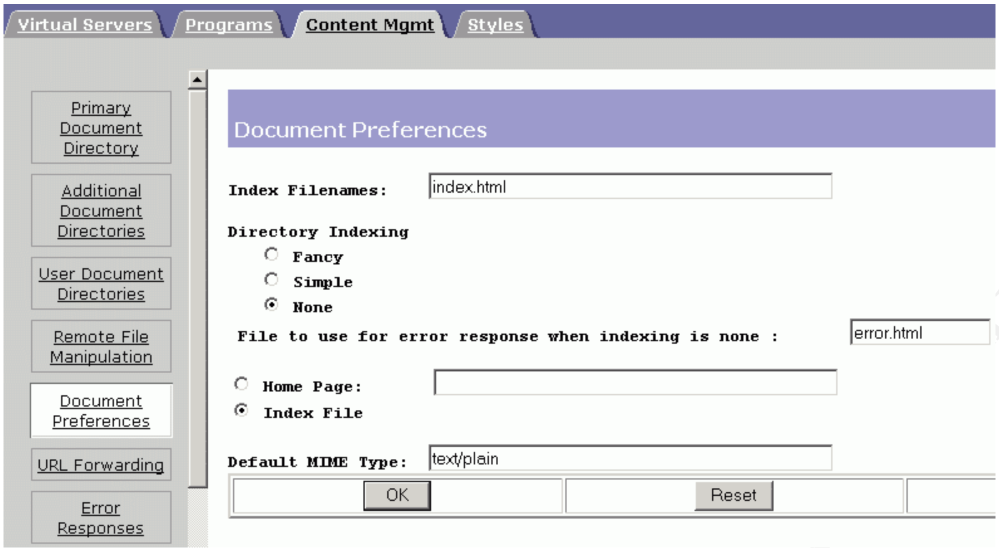
"Indexing Support" and "SNMP Support" are not needed unless you have a very specific requirement. Refer to the Administration Guide [3] for details.

Disable directory browsing and customize the response for such attempts

To prevent other people seeing your directory structure and obtaining additional information about your installation:

Go to the "Virtual Server Class" Tab -> Select the "DefaultClass" -> click the "Manage" button Then select the "Content Management" and click "Document Preferences"

Leave just `index.html` as the Index Filename, select "None" for Directory Indexing and select a filename to response to directory browsing accesses. Remember to create such file where needed.



Index Filenames: index.html

Directory Indexing
○ Fancy
○ Simple
● None

File to use for error response when indexing is none : error.html

○ Home Page:
● Index File

Default MIME Type: text/plain

<u>NOTE</u>: This and all the other images have been taken from the iPlanet Administrative Web Server interface.

Customizing the web server logging properties

Some important HTTP variables are not logged by default at the access log file. Go to the main management page for you instance -> select “Log” TAB -> “Log Preferences”

Then select the “Record IP Addresses” radio button instead the default “Domain Names”. Also select “Log only” radio button and select the `HTTP header, "referer"` and the `HTTP header, "user-agent"` checkboxes. Select the “OK” button to apply the changes.

<u>NOTE</u>: Be careful about using two different log formats on the same log file. If required, rotate the logs and stop the web server before performing this procedure.

Enabling Log Rotation

iWS comes with a cron-like control service called ns-cron, which allows the administrator to automate common repetitive tasks for server maintenance. The activation/deactivation of such service can be controlled via the iWS administrative interface.

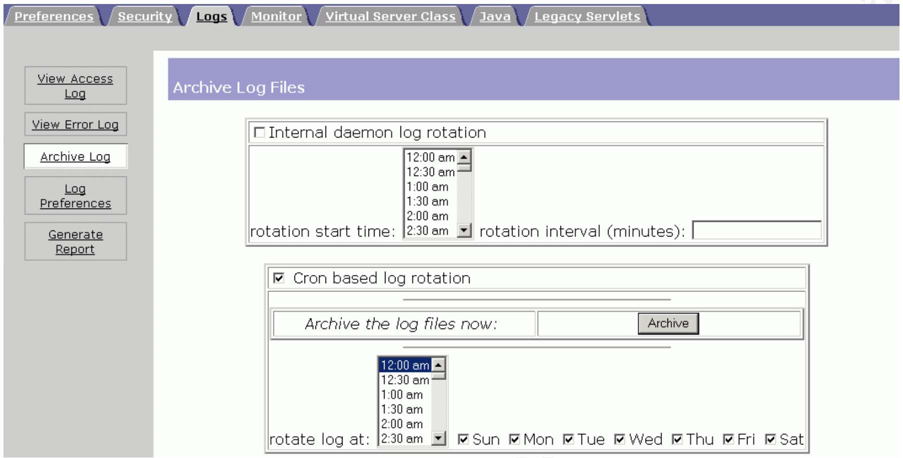
Common tasks could include verification script with triggered action based on specific log patterns (sometimes used by basic Host Intrusion Detection Systems), access file or error file log rotation, etc.

A good log rotation policy will depend on your specific site needs but an excellent one I’ve been working for a while is to cut the log files and “archive” the old ones when your web server is in a valley (opposite of peak) time. This will give you the advantage of performing compression and maybe certain additional basic log processing at a low load time.

The `rotate` script included with the product is an excellent one, including good time stamping features but if it doesn't fit your needs you might want to create your own one (for example, if you or your installation cannot accept the web server to be restarted by the `rotate` script when invoked)

Unfortunately, time based process scheduling does not allow you to cut access or error log files based on its size, so rotate (and compress) them as often as needed to make them manageable is size. If the default log file rotation schema and script fit your needs, just:

Select the "Log" tab -> select the checkbox "Cron based log rotation" -> Click the "OK" button and restart the cron server (actually start it if this is a new installation because ns-cron daemon is NOT running by default).



Archive Log Files

☐ Internal daemon log rotation

rotation start time: 12:00 am / 12:30 am / 1:00 am / 1:30 am / 2:00 am / 2:30 am rotation interval (minutes):

☑ Cron based log rotation

Archive the log files now: Archive

rotate log at: 12:00 am / 12:30 am / 1:00 am / 1:30 am / 2:00 am / 2:30 am ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Removing of default files and document directory mappings

Certain files are placed in the DocumentRoot directory and few directories are mapped as additional document directories after the creation of a new instance. Allowing people to have access to default files may guide an intruder to know more about your system or to easily obtain access to areas non directly visible from the operating system (when performing a directory listing on the web content directories, for example)

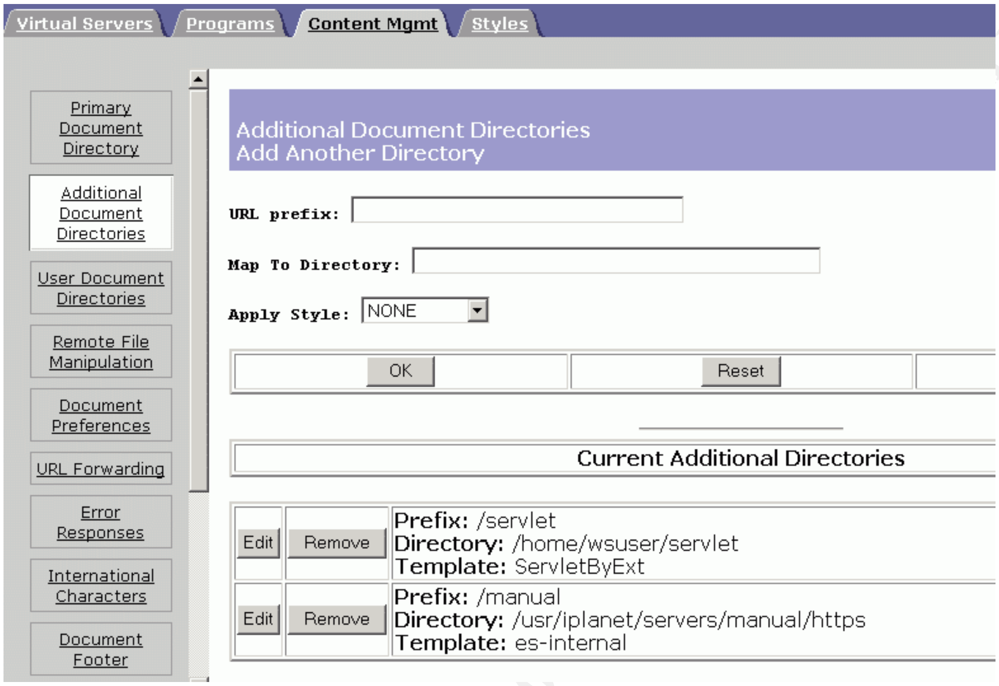
Always remove the following files in the DocumentRoot directory of your new instance, that are copied when the instance is created:

```
index.html
banner.html
launch.html
```

Also, by default the iWS product manual is mapped to the `/manual` and there's a default `/servlet` directory both mapped as "Additional Document Directories" on your recently created instance. You should disable such association:

Select the “Virtual Server Class” Tab of your instance -> Select Class “DefaultClass” and click on the “Manage” button

Go to the “ Content Management” Tab -> Click on the “Additional Document Directories” link and remove the `/servlet` and `/manual` additional document directories by clicking on the “remove” button at the left side of such entries.



Prefix: /servlet
Directory: /home/wsuser/servlet
Template: ServletByExt

Prefix: /manual
Directory: /usr/iplanet/servers/manual/https
Template: es-internal

Configuring minimal file permission

It is also important to assign the minimal privileges to the files the web server will interact with (regular HTML pages, images and other). The web server associated user/group will only require read permissions for the configuration files and write permissions for the log file directory. That user account should has NOT write permission for the configuration files.

The `admpw` file at the administration web instance’s configuration directory, keep the password for the administrative user and although the password cannot be easily modified, it can be cleared, leaving your web server wide open to possible intruders.

By default this file is world readable. Change its permissions to root only with the `chmod` Unix command at the administrative server configuration directory, as shown:

```
# chmod 600 admpw
```

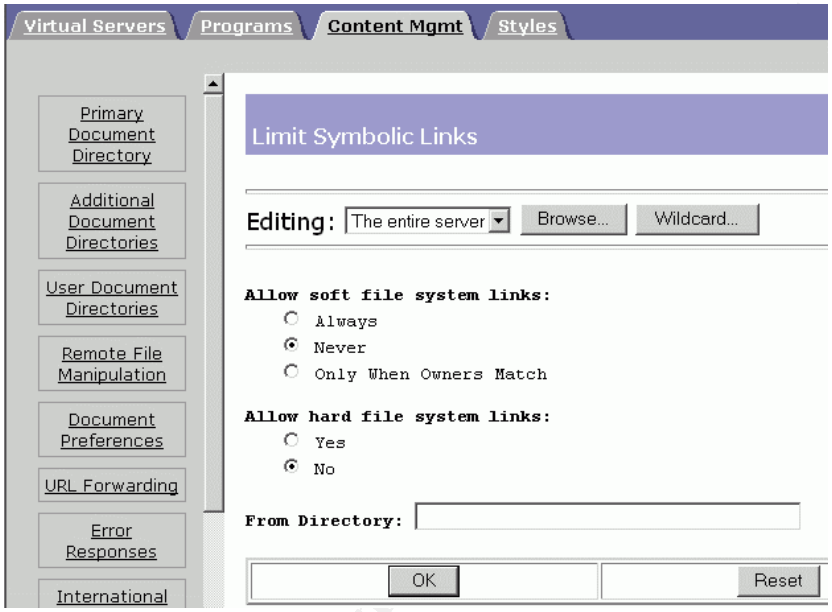
A Host Based Intrusion Detection System (HIDS) could be used to control non-authorized modifications to this file or changes to the regular web server content.

Restricting Symbolic and Hard Links

Symbolic or hard links could unadvertedly grant access to non-public areas of your web server when "linking" to files or directories outside the DocumentRoot directory in your operating system.

To prevent your web server following encountered links when serving user requests, at the main management page for you instance:

Go to the "Virtual Server Class" Tab -> Select the "DefaultClass" -> click the "Manage" button Select the "Content Management" -> Click the "Symbolic Links" link then select the "Never" radio button for soft links and "No" for hard links.



Limit Symbolic Links

Editing: The entire server

Allow soft file system links:

○ Always
● Never
○ Only When Owners Match

Allow hard file system links:

○ Yes
● No

From Directory:

Chroot your DocumentRoot directory

Unix *chroot* allows you to create a "fake" root directory to limit the directory access to a particular program or the web server itself so it think that such particular directory is the top of the directory hierarchy tree – the root directory.

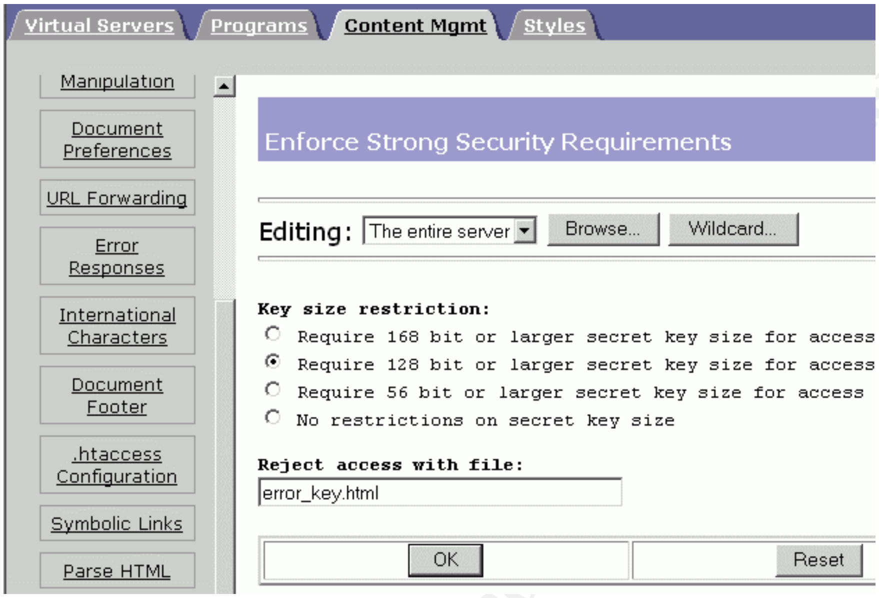
In order to specify the *chroot* directory for a virtual server class, perform the following steps at the Server Manager, select the Virtual Server Class Tab -> Click on the Virtual Server Tab -> Select the proper class in the "Tree View of the Server" section and enter the "fake" root directory at the "Chroot Directory" field. Click "OK" and apply the changes.

After making these changes, you will have to place the whole directory structure required by iWS under the *chrooted* root directory,

Setting Stronger Ciphers

In order to require at least 128 bit encryption keys when client SSL handshaking is performed, at the server instance administration interface:

Choose the “Content Mgmt” tab -> Select “Stronger Ciphers” -> Choose “edit” -> “Browse” -> Wildcard -> And the secret key size restriction of 128 bit or larger. Then enter the file location of the message that will be showed when access is rejected. Select “OK” and apply the changes. Restart the server if needed.



Enforce Strong Security Requirements

Editing: The entire server | Browse... | Wildcard...

Key size restriction:

○ Require 168 bit or larger secret key size for access
● Require 128 bit or larger secret key size for access
○ Require 56 bit or larger secret key size for access
○ No restrictions on secret key size

Reject access with file:

error_key.html

OK | Reset

Enabling Secured Connections

Browser to Web Server

In order to enable SSL to allow secured connection from the end users’ browsers, a “Trust Database” or key-pair file need to be created, and a password will be used to protect it. Choose a strong password.

To create the database, go to the “Server Manager” Tab -> “Security” Tab -> Create Database and enter the password twice, as requested.

After you create the “Trust Database” you might want to request a web server certificate from a well-known or private Certification Authority (it will depend on your needs). In order to receive a Digital Certificate, a public / private key pair will be stored in the “Trust Database” and a Certificate Request (also called Certificate Signature Request) will have to be generated.

After the “Trust Database” is created, automatically your server will prompt you for the database password every time you start your server.

You will need to change the “Trust Database” password as often as necessary in order to add additional protection to your installation [4]. Remember to ALWAYS change your password locally (from the web server itself) to avoid compromising it when it’s sent “clear” on the network.

To change the password, go to the “Server Manager” Tab -> “Security” Tab -> “Change Password”

Finally, to enable SSL at your server, edit the Listen Socket by going to the Server Manager, select the server instance -> select the “Security” tab -> Click on the “Preferences” tab -> click on the “Edit Listen Sockets” link -> Select “Edit” and turn security on for the connection group. Click “OK” to apply the changes and restart the server is needed

Web Server to LDAP database server

iWS allows user authentication via a LDAP database. If you're planning to have an external user database (an LDAP accessible database in other server), it's recommended to enable a secure connection between the web server and the LDAP database server.

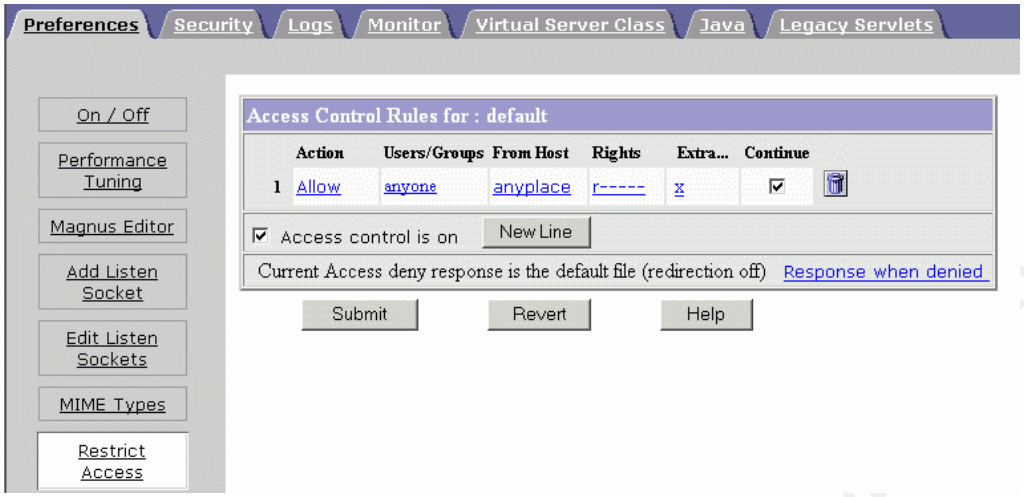
To do it, access the Administration Server -> choose the Global Settings tab -> Select “Configure Directory Service” option -> select “Yes”. Save the changes and click “OK” to change the current port to the standard port for LDAP over SSL (TCP 636). You can use any other port if desired or required.

Controlling access to your web server

The iPlanet Web Server allows granular control when defining who can access files or directories on your web site by creating a hierarchy of rules called *Access Control Entries* (ACEs).

iWS allows you to control (permit or restrict) access based on who’s making the request (user and/or group), where the requests come from (ip address or hostnames), when the request is happening (time of day, etc.) and what type of connection is being used (SSL for example). Based on all these parameters, permissions can be assigned (for example, read, execute or upload a file).

ACLs cannot be “generic” for all sites, they will depend on you needs but you can protect all your web site content by disabling all but the minimal permission needed for the proper functioning of your web server when retrieving content from its Primary DocumentRoot. Allow only “Read” access, which allows users to view files, via the HTTP methods GET, HEAD, POST, and INDEX. Unselect all the other options.



Access Control Rules for : default

	Action	Users/Groups	From Host	Rights	Extra...	Continue
1	Allow	anyone	anyplace	r-----	x	☑

☑ Access control is on

Current Access deny response is the default file (redirection off) Response when denied

Authentication options

Do NOT use "Basic Authentication" because it transfers the password in cleartext. With "Digest Authentication", the browser uses the MD5 algorithm to create a digest value based on the user's password and other information provided by the web server and the same value is calculated at the web server. Then, both values are compared and if they match, the user is successfully authenticated.

You can also apply certificate based client authentication, where the client only needs to present a valid certificate issued by a trusted CA, but this is a challenging approach. For intranet purposes, you can easily create an internal CA and issue certificates by using OpenSSL [5]

NOTE: Modifying the ACLCacheLifetime directive in the `magnus.conf` file can change the amount of time that the ACL user cache is kept at the web server.

Additional access control options

Depending on your needs, you may want to enable strong authentication at your web server by using RSA SecurID tokens [6] or any other mechanism. Refer to the iWS documentation and product for further information.

Protecting the Administrative Web Server instance

Keep it accessible only for few users and computers. Via proper ACLs you can control who can access iPlanet Web Administration Server [3].

Turn on encryption for this instance (enable SSL), in order to avoid people intercepting the communication and getting your administrator password. See "Enabling Secured Connections" in this document for further details).

Additional considerations

Restrict physical access to the server

In order to keep your web server as well as any other server secure, restricted physical access is a must. You should have your server in a secured physical location, including proper facilities (AC, UPS, key locked equipment racks, physical access control mechanisms, surveillance cameras, etc.).

Generating dynamic content via CGIs or JSPs

If you're planning to generate dynamic content at your web server via Java Server Pages (JSPs), use the JRE version suggested at the release notes or higher. Solaris VM Java version 1.2.2 is included with the iWS Enterprise Edition software.

Abstain from installing JDK or any other software that can transform source code into binary code of any other executable form. This type of software could help an intruder to upload source code, compile it and run it, making it easier the process of obtaining additional privileges or accessing private information.

When generating dynamic content via CGIs it is recommended that you:

Remember that vulnerable CGI programs are one of the most common security threats [7]; so only enable it if you have no other option [8].

chroot your CGI directory (to limit the scope of the CGIs to a directory different from the already *chrooted* DocumentRoot) so no one can obtain additional access in case a CGI allows unchecked user input or someone find a way to send command to the interpreter the CGIs are based on.

Enable a CGI directory (usually as an additional document directory called `/cgi-bin`) and keep the directory and file permission only to allow modification by the appropriate group of users. You should also associate a different username and group only for CGI execution purposes.

Do NOT enable CGI as a file type. Let's say you enable CGIs as file with `.cgi` extension, then any `.cgi` file will be treated as a real CGI program and will be executed regardless the place (directory) it's invoked and definitely you won't want any of your web, content or other "masters" users, updating your web content, and placing .cgi file that could be executed unadvertedly.

Configuring Cache Control Directives

If there's sensitive information that you want to protect from being cached by a HTTP 1.1 compliant proxy server, iWS has a way for controlling such behavior by using cache-control directives. For these directives to work, the proxy server must comply with HTTP 1.1 [11].

To set strict cache control directives:

Go to the "Content Management" tab -> "Cache Control Directives" and select "No Cache" or "No Store" and set the cache "Maximum Age" based on your needs.

Preventing Clients from Caching SSL Files

If necessary, you can prevent SSL files from being cached by a client by adding the following line inside the <HEAD> section of a file in HTML:

```
<meta http-equiv="pragma" content="no-cache">
```

This could adversely affect your web server performance of user experience but remember there's always a tradeoff between security and functionality.

You can also use this other two variables for controlling caching parameters globally (at the `magnus.conf` file): `SSLCacheEntries`, which specifies the number of SSL sessions that can be cached and `SSL3SessionTimeout`, which controls SSL3 and TLS session caching.

Do NOT enable Remote File Manipulation or Server-Parsed HTML features

By default, these features are not enabled and changing it could lead you to an insecure web server installation where potentially, any regular end user could perform unauthorized modifications or compromise your installation. A new security flaw related to these services has been recently posted [9].

Do NOT enable SNMP access

Unless you know exactly what you are doing do not use SNMP. Default SNMP Communities are another top security vulnerability [7]. This service could let others to obtain too much information about your web server configuration and status. If you need to enable it, remember that SNMP does not use encryption when transferring the data, so it can be captured in transit.

Perform a concept test of your security settings

With a regular web browser try to browse a directory, place a CGI program and try to execute it or try to obtain the manual page of your server and try to break any of the rules you have just imposed at your web server installation. If none of those attempts are successful, your will know how your web server installation will respond to similar attempts. Taking a look at the error log entries generated by these special cases could help you know what they mean if you encounter them later.

Also, if you have the budget, assess and keep track of your web server configuration using tools like the VigilEnt Agent from PentaSafe [10] that helps you automate the processes.

References

[1] Noordergraaf, Alex. "Solaris Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology". Sun BluePrints™ OnLine. November 2000
http://www.sun.com/blueprints/1100/minimize-updt1.pdf (February 02, 2002)

[2] Buetler, Ivan. Compass Security AG, "Hardening Solaris". March 08, 2001
http://www.csnc.ch/downloads/docs/hardening/SolarisHardening_CSNC.pdf (February 02, 2002)

[3] iPlanet Web Server. "Enterprise Edition 6.0 SP1 Administrator's Guide". August 14, 2001
http://docs.iplanet.com/docs/manuals/enterprise/60sp1/ag/contents.htm (February 02, 2002)

[4] Hayes, James M. " Guide to the Secure Configuration and Administration of iPlanet Web Server, Enterprise Edition 4.1". National Security Agency, security Recommendation Guides. July 3, 2001
http://nsa2.www.conxion.com/support/guides/sd-2.pdf (February 02, 2002)

[5] The OpenSSL Project
http://www.openssl.org/ (February 02, 2002)

[6] "RSA ACE/Agent for iPlanet", RSA Security
http://www.rsasecurity.com/products/securid/techspecs/iplanet.html (February 02, 2002)

[7] The SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities". November 15, 2001
http://www.sans.org/top20.htm (February 02, 2002)

[8] The CERT® Coordination Center. "Securing Public Web Servers". CERT® Security Improvement Modules. June 12, 2000
http://www.cert.org/security-improvement/practices/p078.html (February 02, 2002)

[9] Brain, Richard. "ProCheckUp Security Bulletin PR01-04". January 02, 2002
http://www.procheckup.com/vulnerabilities/pr0105.html (February 02, 2002)

[10] PentaSafe Security Technologies, Inc. . "PentaSafe VigilEnt Security Agent for Web Servers"

http://www.pentasafe.com/products/vsaweb.htm (February 02, 2002)

[11] Fielding, R. “The Hypertext Transfer Protocol--HTTP/1.1 Specification”, IETF Request For Comments. RFC 2068. January 1997
http://www.ietf.org/rfc/rfc2068.txt (February 02, 2002)