HTTPS Linux Apache

ÍNDICE

1. Introducción

Durante la instalación de Apache sobre Linux se crea un sitio virtual **HTTPS** por defecto, pero no está activo, así como tampoco está activo el módulo que permite su utilización ni está abierto su puerto de escucha.

2. Servidor virtual HTTPS por defecto

Para poder utilizar el servidor HTTPS de Apache, deberemos realizar las siguientes acciones:

1) Habilitar el módulo que permite la utilización de HTTPS: `a2enmod ssl`

```
root@debian:~# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and create sel
-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
root@debian:~#
```

2) Verificamos el puerto de escucha por defecto para HTTPS cuando el módulo ssl está activo:

```
  GNU nano 2.2.4            Fichero: /etc/apache2/ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz

NameVirtualHost *:80
Listen 80

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>
```

Observad que hasta que no se reinicia el servicio para aplicar los cambios, el puerto de escucha 443 no se abrirá (el comando para informar sobre qué puertos están abiertos es `netstat -ltn`).

```
tcp        0      0 0.0.0.0:38096           0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.101:53       0.0.0.0:*               LISTEN
tcp        0      0 172.26.25.100:53        0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:25                  :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
root@debian:~# service apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's fully quali
fied domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain name,
 using 127.0.1.1 for ServerName
.
root@debian:~# netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:38096           0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.101:53       0.0.0.0:*               LISTEN
tcp        0      0 172.26.25.100:53        0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:25                  :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
root@debian:~#
```

3) Editamos el fichero de configuración del sitio seguro por defecto para añadirle una página a cargar por defecto (`seguro.html`) que posteriormente deberemos crear:

```
  GNU nano 2.2.4    Fichero: /etc/apache2/sites-available/default-ssl

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                DirectoryIndex seguro.html
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
```

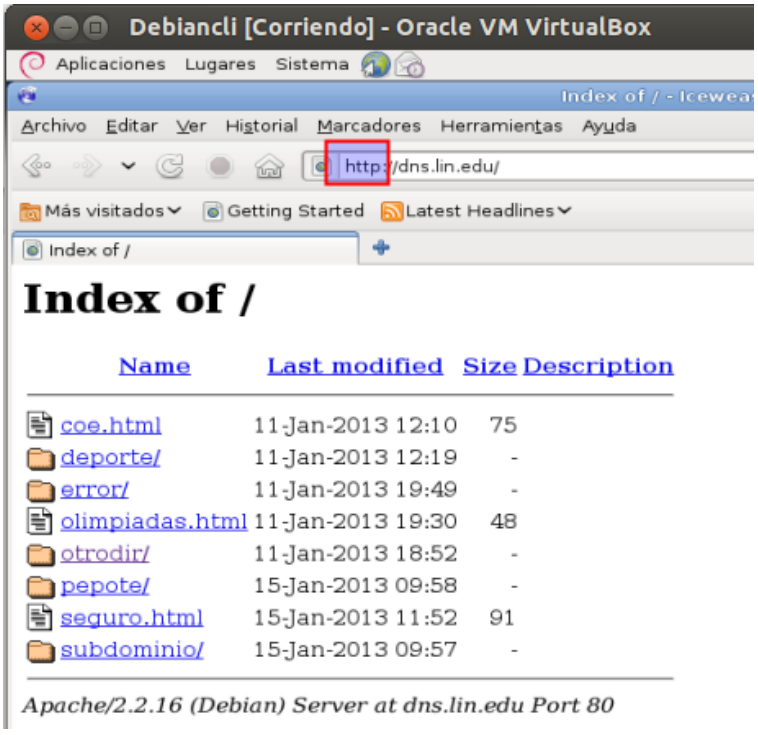
En el mismo fichero podemos observar la ruta y ficheros del certificado digital y su firma, ambos creados por defecto en la instalación de Apache.

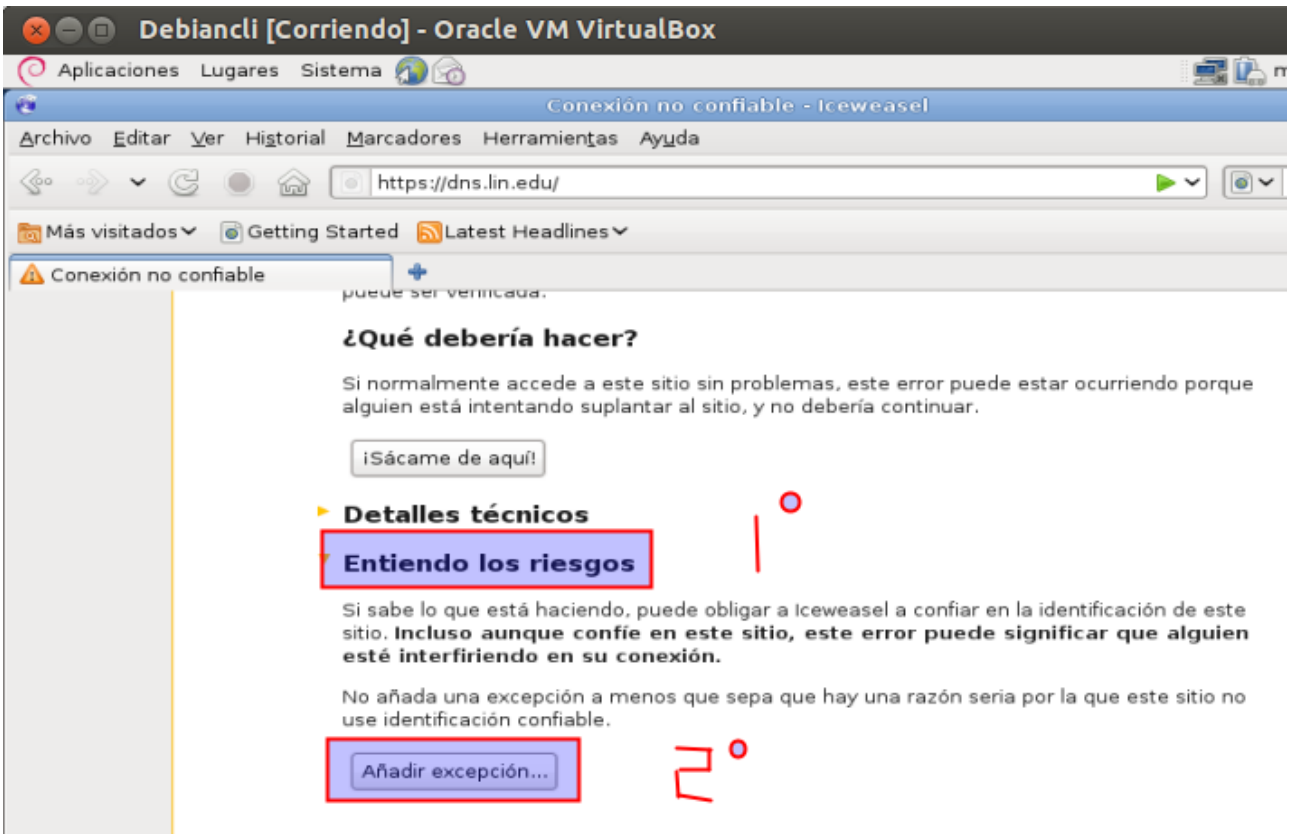
```
 GNU nano 2.2.4    Fichero: /etc/apache2/sites-available/default-ssl     Modifi

        #   A self-signed (snakeoil) certificate can be created by installing
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
        #   If both key and certificate are stored in the same file, only the
        #   SSLCertificateFile directive is needed.
        SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
        SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

4) Activamos ahora el sitio virtual HTTPS por defecto y reiniciamos el servicio:

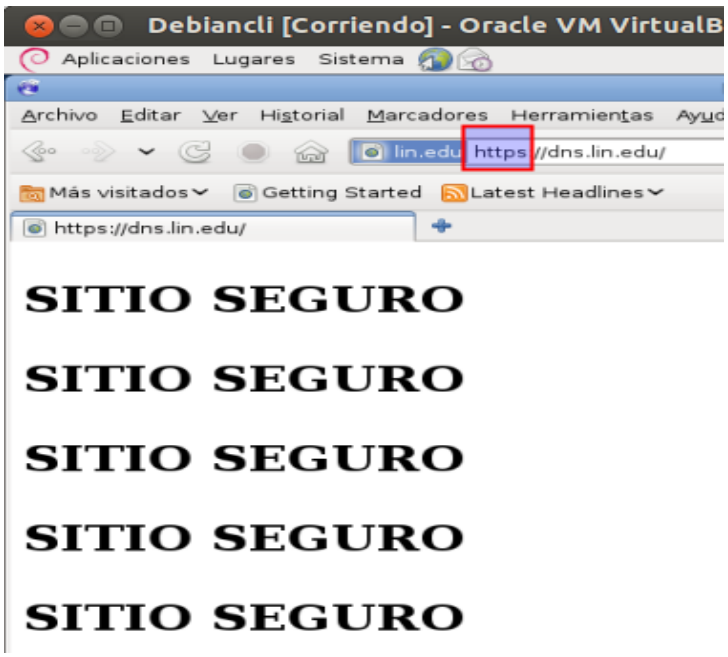
```
root@debian:~# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@debian:~# service apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's fully
 qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain
 name, using 127.0.1.1 for ServerName
.
root@debian:~#
```

5) Probamos su funcionamiento desde el cliente del sitio por defecto al utilizar HTTP y al utilizar HTTPS:




Debiancli [Corriendo] - Oracle VM VirtualBox
Aplicaciones Lugares Sistema
Conexión no confiable - Iceweasel
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
https://dns.lin.edu/
Más visitados Getting Started Latest Headlines
Conexión no confiable
¿Qué debería hacer?
Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.
¡Sácame de aquí!
Detalles técnicos
Entiendo los riesgos
1°
Si sabe lo que está haciendo, puede obligar a Iceweasel a confiar en la identificación de este sitio. Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.
No añada una excepción a menos que sepa que hay una razón seria por la que este sitio no use identificación confiable.
Añadir excepción...
2°


Añadir excepción de seguridad
Está a punto de alterar cómo identifica Iceweasel este sitio.
Los bancos, tiendas y otros sitios públicos legítimos no le pedirán hacer esto.
Servidor
Dirección: https://dns.lin.edu/
Obtener certificado
Estado del certificado
Este sitio intenta identificarse a sí mismo con información no válida.
Ver...
Sitio erróneo
El certificado pertenece a un sitio diferente, lo que podría indicar una suplantación de identidad.
Identidad desconocida
No se confía en el certificado, porque no ha sido verificado por una autoridad reconocida.
Guardar esta excepción de manera permanente
Confirmar excepción de seguridad
Cancelar



3. Un único servidor virtual HTTPS distinto al de defecto

Aparte del sitio virtual HTTPS por defecto podemos utilizar otros personalizados, en los que, lo adecuado sería tener una solicitud de certificado firmada por una entidad certificadora autorizada para poder utilizarlo sin problemas en Internet.

Se debe tener en cuenta que para que funcionen los sitios virtuales por HTTPS deberemos desactivar el sitio HTTPS por defecto anterior, ya que, por seguridad, son incompatibles en cuanto funcionamiento al utilizar el mismo puerto de escucha.

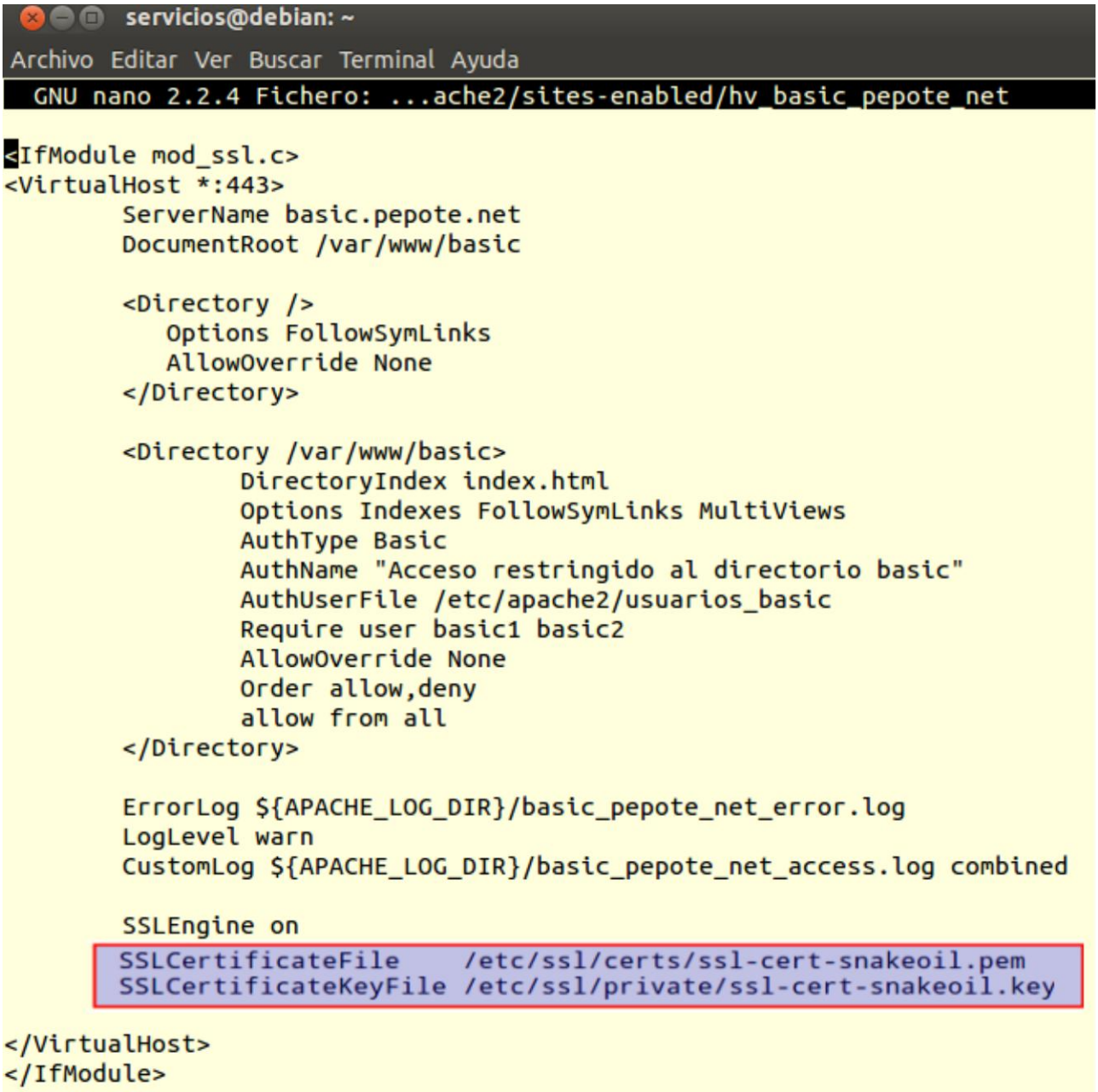
```
root@debian:/etc/apache2/sites-available# a2dissite default-ssl
Site default-ssl disabled.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@debian:/etc/apache2/sites-available# service apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's
fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1 for ServerName
.
root@debian:/etc/apache2/sites-available#
```

Nota. En nuestro caso utilizaremos los certificados de prueba incluidos en la instalación por defecto Apache.

Como ejemplo de un nuevo sitio seguro con acceso por HTTPS utilizaremos el del ejemplo anterior con autenticación `basic` para comprobar el funcionamiento conjunto de autenticación segura.

El sitio será accesible por el nombre de dominio `basic.pepote.net`, cargando la página por defecto `index.html`, con los ficheros de errores y accesos personalizados.

El contenido del fichero de configuración del sitio seguro por HTTPS añadido distinto al de defecto, tendrá como nombre `hv_basic_pepote_net` y su contenido será:



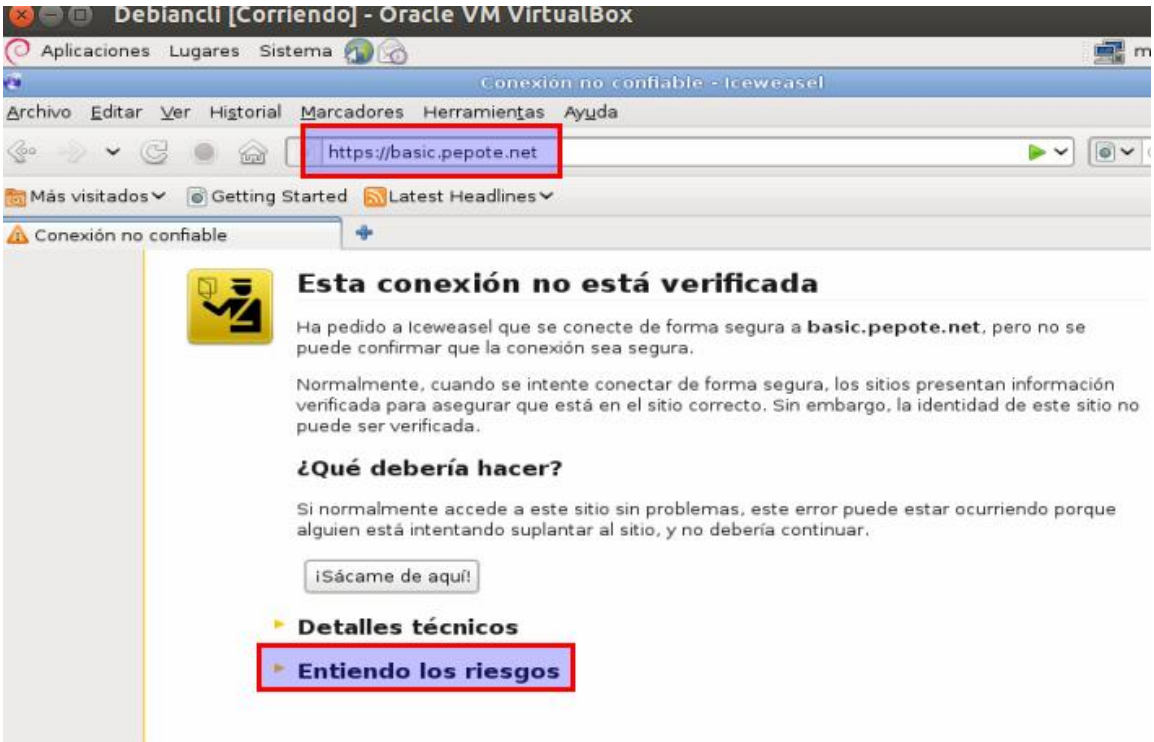
Activamos el nuevo sitio seguro y reiniciamos el servicio:

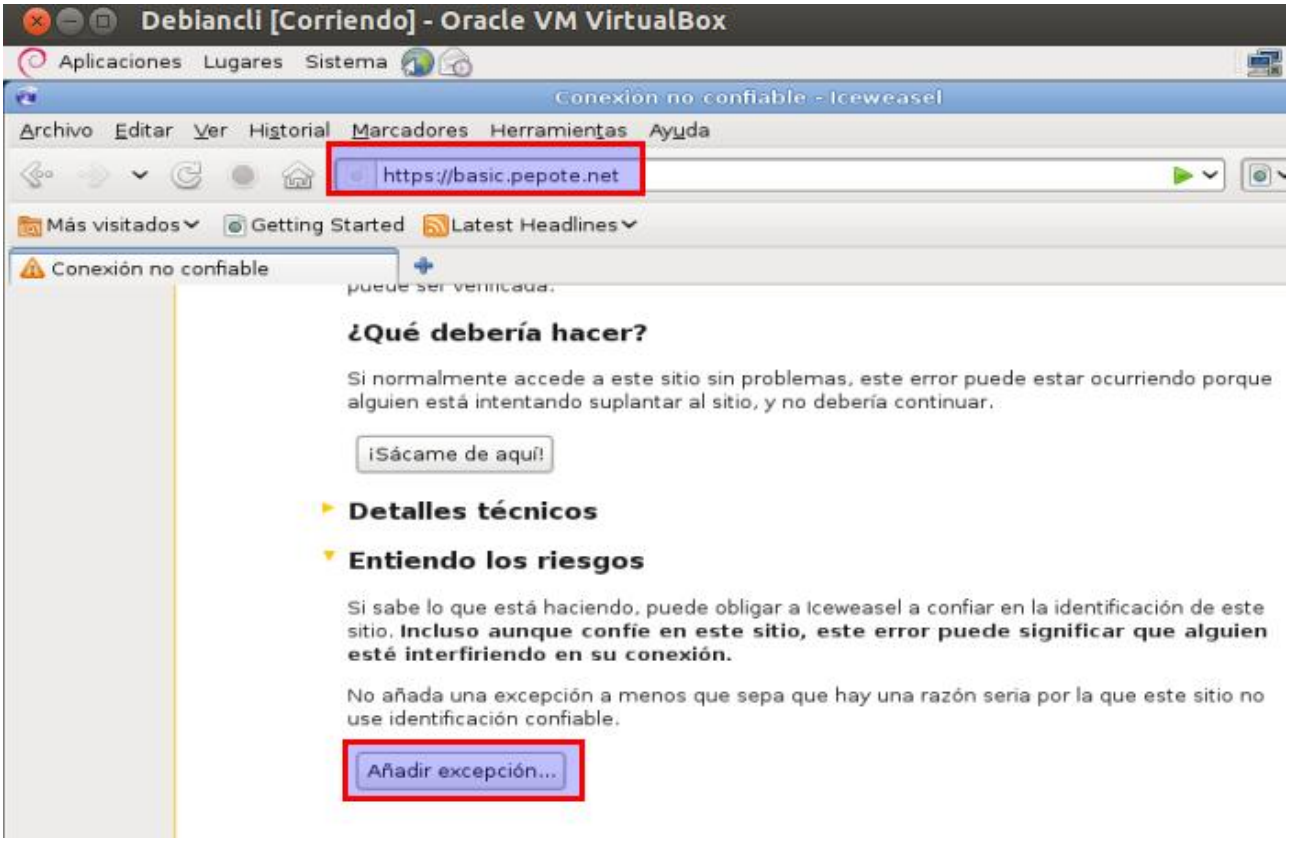
```
root@debian:/etc/apache2/sites-available# a2ensite hv_basic_pepote_net
Enabling site hv_basic_pepote_net.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@debian:/etc/apache2/sites-available# service apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's
fully qualified domain name, using 127.0.1.1 for ServerName
[Tue Jan 15 22:14:35 2013] [warn] _default_ VirtualHost overlap on port 443, the
first has precedence
 ... waiting apache2: Could not reliably determine the server's fully qualified d
omain name, using 127.0.1.1 for ServerName
[Tue Jan 15 22:14:36 2013] [warn] _default_ VirtualHost overlap on port 443, the
first has precedence
.
root@debian:/etc/apache2/sites-available#
```

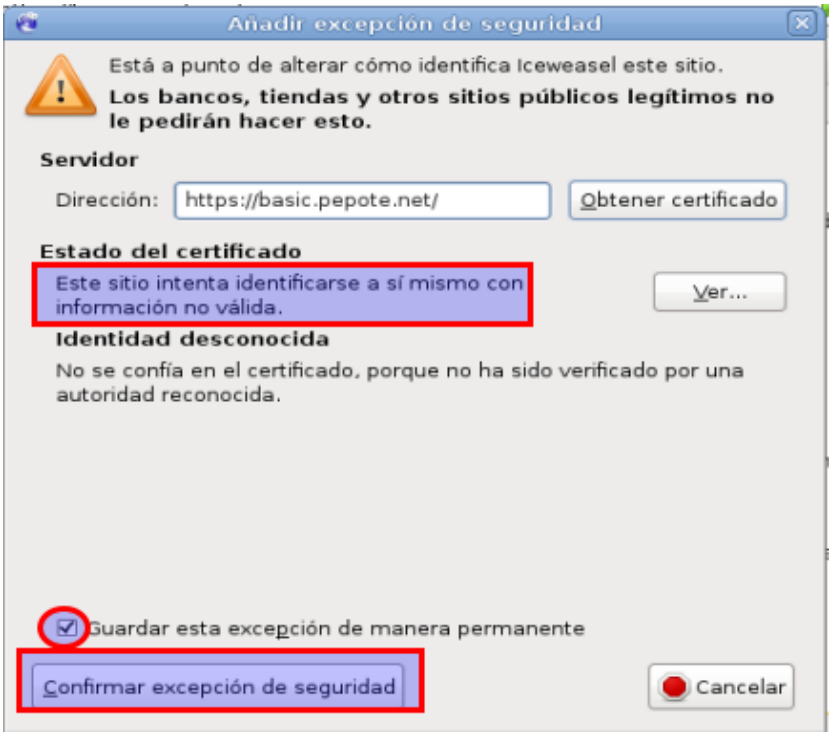
1) Configuramos el nombre DNS y reiniciamos dicho servicio:

```
  GNU nano 2.2.4       Fichero: /var/lib/bind/pepote.net.maestro

@ IN SOA www correo (1 2 3 4 5)
  IN NS www
www IN A 172.26.25.100
basic IN CNAME www
```

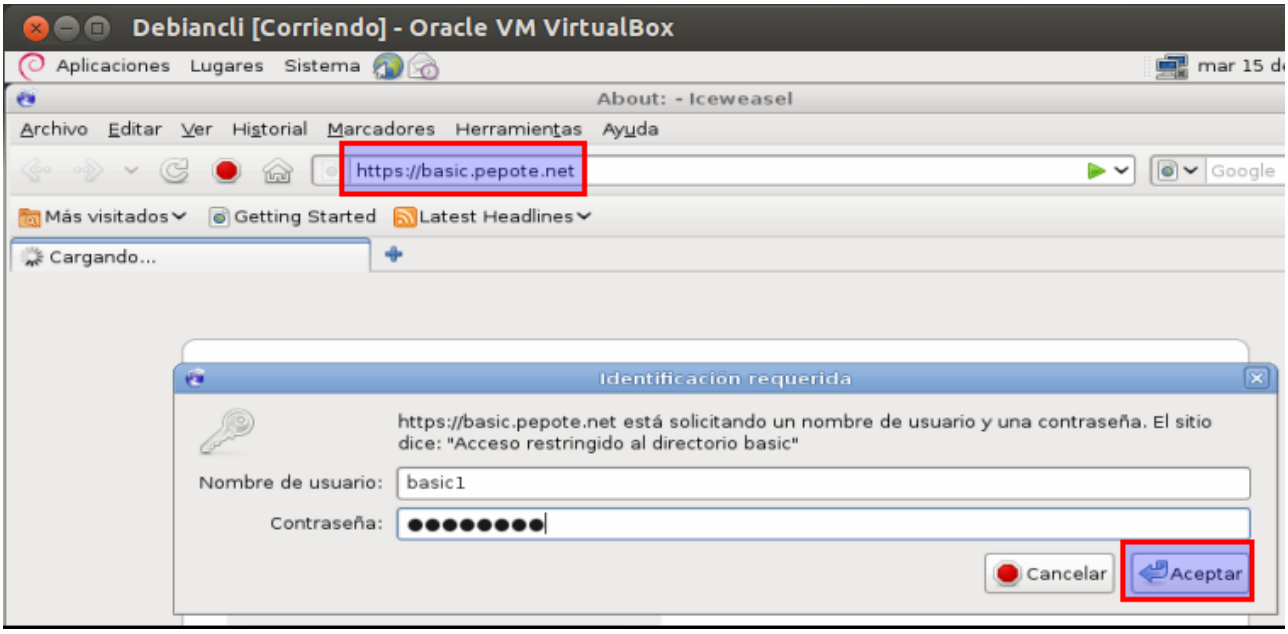
2) Probamos el funcionamiento desde el cliente:



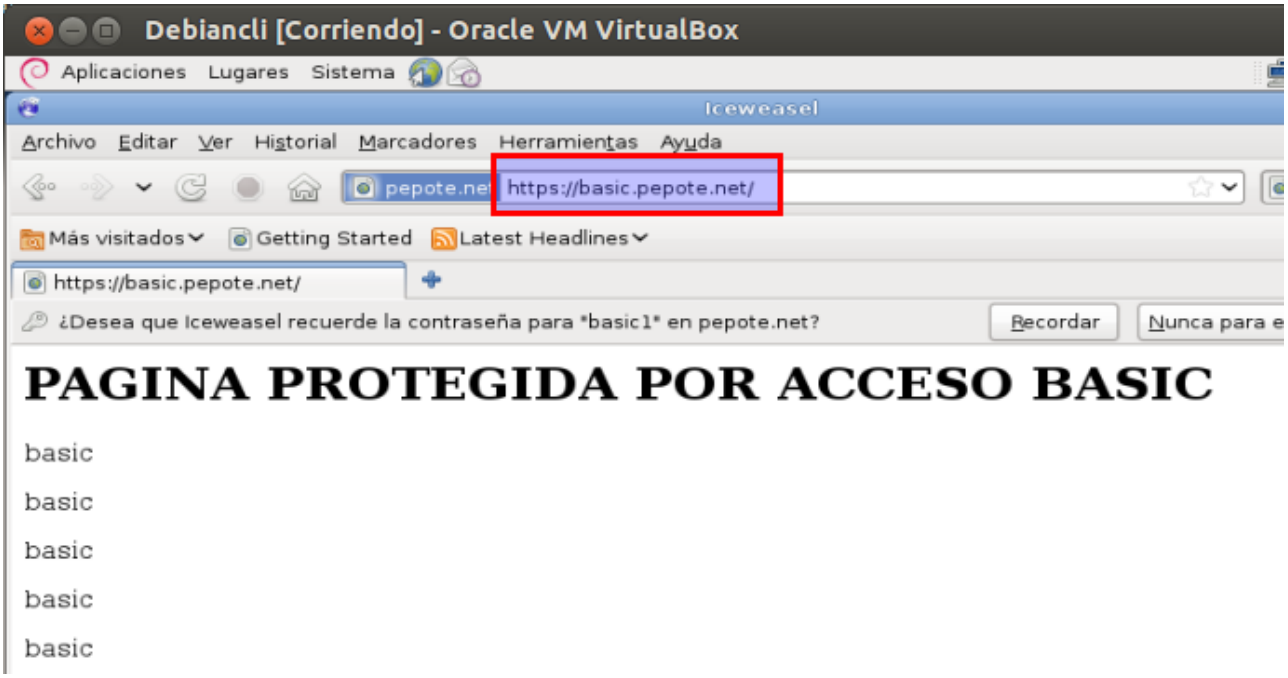

Debiancli [Corriendo] - Oracle VM VirtualBox
Aplicaciones Lugares Sistema
Conexión no confiable - Iceweasel
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
https://basic.pepote.net
Más visitados Getting Started Latest Headlines
Conexión no confiable
¿Qué debería hacer?
Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.
¡Sácame de aquí!
Detalles técnicos
Entiendo los riesgos
Si sabe lo que está haciendo, puede obligar a Iceweasel a confiar en la identificación de este sitio. Incluso aunque confíe en este sitio, este error puede significar que alguien esté interfiriendo en su conexión.
No añada una excepción a menos que sepa que hay una razón seria por la que este sitio no use identificación confiable.
Añadir excepción...


Añadir excepción de seguridad
Está a punto de alterar cómo identifica Iceweasel este sitio.
Los bancos, tiendas y otros sitios públicos legítimos no le pedirán hacer esto.
Servidor
Dirección: https://basic.pepote.net/
Obtener certificado
Estado del certificado
Este sitio intenta identificarse a sí mismo con información no válida.
Ver...
Identidad desconocida
No se confía en el certificado, porque no ha sido verificado por una autoridad reconocida.
Guardar esta excepción de manera permanente
Confirmar excepción de seguridad
Cancelar

Después de entender los riesgos y añadir la excepción, se nos solicitará la autenticación, pero teniendo en cuenta que ahora se realizará bajo una conexión segura por el protocolo HTTPS:



Si la autenticación es correcta se permitirá el acceso:



4. Configurar otros servidores virtuales HTTPS por distinto puerto de escucha

Existe la posibilidad de crear varios servidores virtuales seguros por HTTPS funcionando conjuntamente dentro de un mismo servidor web, pero por motivos de seguridad únicamente se podrá configurar uno por cada puerto de escucha.

Por defecto el puerto de escucha de HTTPS es el 443, por lo que si deseamos añadir servidores web seguros adicionales, deberemos añadir nuevos puertos de escucha para el protocolo HTTPS.

En nuestro caso crearemos un nuevo sitio virtual accesible por el puerto *444*, de nombre FQDN `seguro.pepote.net`, con el directorio de trabajo `/var/www/dirseguro` cargando la página de defecto de Apache y configurando su funcionalidad en el fichero `hv_seguro_pepote_net`.

1) Añadir nuevo puerto de escucha para HTTPS en el fichero `/etc/apache2/ports.conf`:

```
  GNU nano 2.2.4        Fichero: /etc/apache2/ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default
# This is also true if you have upgraded from before 2.2.9-3 (i.e. from
# Debian etch). See /usr/share/doc/apache2.2-common/NEWS.Debian.gz and
# README.Debian.gz

NameVirtualHost *:80
Listen 80

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
    Listen 444
</IfModule>
```

2) Crearemos el alias para utilizar en el acceso, es decir, `seguro.pepote.net`:

```
  GNU nano 2.2.4     Fichero: /var/lib/bind/pepote.net.maestro

@ IN SOA www correo (1 2 3 4 5)
  IN NS www
www IN A 172.26.25.100
basic IN CNAME www
seguro IN CNAME www
```

3) Crearemos la carpeta para el nuevo sitio seguro, es decir, `/var/www/dirseguro`, y su contenido a mostrar:

```
cd /var/www
mkdir dirseguro
nano index.html
```

```
root@debian:/var/www/dirseguro# ls -l
total 4
-rw-r--r-- 1 root root 159 ene 16 15:21 index.html
root@debian:/var/www/dirseguro# cat index.html
<H1>OTRO SITIO WEB SEGURO</H1>
<p>PUERTO DISTINTO (444)
<p>PUERTO DISTINTO (444)
<p>PUERTO DISTINTO (444)
<p>PUERTO DISTINTO (444)
<p>PUERTO DISTINTO (444)
```

4) Ahora crearemos el fichero de configuración del nuevo sitio seguro (`hv_seguro_pepote_net`) con las condiciones requeridas:

```
  GNU nano 2.2.4          Fichero: hv_seguro_pepote_net
<IfModule mod_ssl.c>

<VirtualHost *:444>
        ServerName seguro.pepote.net
        DocumentRoot /var/www/dirseguro

        <Directory />
           Options FollowSymLinks
           AllowOverride None
        </Directory>

        <Directory /var/www/dirseguro>
                DirectoryIndex index.html
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/seguro_pepote_net_error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/seguro_pepote_net_access.log combined
        SSLEngine on
        SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
        SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

</VirtualHost>
```

5) Activamos el nuevo sitio seguro y reiniciamos el servicio web y DNS:

```
root@debian:/etc/apache2/sites-available# a2ensite hv_seguro_pepote_net
Enabling site hv_seguro_pepote_net.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@debian:/etc/apache2/sites-available# service apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's
 fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
.
root@debian:/etc/apache2/sites-available# service bind9 restart
Stopping domain name service...: bind9 waiting for pid 838 to die.
Starting domain name service...: bind9.
root@debian:/etc/apache2/sites-available#
```

6) Probamos su funcionalidad, teniendo en cuenta que ahora existe la posibilidad de acceder a cada uno de los sitios seguro del servidor web, es decir al del puerto por defecto (443) y al del nuevo puerto configurado (444):