Lab - Servidor Multisite

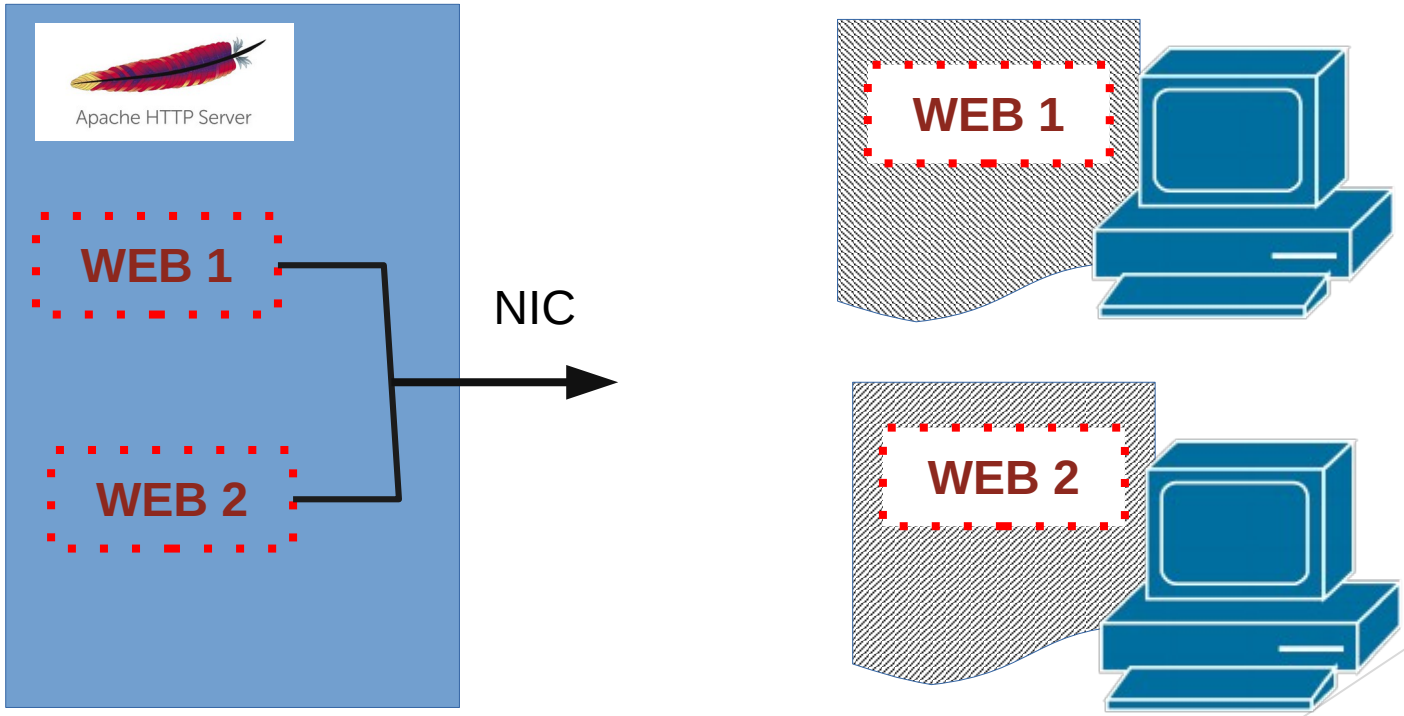
Servicios de Red e Internet – 2º DAW

Francisco Cuesta

Escenario

Puesta en marcha de un servidor apache con dos sitios web:

- Espacio público: Aloja la página web de la empresa en el puerto 443
- Intranet: Aloja la intranet de la empresa
- Sistema de autenticación con usuario/contraseña para la zona privada



Instalación

Instalamos el servidor apache2

sudo apt-get install apache2

Podemos comprobar que está instalado con los cualquiera de las siguientes opciones:

1.- **systemctl status apache2**
2.- **apachectl status**
3.- Desde un navegador vemos la página por defecto de la instalación

El servidor lo vamos a configurar para utilizar certificados para lo que hay que activar el módulo de seguridad

a2enmod -m ssl

Cerraremos el puerto 80 porque no se va a utilizar comentando la línea correspondiente del fichero **/etc/apache2/ports.conf**

Y por último deshabilitaremos el sitio web por defecto que ya no lo vamos a utilizar

sudo a2dissite 000-default.conf

Preparación pruebas

Para realizar las pruebas será necesario resolver nombres. La forma correcta sería configurando entradas en un servidor DNS.

En este caso, para simplificar, pondremos las entradas en el fichero /etc/hosts de la **máquina desde la que vamos a realizar las pruebas**.

```
  GNU nano 4.8                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       xucliente
192.168.1.155   empresa.com www.empresa.com publica.com intranet.empresa.com intranet

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Configuración página pública

Directorio de almacenamiento:
/var/www/publica/empresa.com/

Fichero de la empresa pública: **index.html**

Fichero de configuración del espacio web será **/etc/apache2/empresa.com.conf** que lo generamos con el siguiente comando

cd /etc/apache2/sites-available/
sudo cp default-ssl.conf empresa.com.conf

En la siguiente transparencia se muestran los contenidos

Para activar la web deberemos realizar
sudo a2ensite empresa.com.conf
systemctl reload apachectl

Observa en la siguiente configuración:
La página responderá a **empresa.com** y a **www.empresa.com**

Configuración página pública

IP y Puerto: *:443

Directorio página

ServerName
Nombre de la página a la que responde

Registros

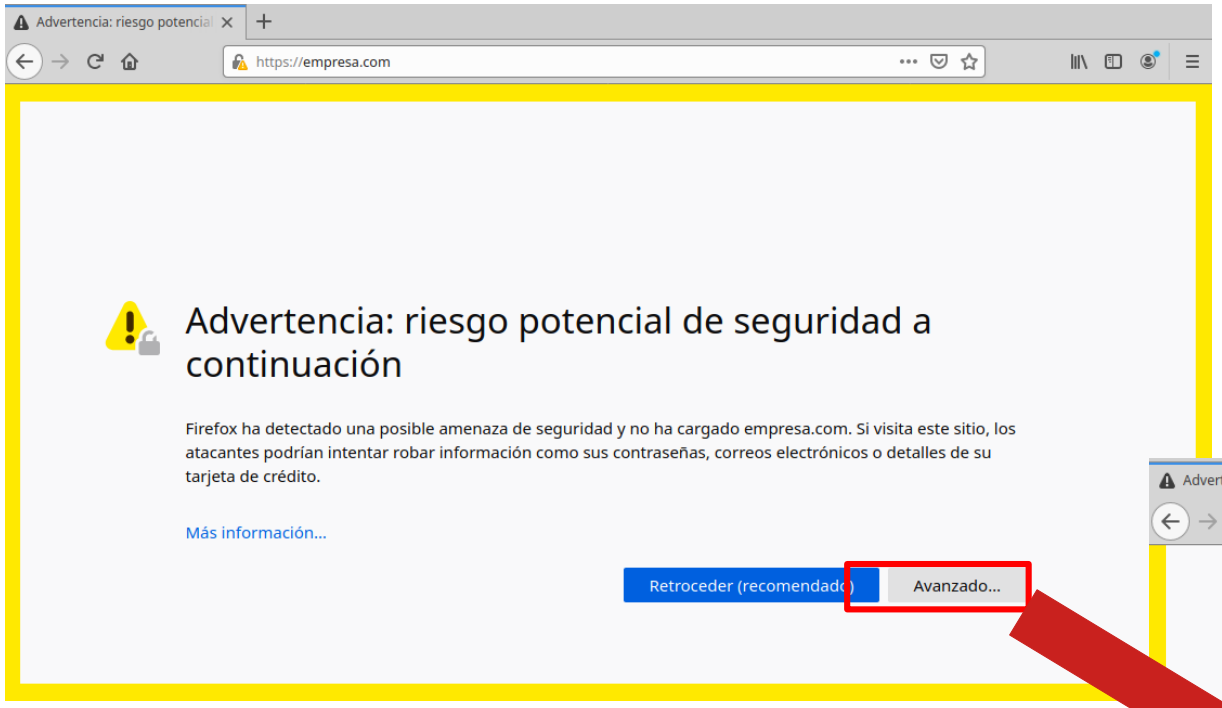
Activación SSL

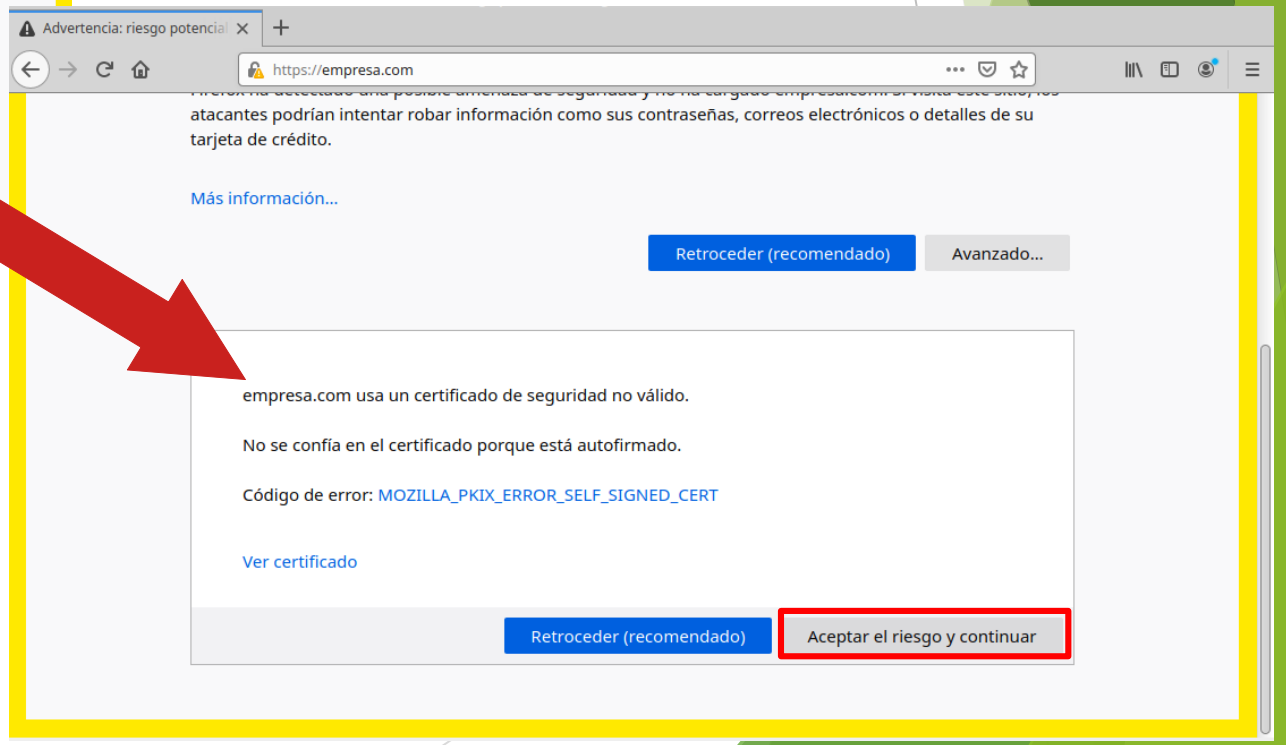
Certificados y clave
Estos no son válidos pero sirven para las pruebas

Directorio
Las opciones y permisos se colocan en esta sección

```
ico@empresa:~$ cat /etc/apache2/sites-available/empresa.com.conf
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerAdmin webmaster@empresa.com

                DocumentRoot /var/www/publica/empresa.com
                ServerName www.empresa.com
                ServerAlias empresa.com

                # Registros de error
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log vhost_combined

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/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

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
                <Directory /var/www/publica/empresa.com>
                </Directory>


        </VirtualHost>
</IfModule>
```

Prueba de la página





Debido a que usamos unos certificados no válidos el navegador nos avisa de que se trata de una conexión no segura

Configuración página privada

Directorio de almacenamiento:
/var/www/privada/intranet.com/

Fichero de la empresa pública: **index.html**

Fichero de configuración del espacio web será **/etc/apache2/intranet.empresa.com.conf** que lo generamos con el siguiente comando

cd /etc/apache2/sites-available/
sudo cp default-ssl.conf intranet.empresa.com.conf

En la siguiente transparencia se muestran los contenidos

Para activar la web deberemos realizar
sudo a2ensite intranet.empresa.com.conf
systemctl reload apachectl

Observa en la siguiente configuración:
La página responderá a **intranet.empresa.com** a **intranet.com** y a **intranet**

Configuración página privada

En este momento, cada vez que accedamos a las páginas web, según el nombre utilizado, nos llevará a una página o a la otra

https://intranet.empresa.com

Comando CLI alternativo para hacer la prueba
curl -k -H "Host:intranet.empresa.com" https://127.0.0.1

Solicita la página del vhost: intranet.empresa.com
A la dirección local con HTTPS

https://empresa.com

Comando CLI alternativo para hacer la prueba
curl -k -H "Host:www.empresa.com" https://127.0.0.1

Solicita la página del vhost: www.empresa.com
A la dirección local con HTTPS

Configuración página por defecto

NOTA: Apache busca siempre el sitio web con el nombre solicitado pero si no encuentra ninguno:

1) Devuelve el que ServerName = Nombre de la máquina del servidor
2) Si no existe ese dominio, devuelve el primero que encuentra.

Se recomienda hacer un dominio por defecto que responderá al nombre de la máquina del servidor, es decir si la máquina se llama “www” poner **ServerName www** en su configuración.

Crea un dominio por defecto en el que salga una página con dos links, uno a empresa.com y otro a intranet.empresa.com.

Habilitar contraseña en intranet

Vamos a crear el usuario “empleado” para probar entrar un método de autenticación de entrada a la intranet.
Vamos a realizar el método más básico en el que Apache leerá los usuarios de un fichero.
Crearemos los usuraios en **/opt/apache2/intranet.com/** para lo cual hay que crear las carpetas de la ruta.
Comando:
sudo htpasswd -c /opt/apache2/intranet.com/passwords empleado

Esto nos introduce la contraseña en el fichero **/opt/apache2/intranet.com/passwords**

A continuación modificamos el fichero de configuración de la intranet.com.conf añadiendo entre las etiquetas <Directory> la siguiente infromación

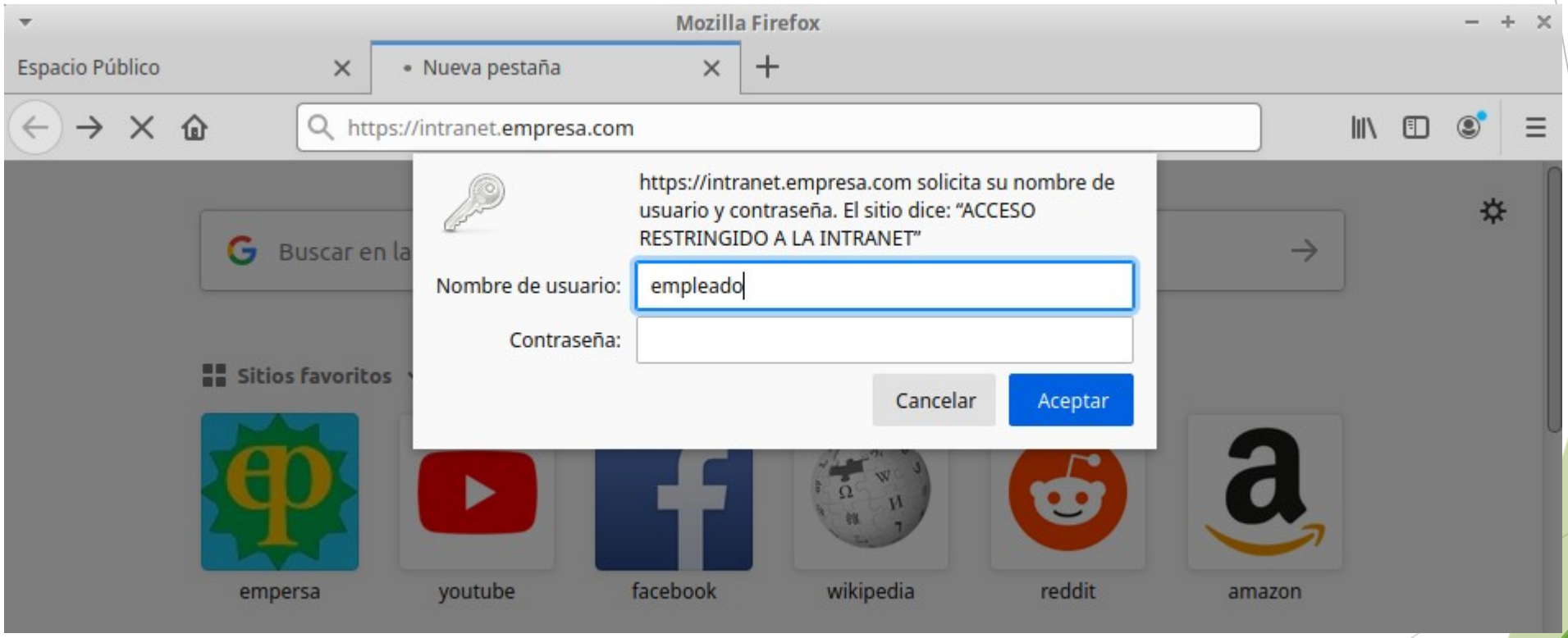
```
<Directory /var/www/privada/intranet.com>
        Options Indexes
        AuthType Basic
        AuthName "ACCESO RESTRINGIDO A LA INTRANET"
        AuthBasicProvider file
        AuthUserFile "/opt/apache2/intranet.com/passwords"
        Require valid-user
</Directory>
```

Una vez terminemos hay que recargar apache

Nota: Para que funcione debe estar presente el módulo auth_basic que normalmente está habilitado por defecto.

Habilitar contraseña en intranet

Con la autenticación puesta en marcha nos saldrá la siguiente pantalla antes de acceder al sitio.



FIN

Servidor Apache con múltiples sitios web