Apéndice B

Manual de instalación y configuración

Para la intalación del sistema nos debemos asegurar, en primer lugar, que disponemos de la versión 0.82 de NoCatAuth, que está disponible en la web nocat.net. Dependiendo de lo que se quiera instalar se necesitará:

- El parche NoCatAuth-0.82-Eneo.diff. Para aplicar los cambios realizados en la aplicación para su control y rellenado de tablas.
- El archivo comprimido EneoAdmin.tar.gz. Para instalar la aplicación de administración.

Los pasos a seguir en la instalación son los siguientes:

1. Descomprimir el archivo NoCatAuth-0.82.tar.gz como superusuario:
   ```
   su -
   tar zvxf NoCatAuth-0.82.tar.gz
   ```
2. Aplicar el parche al directorio NoCatAuth. Desde el directorio que cuelga el directorio NoCatAuth-0.82, se ejecuta:
   ```
   patch -p0 <NoCatAuth-0.82-Eneo.diff
   ```
   Con esto queda parcheado el directorio, y ya contiene todos los archivos necesarios para la instalación.

A partir de aquí se distingue si se está instalando la pasarela o el servidor de autenticación, ya que los pasos son distintos.

B.1. Pasarela

La pasarela está diseñada para ejecutarse en una máquina independiente. Si hubiera otras reglas del cortafuegos definidas serán sobreescritas.

Para ejecutar el demonio de la pasarela se necesita permiso de superusuario. Los pasos a seguir para la instalación son los siguientes:

1. Asegurarnos de que están instalados los requisitos previos:
   - Linux 2.4.x con iptables.
   - gpgv. Sirve para verificar la firma PGP. Está incluido en paquete gnupg, y puede ser descargado desde http://www.gnupg.org/download.html
   - Tener instalado el paquete iproute2 con el comando tc. Para la calidad de servicio.
2. Editar el Makefile. La única opción que hay es la ruta donde instalar la pasarela. Por defecto está en PREFIX = /usr/local/nocat.
3. Desde el directorio NoCatAuth-0.82 se ejecuta:
   `make gateway`
   Esto instalará todo el software.
4. Editar el archivo de configuración /usr/local/nocat/nocat.conf. Estos son los parámetros necesarios:
   - GatewayMode. Debe estar en modo Pasivo.
   - LoginTimeout. Se debe poner al mínimo permitido que es 60. Este es el tiempo de gracia que se le concede a los usuarios una vez expulsados del sistema.
   - TroustedGroups. Debe poner Any para que todos los grupos sean válidos, y cuando se pasa la marca de política funcione correctamente.
   - AuthServiceAddr. Debe contener la dirección del servidor de autenticación.
   - InternalDevice. Debe ser el nombre de la interfaz local, normalmente será el nombre de la tarjeta inalámbrica o de la tarjeta ethernet conectada con el punto de acceso.
   - ExternalDevice. Debe ser el nombre de la interfaz exterior.
   - LocalNetwork. Debe ser la dirección de la red local y la máscara de red. Se puede usar el formato reducido 111.222.333.444/24.
   - DNSAddr. Debe ser la dirección del servidor de nombres.

- Nuevas directivas introducidas en este proyecto. Las directivas anteriores son de NoCatAuth, y vienen en su documentación, y además hay una traducción completa del archivo de configuración en la sección A.1 de este proyecto. Las nuevas directivas que hay que rellenar son:
  - Ubicacion. Se debe rellenar con la MAC de la pasarela, o un nombre único que la describa. Es el valor que se utiliza para rellenar la tabla *conexiones*.
  - MarkPolicyX. Deben estar todas estas directivas rellenas, aunque no se haya definido ninguna política. Pueden tener todas el mismo valor.
  - PolicyX. Se usan para definir las políticas que se van aplicar a los usuarios. Se pueden definir las que se desee de las seis disponibles. La forma de definir una política es introduciendo una lista de los puertos que se van a dejar abiertos para el uso de los usuarios que pertenezcan a esa política. A cada política definida debe corresponder una marca distinta.
  - MinBandWidthDown. Indica el ancho de banda mínimo que se asigna a la clase por defecto en la interfaz interna.
  - MinBandWidthUp. Idem, para la interfaz externa.
  - MaxBandWidthDown. Es el ancho de banda total disponible para la interfaz interna.
  - MaxBandWidthUp. Idem, para la interfaz externa.

5. Copiar el guión de inicio en /etc/init.d/. Si se quiere se inicie el servicio al reiniciar la pasarela cree los enlaces correspondientes en los directorios rc.X.

Para arrancar la pasarela ejecutar el guión de inicio:

```
/etc/init.d/gateway start
```

B.2. Servidor de autenticación

Una vez descomprimido el archivo NoCatAuth-0.82, y aplicado el parche, los pasos a seguir son los siguientes:

1. El software que es necesario tener instalado es el siguiente:
   - Tener instalado un servidor web seguro que soporte el uso de protocolos SSL[1] y TLS[2].
   - Tener un interprete de Perl 5 (5.6 o mejor recomendado).

[1] Secure Sockets Layer.
[2] Transport Layer Security.

- Tener los siguientes módulos de perl: Digest::MD5, DBI y DBD::MySQL. Se pueden conseguir a través de CPAN.
- gnupg. Para cifrar las comunicaciones entre la pasarela y el servidor.
- MySQL. La version 3.23.4x o superior.
- sshd. Se necesita un servidor ssh instalado para la comunicación entre la pasarela y el servidor.

Para ejecutar el Servidor Web seguro se necesita una clave y un certificado. Se puede generar un certificado autofirmado o comprar un certificado firmado por CA (Certificate Authority). Las ventajas de usar un certificado firmado por CA permite que los navegadores se conecten de forma segura sin hacer ninguna pregunta de confirmación. Y además cuando la CA emite un certificado firmado, se está garantizando la identidad de la organización que proporciona las páginas web al navegador.

2. Editar el Makefile. La única opción disponible es el path donde instalar los archivos. Por defecto es PREFIX = /usr/local/nocat.

3. Desde el directorio NoCatAuth-0.82 ejecuta:
   `make authserv`
   Esto instalará las partes más importantes del servidor.

4. Ejecuta `make pgpkey`. Las opciones por defecto están bien para la mayoria de configuraciones. Es muy importante no introducir ninguna clave. Con esto se crean las claves pública y privada para cifrar las comunicaciones.

5. Editar el archivo /usr/local/nocat/nocat.conf. Los parámetros necesarios son:

   - DataSource. Debe estar en DBI. Para usar la autenticación desde MySQL.
   - Database. Debe ser `dbi:mysql:database=nocat`. O cualquier otro nombre para la base de datos.
   - DB_user. El nombre de usuario para abrir la sesión con la base de datos en MySQL.
   - DB_Passwd. La clave que se usa para abrir la sesión.

   En la sección A.1.2 hay una traducción del archivo de configuración donde se expilcan todas las directivas que contiene.

6. Asegurarse que el directorio /usr/local/nocat/pgp y todo su contenido pertenece al usuario que ejecuta el servidor apache. Normalmente será el usuario Apache:
   `chown -R apache.apache /usr/local/nocat/pgp`

7. Incluir en el archivo de configuración de apache el archivo etc/authserv.conf. Se puede poner un `Include` dentro del archivo de configuración.

8. Crear las tablas de nocat. Lo primero que debemos hacer es crear la base de datos nocat. Para crear la base de datos nocat hay que crear un usuario. Nos debemos conectar a MySQL como administrador y ejecutar:
   ```
   GRANT ALL ON nocat.* TO nocat@localhost IDENTIFIED BY ''mypasswd''
   ```
   Para crear la base de datos ejecutar:
   ```
   CREATE DATABASE nocat;
   ```
   Para crear la tablas necesarias ejecutar los comandos:
   ```
   use nocat
   \. NoCatAuth-0.82/etc/nocat.schema
   ```
   Ya tenemos creada la base de datos nocat y sus tablas. No es necesario rellenar nada en estas tablas.

9. Crear la base de datos ControlNocat. Es importante configurar las dos bases de datos para que sean accedidas por el mismo usuario:
   ```
   GRANT ALL ON ControlNocat.* TO nocat@localhost IDENTIFIED BY
   ''mypasswd''
   CREATE DATABASE ControlNocat;
   use ControlNocat
   \. NoCatAuth-0.82/tablas/crea_tablas.sql
   ```

10. Rellenar las tablas de la base de datos ControlNocat. Para rellenar las tablas se utiliza el archivo llena_tablas.sql. Antes de ejecutarlo hay que editarlo para definir las ubicaciones disponibles, y las políticas definidas. El código de política debe condicidir con las marcas definidas en el archivo de configuración de la pasarela. Una vez editado y cambiado los valores, se ejecuta:
    ```
    mysql -unocat -p ControlNocat <llena_tablas.sql
    ```
    Para rellenar la tabla de id_cola. Ejecutar el siguiente script desde el bash:
    ```
    ./fill_id
    ```

11. Editar el archivo lib/ControlNocat.pm y poner en las constantes definidas el valor de usuario, de clave y el nombre de la base de datos:
    ```
    use constant USER => "nocat";
    use constant PASSWD => "mypasswd";
    use constant DRIVER_DB => "dbi:mysql:ControlNocat";
    ```

12. Copiar el archivo /usr/local/nocat/trustedkeys.gpg a todas las pasarelas.

13. Reinicia el servidor Web, y asegúrate de que MySQL y sshd están iniciados.

B.3. Programa de administración

Para instalar el programa de administracion descomprimir el archivo EneoAdmin.tar.gz en el directorio /usr/local/, o donde se haya instalado el servidor de au-

tenticación:

```
tar zxvf EneoAdmin.tar.gz
```

Esto creará los archivos correspondientes en los directorios correspondientes. Debemos asegurarnos que el propitario del directorio cgi-bin/admin es apache, o el usuario con el que se ejecute el servidor.

Para el correcto funcionamiento debemos asegurarnos que el archivo de configuración de apache contiene las siguientes directivas:

```
DocumentRoot /usr/local/nocat/htdocs
AccessFileName .htaccess
AllowOverride All
```

Por defecto está configurado para que se permita sólo el acceso al usuario "nocat" con la clave "eneotecnologia". Para cambiar esto debemos ir al directorio usuarios y borrar el fichero .htpasswd. Seguidamente lo volvemos a crear con el nombre de usuario que se desee utilizar:

```
htpasswd -c /usr/local/nocat/usuarios/.htpasswd nombre_de_usuario
```

Se solicitará la clave y ya está creado el archivo de nuevo. Ahora tenemos que editar el archivo .htaccess en los directorios nocat/htdocs/admin/ y nocat/cgi-bin/admin/. En ambos hay que cambiar la directiva:

```
require user nombre_de_usuario
```

Por último para abrir la aplicación de administración debemos abrir un navegador y poner en la barra de dirección:

```
https://localhost/admin/admin.html
```

Si se ejecuta remotamente habrá que sustituir localhost por la dirección del servidor de autenticación.