

Tech Note

Nota Técnica

LHM y Hotspots

Introducción

Un **hotspot** ('punto caliente') es una zona de cobertura Wi-Fi, en el que un punto de acceso (*access point*) o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP). Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etcétera. Este servicio permite mantenerse conectado a Internet en lugares públicos, y puede brindarse de manera gratuita o pagando una suma que depende del proveedor. (definición extraída de Wikipedia)

Los dispositivos UTM de Sonicwall permiten dos modos de configuración de Hotspots. En el primero de ellos, el propio Sonicwall actúa como portal cautivo, mostrando a los usuarios una página pidiendo credenciales de acceso y encargándose de la validación de los usuarios invitados (Guest Users); en el segundo caso, el Sonicwall intercepta los intentos de acceso de los usuarios a la red y redirige el tráfico a un servidor web externo que hará las funciones de portal cautivo, mostrando al usuario algún tipo de desafío que ha de superar antes de obtener acceso a la red. En este segundo caso, la comunicación entre el Sonicwall y el servidor web externo se realiza usando el protocolo LHM (Lightweight Hotspot Messaging).

Este documento hace referencia exclusivamente a la configuración de los portales cautivos y los diferentes métodos de autenticación que ofrecemos como ejemplo, pero no explica cómo configurar la red wireless ni los SonicPoints. Para obtener información más detallada sobre cómo configurar la red wireless con SonicPoints y puntos de acceso virtuales (VAP), puedes consultar las siguientes notas técnicas:

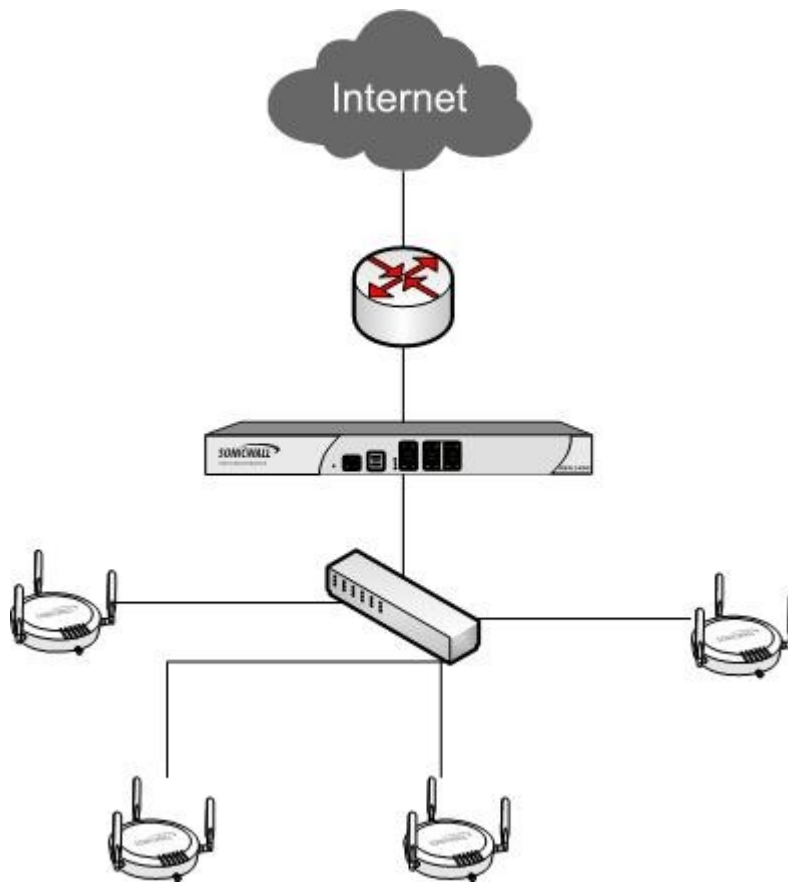
- SonicOS Enhanced 5.0 Virtual Access Points Feature Module:
<https://www.fuzeqna.com/sonicwallkb/csr/kbdetail.asp?kbid=5800>
- Configuring a **Virtual Access Point (VAP)** Profile for **Wireless Corporate Users** using SonicPoints:
<https://www.fuzeqna.com/sonicwallkb/csr/kbdetail.asp?kbid=5801>
- Configuring a **Virtual Access Point (VAP) Profile** for Wireless Guest access using SonicPoints:
<https://www.fuzeqna.com/sonicwallkb/csr/kbdetail.asp?kbid=5798>

Escenario de ejemplo 1

Para la elaboración de este documento, vamos a usar como ejemplo una red wireless sencilla formada por un dispositivo UTM, un switch y 4 puntos de acceso SonicPoints.

Cada uno de estos SonicPoints anunciará dos redes, una para usuarios internos que llamaremos WLAN_Corporativa, que tendrá la señal de radio encriptada con WPA2-PSK; y otra red wireless abierta que llamaremos HotspotInvitados y que será nuestro Hotspot.





Sonicwall como portal cautivo

En este ejemplo, el propio Sonicwall hará las funciones de portal cautivo obligando a los usuarios a autenticarse con un nombre de usuario y contraseña. Estos usuarios hará falta crearlos en el Sonicwall, pero no como usuarios normales, sino como usuarios invitados (guest users).

Una vez que la red wireless está configurada y funcionando, lo primero que debemos hacer para configurar este tipo de hotspot es habilitar los Guest Services en la zona que nos interese (normalmente una red wireless abierta, sin encriptación).

Tech Note

The screenshot displays the SonicWall Network Security Appliance web interface. The left sidebar shows the navigation menu with 'Zones' selected. The main content area is titled 'Guest Services' and includes the following configuration options:

- ☒ Enable Guest Services
 - ☐ Enable inter-guest communication
 - ☐ Bypass AV Check for Guests
 - ☐ Enable External Guest Authentication: [Configure...](#)
 - ☐ Enable Policy Page without authentication: [Configure...](#)
 - ☐ Custom Authentication Page: [Configure...](#)
 - ☐ Post Authentication Page:
 - ☐ Bypass Guest Authentication:
 - ☐ Redirect SMTP traffic to:
 - ☐ Deny Networks:
 - ☒ Pass Networks:
- Max Guests:
- Wireless Zone Guest Services Options:
 - ☒ Enable Dynamic Address Translation (DAT)

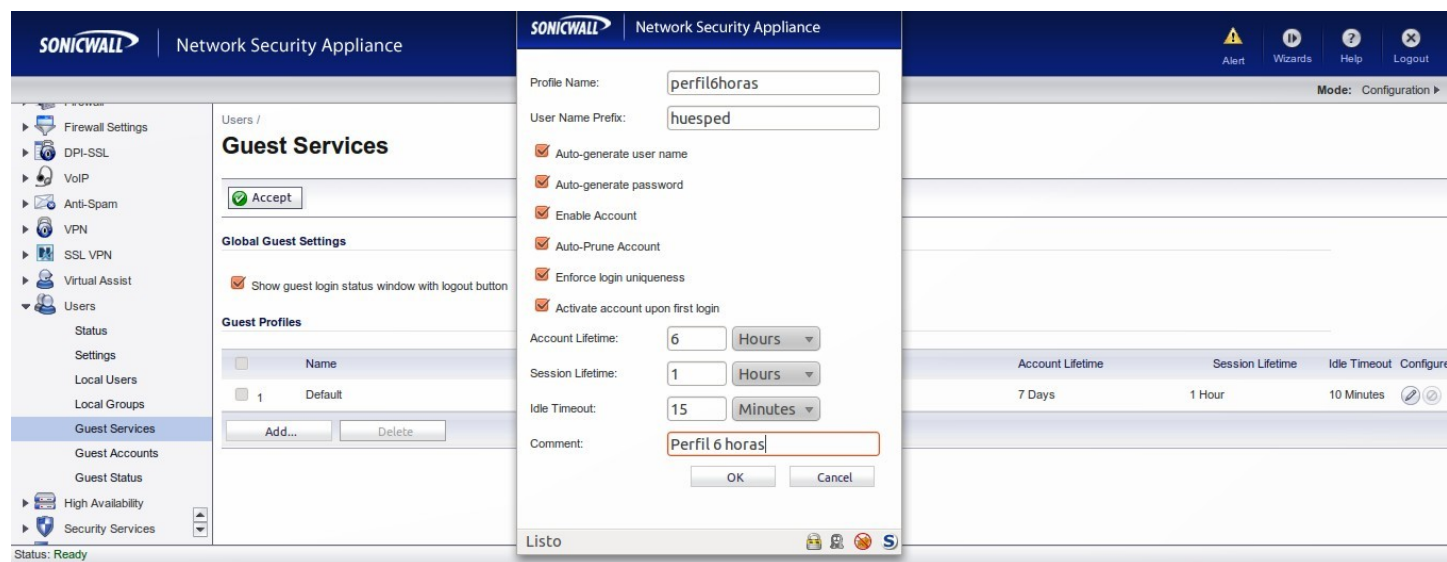
The status bar at the bottom indicates 'Ready'.

Algunas de las opciones de configuración que nos ofrecen los Guest Services son:

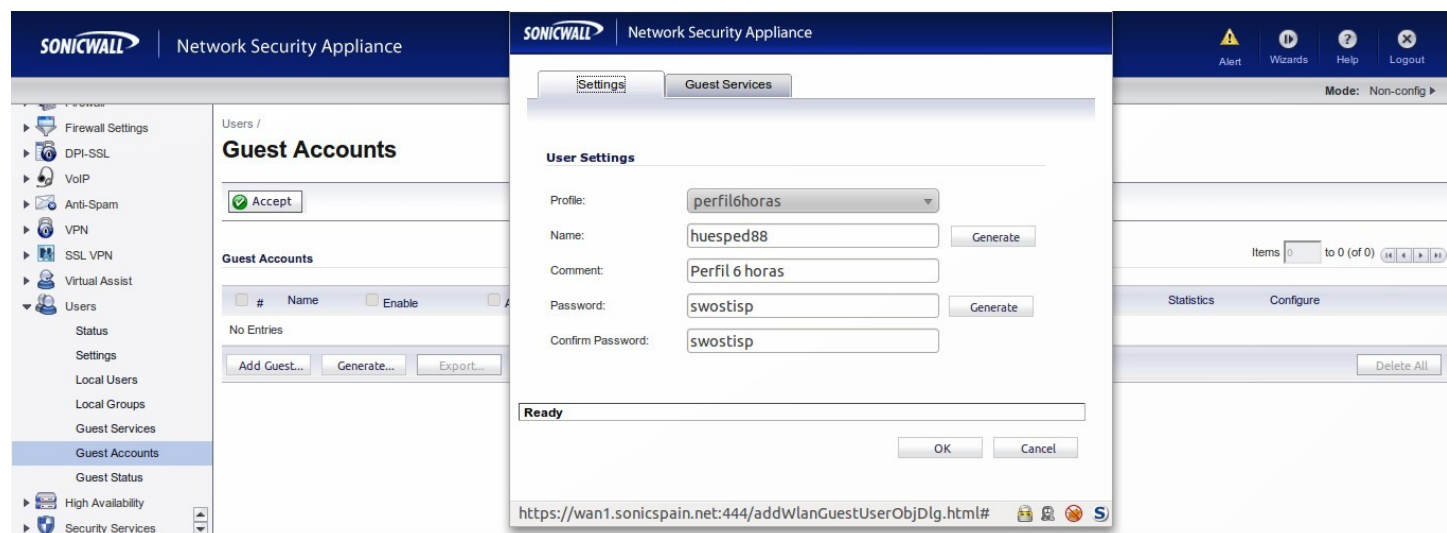
- Enable inter-guest communication: Permite que los usuarios wireless se puedan comunicar entre sí una vez autenticados.
- Enable Policy Page without authentication: Como alternativa al método de autenticación con usuario/contraseña, esta opción permite usar como portal cautivo una página con normas de uso del servicio (disclaimer). Si se usa este método, no haría falta crear Guest Users.
- Custom Authentication Page: Permite personalizar el portal cautivo modificando la cabecera y el pie de página. Las opciones de personalización son limitadas.
- Post Authentication Page: Página web a la que serán redirigidos los usuarios una vez autenticados.
- Deny/Pass Networks: El acceso a las redes definidas en esta sección estará permitido o denegado independientemente de que el usuario esté autenticado o no.
- Enable Dynamic Address Translation (DAT): En caso de que el usuario tenga su adaptador de red wireless configurado con una IP estática en lugar de dinámica, con esta opción activada el usuario tendrá acceso igualmente a la red independientemente de la dirección IP de su adaptador.

Creacion de Usuarios Invitados (Guest Users)

Cuando usamos el UTM como portal cautivo, es el propio UTM quien se encarga de la validación de usuarios. Teniendo en cuenta que el perfil de estos usuarios es muy dinámico, haciendo uso esporádico de la red y durante un tiempo limitado, los dispositivos UTM de Sonicwall permiten crear perfiles de conexión y usuarios invitados de una forma cómoda y sencilla. Para ello, primero hemos de ir a la sección Users → Guest Service y crear un nuevo perfil:

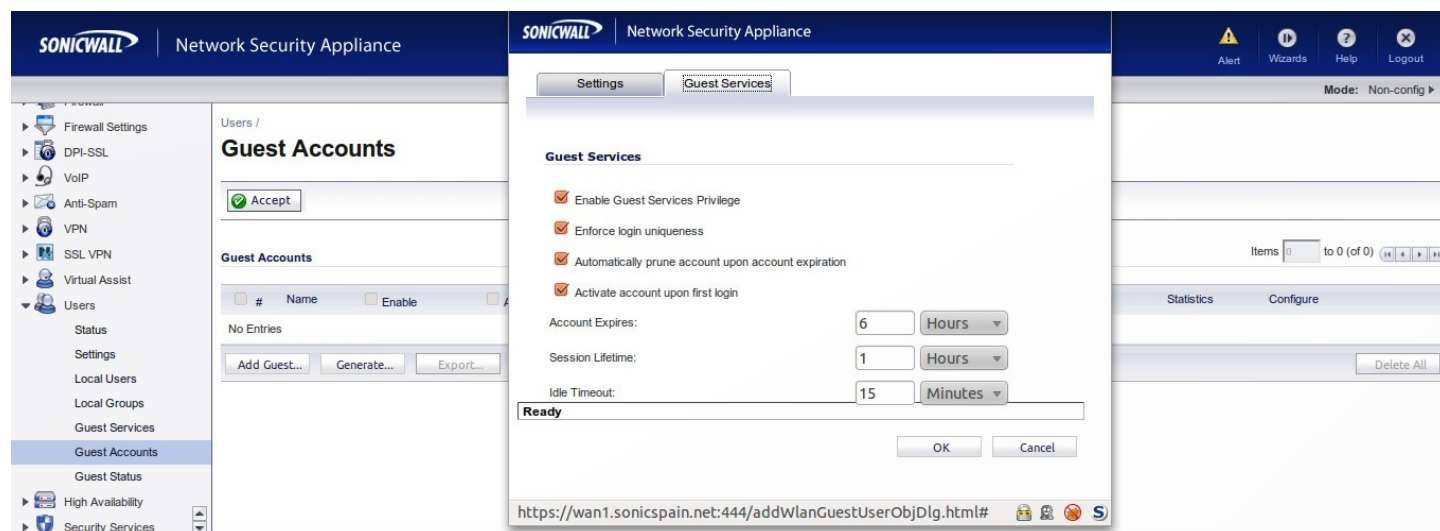


Una vez que hemos creado todos los perfiles necesarios, vamos a la sección de Users → Guest Accounts y generamos las cuentas de invitados. En caso de que necesitemos generar una única cuenta, pulsaremos el botón Add Guest, y seleccionaremos alguno de los perfiles que hemos creado en el paso anterior.

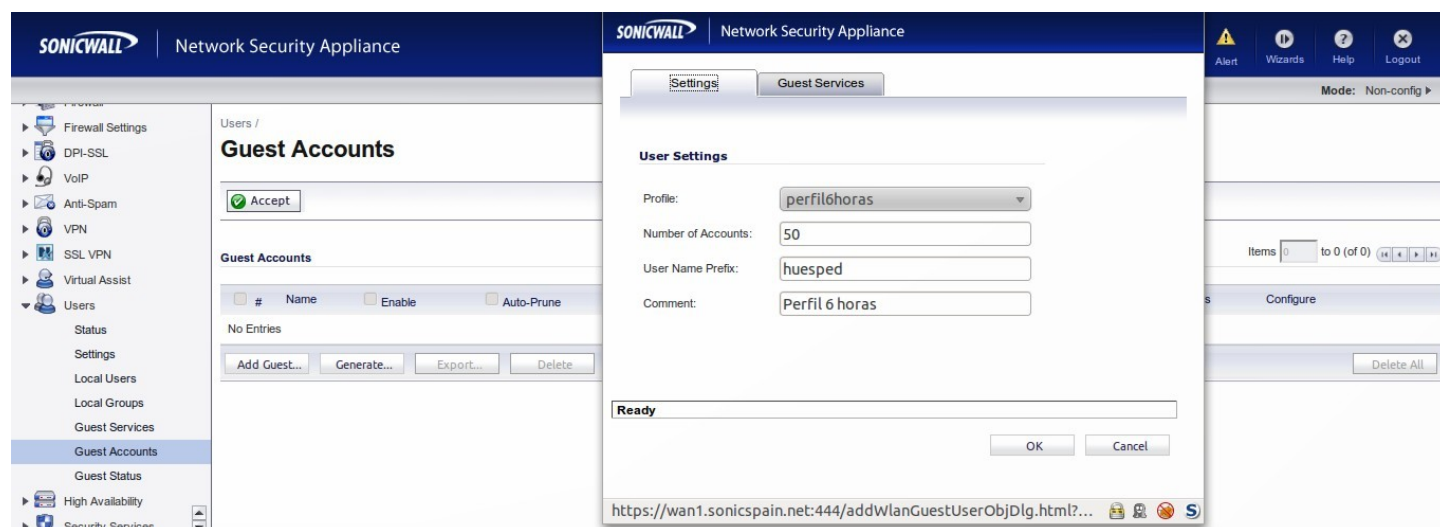


Tech Note

Desde la pestaña Guest Service, podremos sobrecribir cualquier parámetro por defecto del perfil, y dichos cambios se aplicarán únicamente a este usuario:



Si el administrador necesitase crear un lote de usuarios en un único paso, lo puede hacer pulsando el botón Generate, en cuyo caso podrá seleccionar un perfil, y el número de cuentas invitado que quiere generar en ese lote:



Tech Note

Una vez que los usuarios han sido creados, es posible imprimir el ticket con las credenciales que le darán acceso durante el tiempo contratado:

The screenshot shows the SonicWall Network Security Appliance web interface. The left sidebar contains a navigation menu with options like Firewall, Firewall Settings, DPI-SSL, VoIP, Anti-Spam, VPN, SSL VPN, Virtual Assist, Users, Status, Settings, Local Users, Local Groups, Guest Services, Guest Accounts (selected), Guest Status, and High Availability. The main content area is titled 'Guest Accounts' and includes an 'Accept' button. Below it, a table lists guest accounts. A modal window titled 'Guest Account Detail' is open, showing the following information:

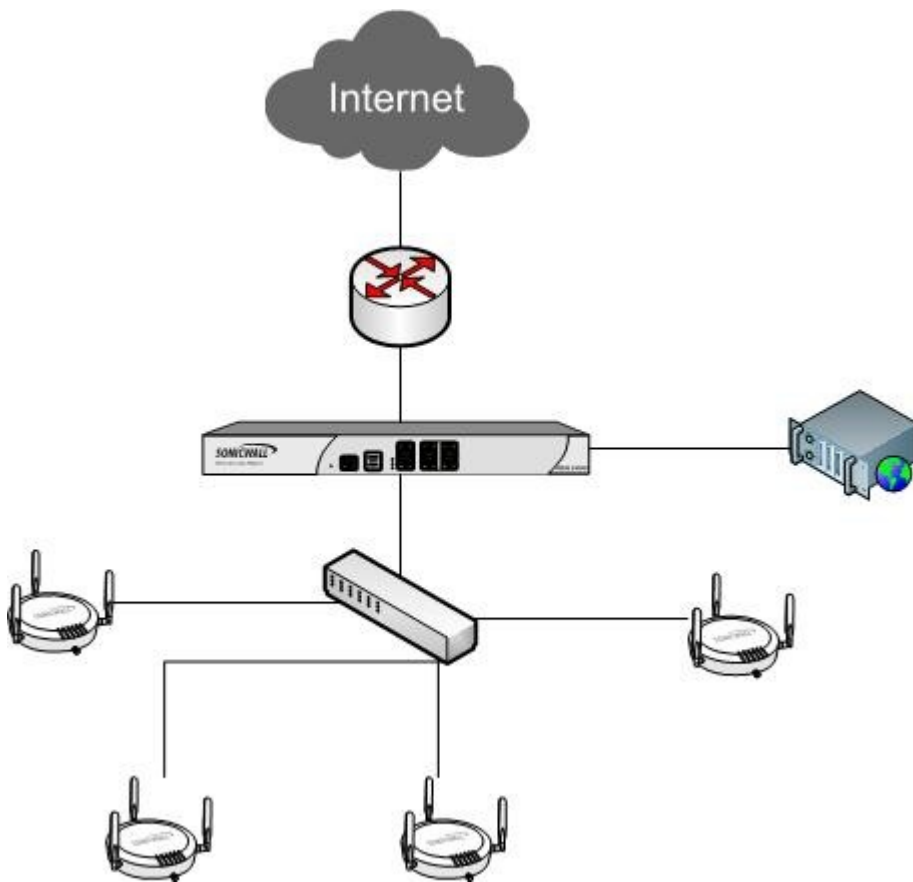
Description	Value
Account Name:	huesped79
Password:	deubriw
Enabled:	Yes
Comment:	Perfil 6 horas
Created:	THU MAR 17 00:24:10 2011
Account Expires:	Unused
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	15 Minutes

The modal window also includes a 'Listo' button and a '15 Minutes' timer. The main interface also features buttons for 'Add Guest...', 'Generate...', 'Export...', and 'Delete'. A status message at the bottom indicates 'Status: The configuration has been updated.'

Escenario de ejemplo 2

Para nuestro segundo ejemplo, vamos a modificar ligeramente el escenario anterior, añadiendo un servidor web que será el encargado de autenticar a los usuarios mediante un portal cautivo personalizable.

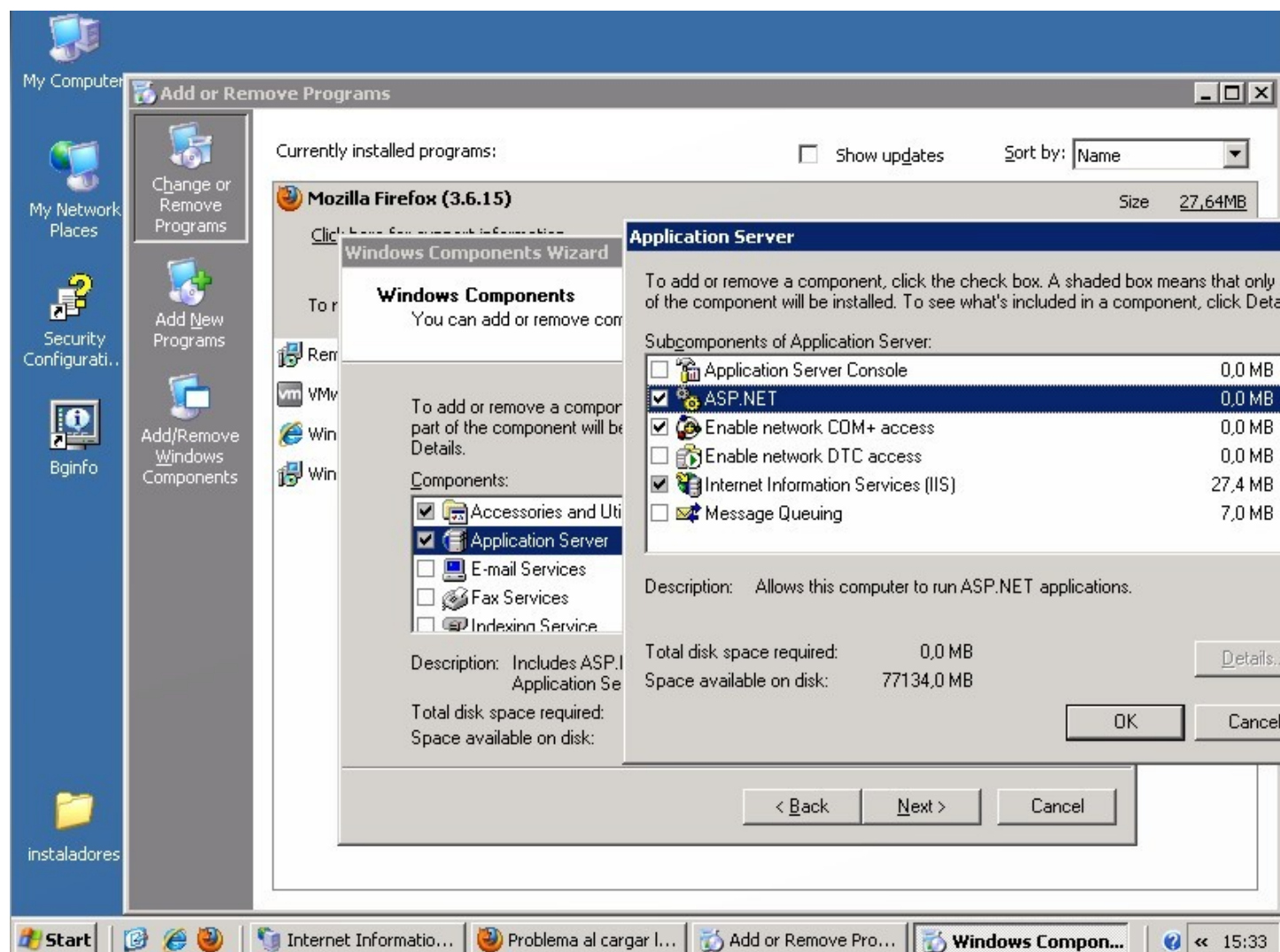
Para configurar el acceso al portal cautivo en el servidor web, previamente es necesario importar alguno de nuestros scripts de ejemplo en el propio servidor web, y configurar el UTM para que apunte a la URL que contiene el portal cautivo escogido.



Instalación y configuración del servidor web

Para este ejemplo, vamos a usar como servidor web Internet Information Server instalado sobre un servidor Windows 2003, pero es posible montar este tipo de escenarios usando un servidor diferente (p.ej., Linux) o un servidor web alternativo como Apache.

El primer paso, sería instalar el servidor web (IIS) y el componente ASP.NET, que será necesario para la correcta ejecución de nuestros scripts de ejemplo, ya que son páginas ASP escritas en lenguaje VisualBasic.



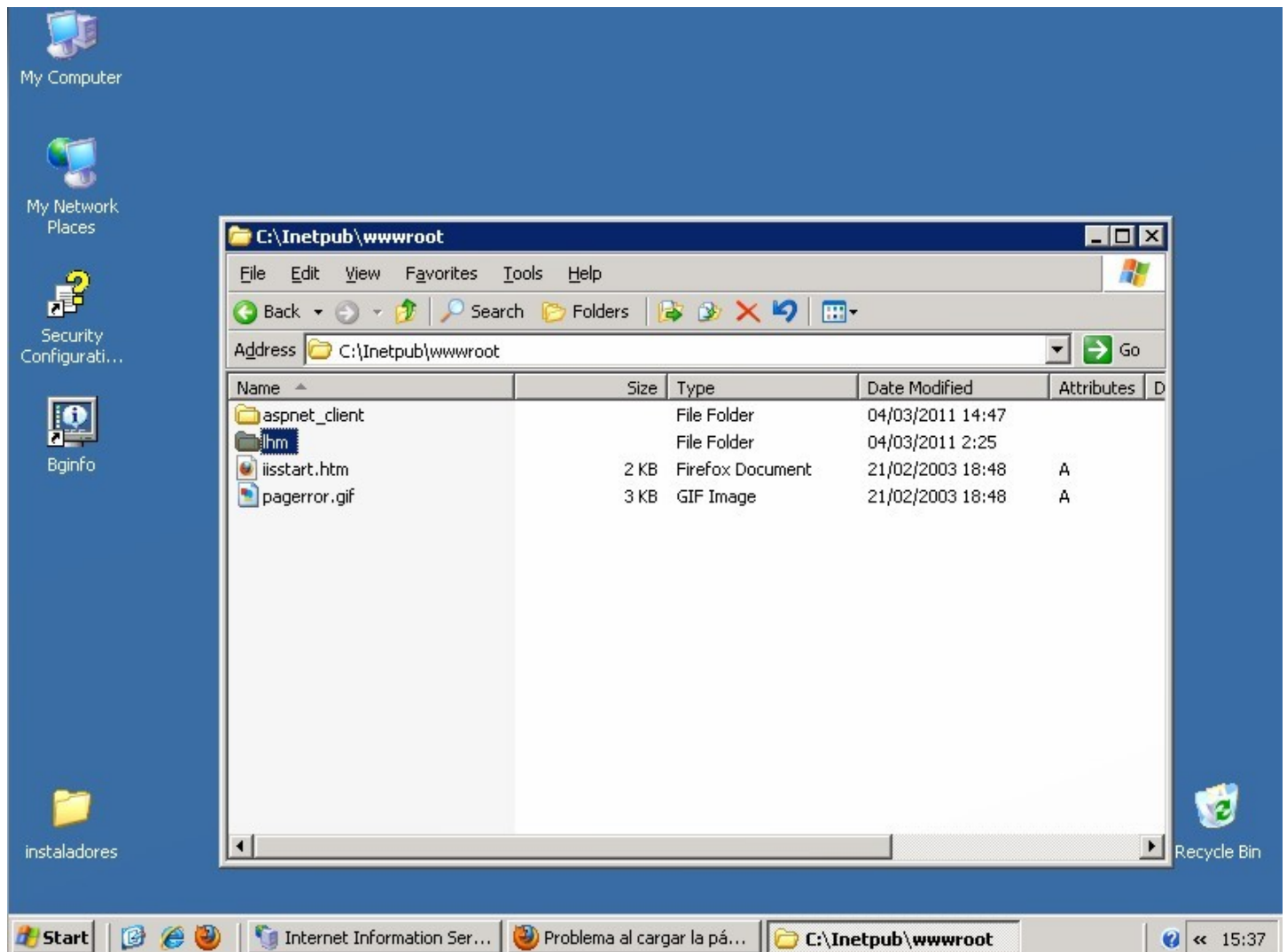
Tech Note

En segundo lugar, tendríamos que copiar alguno de los scripts de ejemplo en el directorio por defecto de nuestro servidor web, que en este caso es C:\InetPub\wwwroot.

Nuestros scripts de ejemplo se pueden descargar desde la siguiente URL:

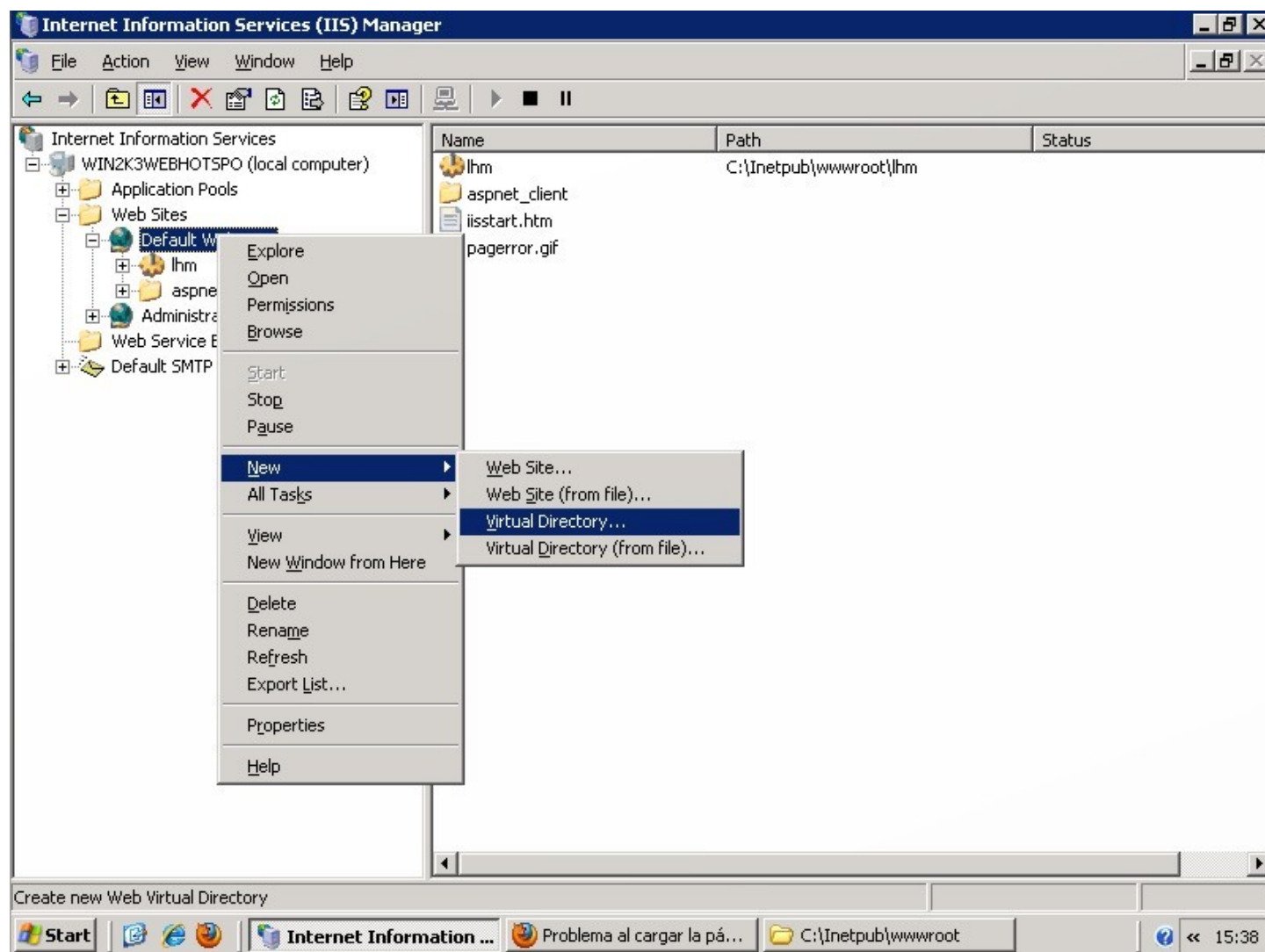
ftp://avbpartner:so3wrlaS9@ftp.sonicwall.eu.com/Restricted/Alex/Firmwares/UTM/Wireless/Hotspots/SonicWALL_ASP_Authentication_Scripts_Library.zip

Una vez descargado el fichero zip, debemos descomprimirlo y copiar el script de ejemplo elegido en el directorio C:\InetPub\wwwroot del servidor web.



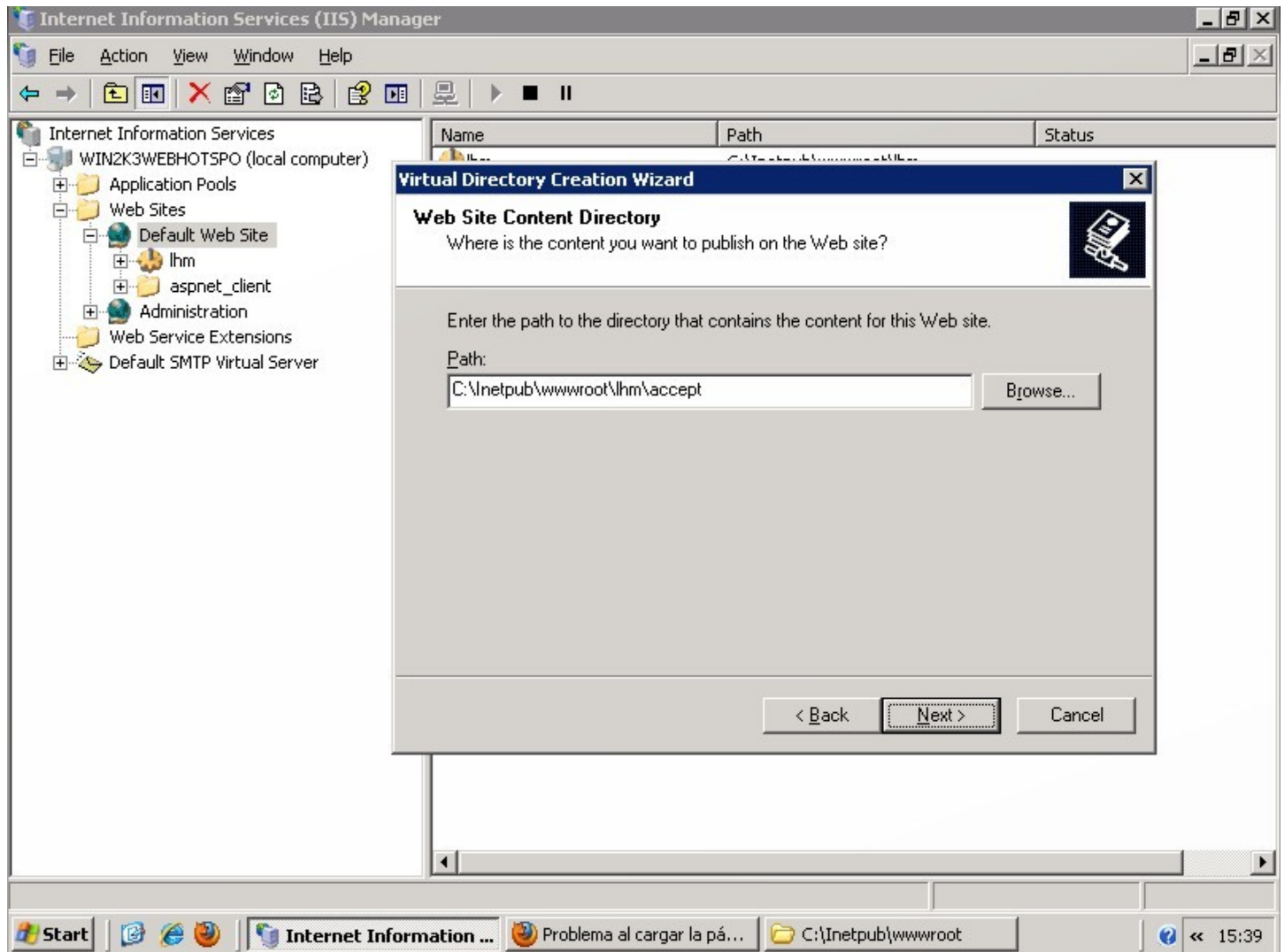
Tech Note

Por último, hemos de configurar nuestro servidor web para que pueda mostrar correctamente las páginas ASP de ejemplo. Para ello, creamos un nuevo directorio virtual:



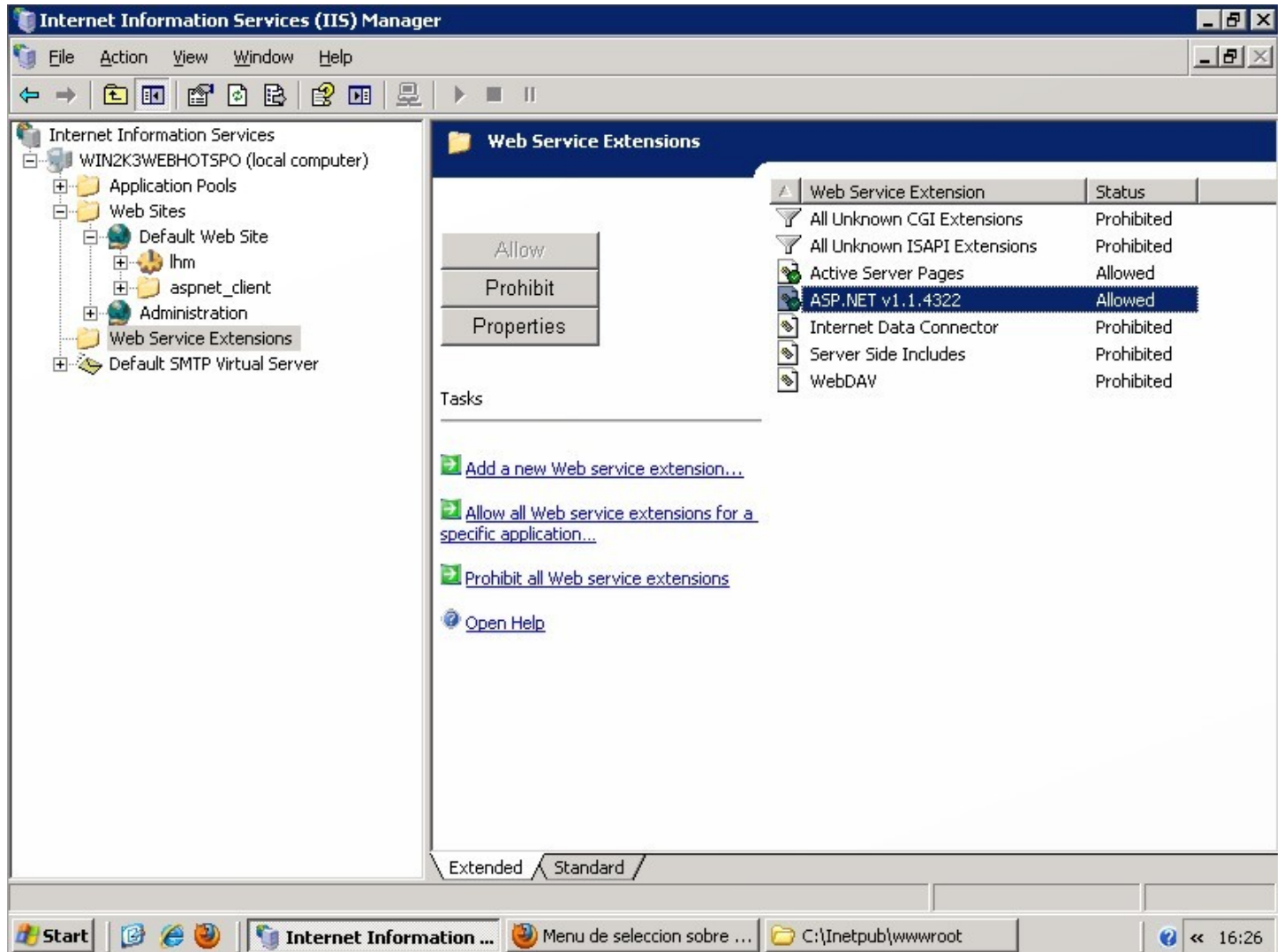
Tech Note

Le damos un nombre, y seleccionamos el directorio donde están las páginas ASP que hemos escogido para nuestro portal cautivo:



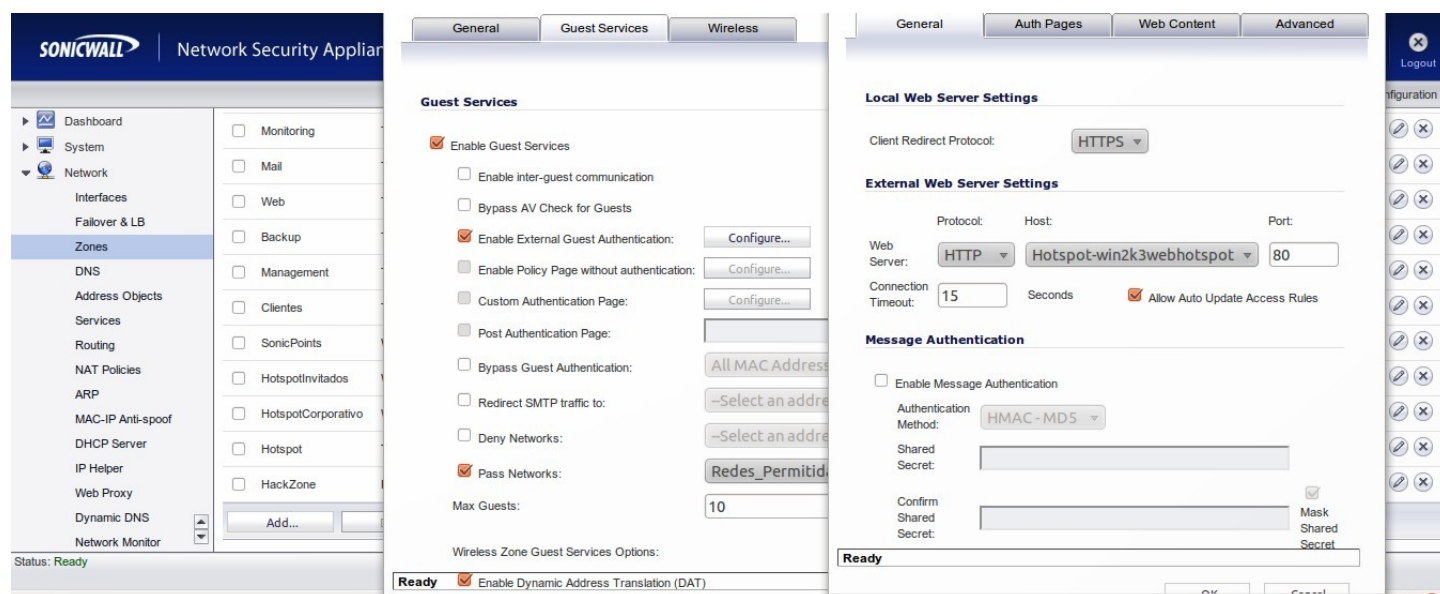
Tech Note

En la sección Web Service Extensions del gestor de IIS, podremos verificar si la extensión ASP.NET está permitida o no. Para una correcta ejecución de los scripts, es necesario habilitar este componente:



Configuración del UTM con autenticación externa

Una vez que el servidor web está correctamente instalado y configurado, tendremos que configurar el UTM para que capture las peticiones de acceso a la red de los usuarios del hotspot, y las redirija al servidor web externo para su identificación. Para ello, tenemos que loguearnos en el UTM, ir a la sección de Network → Zones, seleccionar la zona donde queremos habilitar nuestro hotspot, activar la opción de Enable Guest Services, habilitar la opción de Enable External Guest Authentication y pulsar el botón Configure:



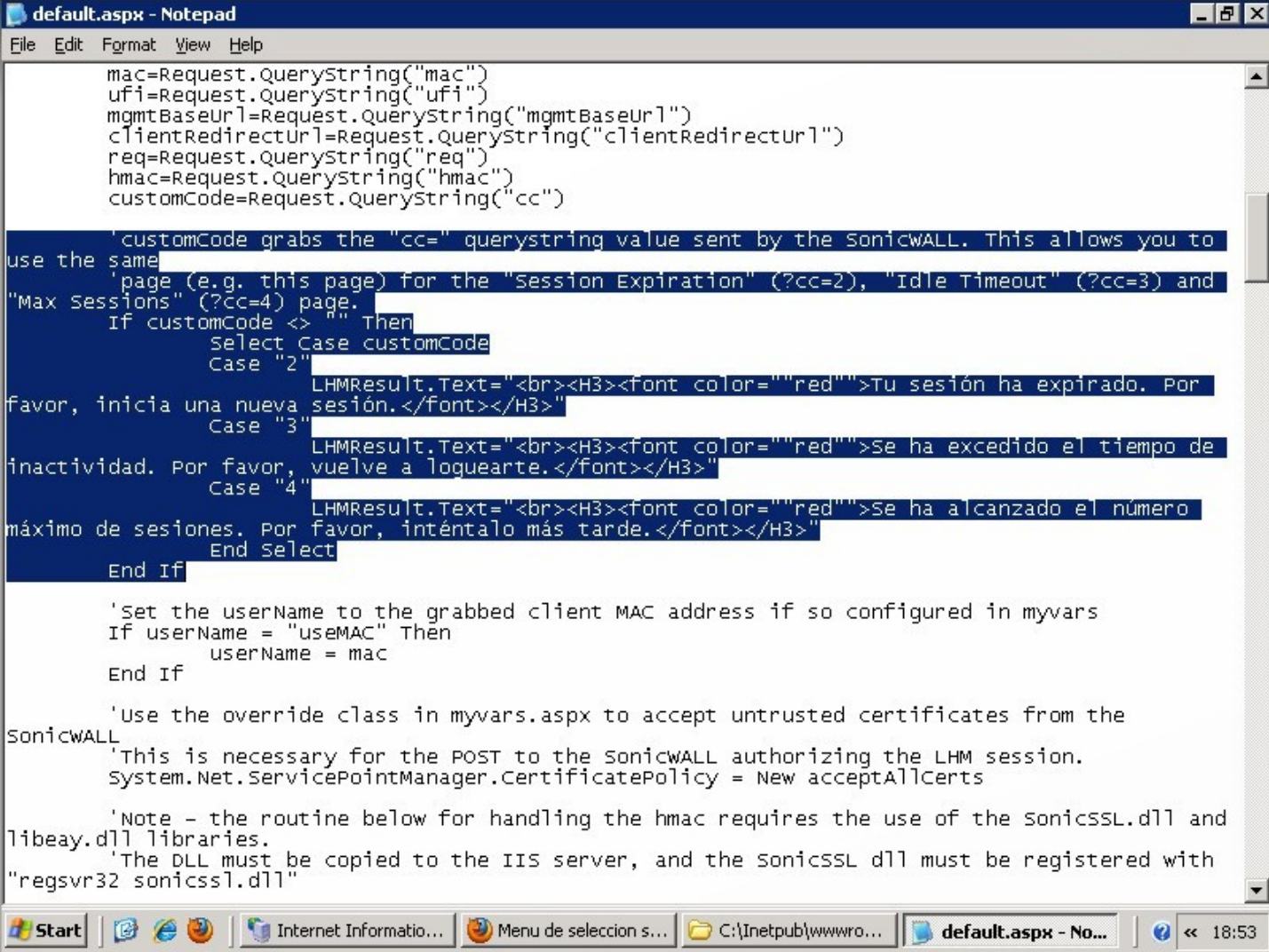
Al pulsar el botón Configure, se abrirá un pop-up que nos pedirá información sobre el servidor web a donde queremos redirigir a los usuarios del hotspot para su identificación. En la sección Local Web Server Settings, podremos escoger el protocolo de redirección de los clientes (Client Redirect Protocol), pudiendo escoger entre HTTP y HTTPS. La opción escogida en esta sección hace referencia al protocolo que se usará durante el proceso de autenticación en la comunicación entre los clientes y el dispositivo UTM. Si nos fijamos en el diagrama de red de este ejemplo, veremos que nuestro servidor web está instalado en una zona diferente a donde están instalados los SonicPoints, de esta forma forzamos a que la comunicación entre los clientes wireless de nuestro hotspot y el servidor web pase a través del UTM.

En la sección de external web server settings, tendremos que configurar la IP, el puerto y el protocolo que se usará para la comunicación con nuestro servidor web. La opción que escojamos en la sección Protocol hará referencia al protocolo que se usará en la comunicación entre el UTM y el servidor web. Para que los clientes hotspot puedan acceder al portal cautivo e identificarse correctamente, el UTM tiene que permitir el acceso. Si la opción que dice Allow Auto Update Access Rules está habilitada, las reglas de acceso necesarias serán creadas automáticamente.

En la sección de Message Authentication, podremos configurar algunos parámetros adicionales para incrementar la seguridad de nuestro escenario hotspot durante el proceso de autenticación. Estas opciones de seguridad van más allá del propósito de este documento, si estás interesado en obtener más información sobre estas opciones, consulta la Guía del Administrador.

Tech Note

En la pestaña Auth Page, tendremos que indicar las rutas para acceder a los scripts que previamente hemos instalado en nuestro servidor web. Podremos introducir diferentes rutas para la página que queremos que se muestre para la autenticación (Login Page), cuando la sesión ha expirado (Session Expiration Page), cuando se ha alcanzado el tiempo de inactividad (Idle Time Out Page) o cuando se ha alcanzado el número máximo de sesiones (Max Sessions Page). En nuestros scripts de ejemplo, en lugar de tener páginas diferentes para cada una de estas opciones, tenemos una única página o script (default.aspx), al que podemos invocar con diferentes parámetros:



```
default.aspx - Notepad
File Edit Format View Help

mac=Request.QueryString("mac")
ufi=Request.QueryString("ufi")
mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
clientRedirectUrl=Request.QueryString("clientRedirectUrl")
req=Request.QueryString("req")
hmac=Request.QueryString("hmac")
customCode=Request.QueryString("cc")

'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows you to
use the same
'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout" (?cc=3) and
"Max Sessions" (?cc=4) page.
If customCode <> "" Then
    Select Case customCode
        Case "2"
            LHMResult.Text="<br><H3><font color=""red"">Tu sesión ha expirado. Por
favor, inicia una nueva sesión.</font></H3>"
        Case "3"
            LHMResult.Text="<br><H3><font color=""red"">Se ha excedido el tiempo de
inactividad. Por favor, vuelve a loguearte.</font></H3>"
        Case "4"
            LHMResult.Text="<br><H3><font color=""red"">Se ha alcanzado el número
máximo de sesiones. Por favor, inténtalo más tarde.</font></H3>"
    End Select
End If

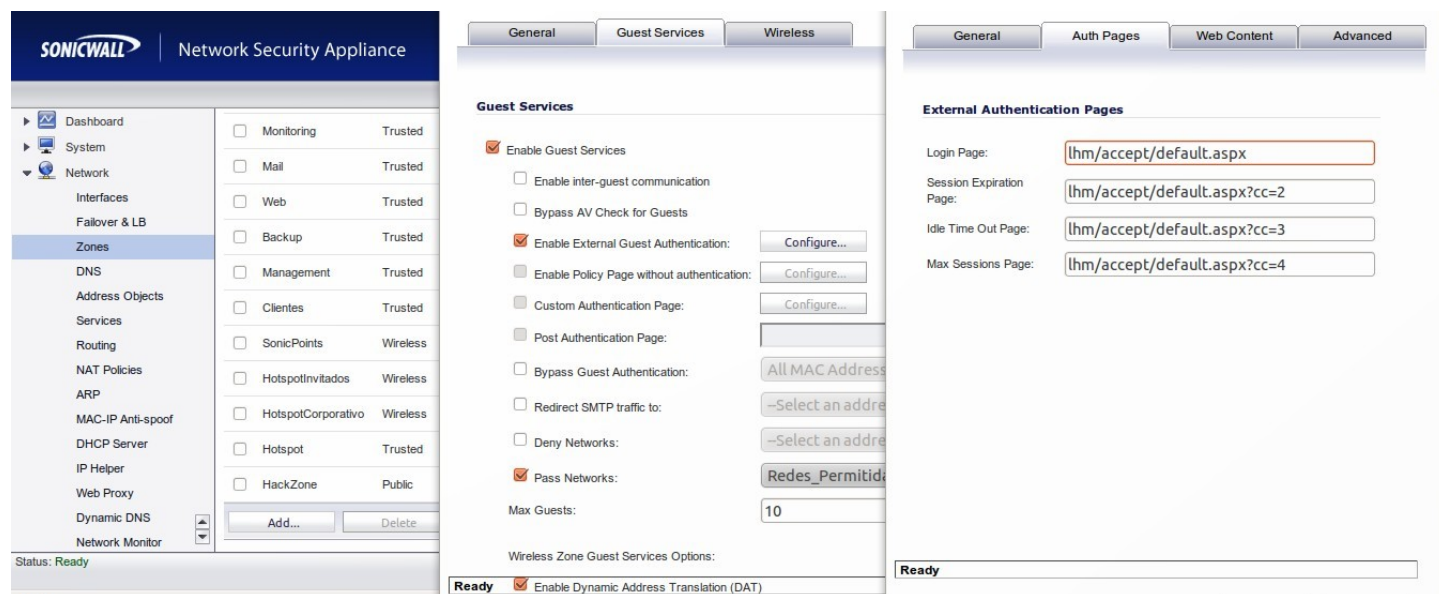
'Set the userName to the grabbed client MAC address if so configured in myvars
If userName = "useMAC" Then
    userName = mac
End If

'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

'Note - the routine below for handling the hmac requires the use of the SonicSSL.dll and
libeay.dll libraries.
'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered with
"regsvr32 sonicssl.dll"
```

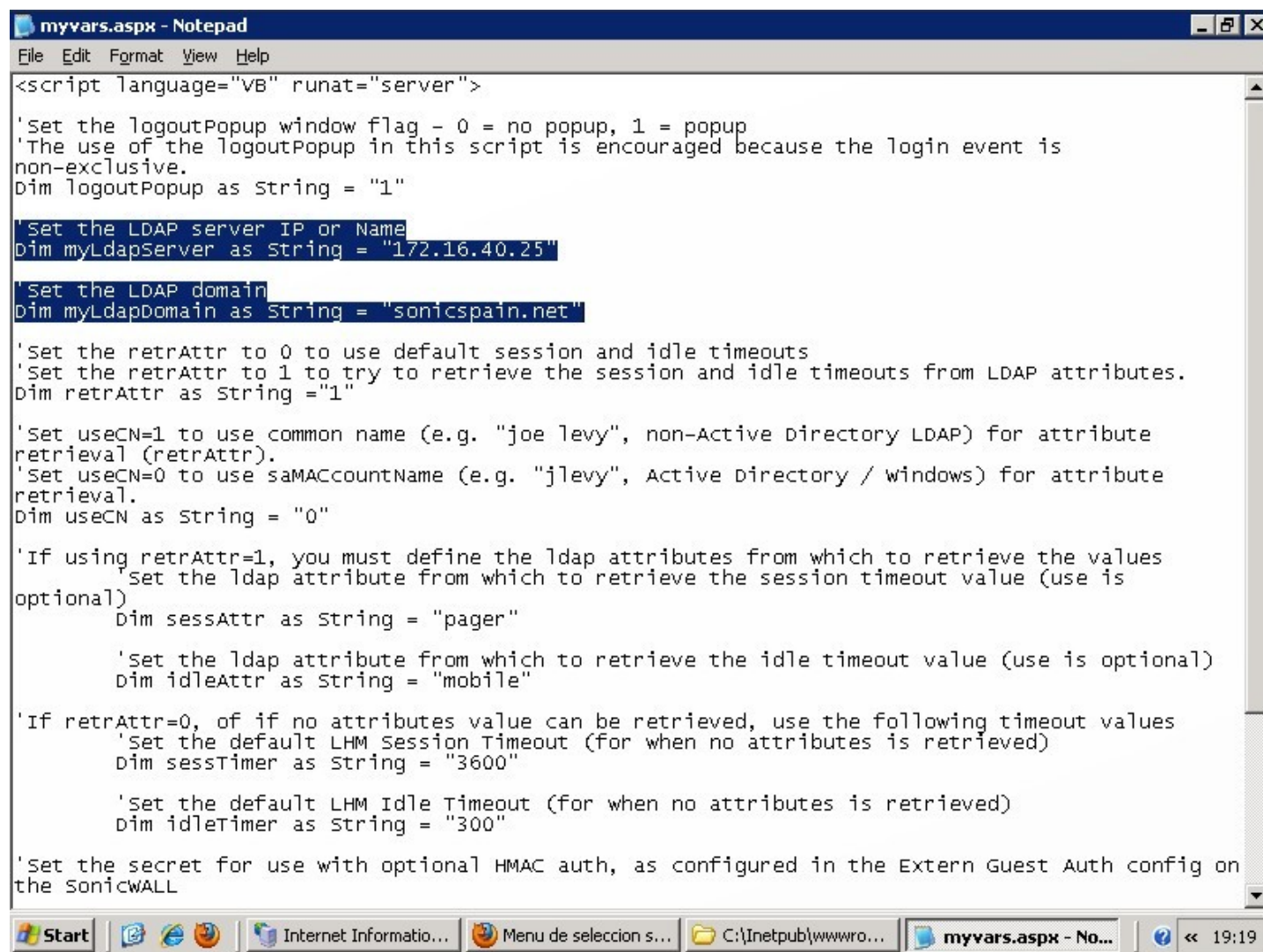

Tech Note

En la imagen de más abajo yo he escogido como ejemplo el script Accept, al que referencio en cada uno de los menús, pero con diferentes parámetros (?cc=n)



En cada uno de los scripts de ejemplo, también hay un fichero (myvars.aspx) que contiene algunas variables a las que se hace referencia desde el script principal (default.aspx). Este fichero variará ligeramente en función del script que hayamos escogido, pero en cualquier caso es conveniente revisarlo y adaptarlo a nuestro escenario. En la imagen de más abajo podemos ver un extracto del fichero myvars.aspx del script de ejemplo AD Auth:

Tech Note



```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LDAP server IP or Name
Dim myLdapServer as String = "172.16.40.25"

'Set the LDAP domain
Dim myLdapDomain as String = "sonicspain.net"

'Set the retrAttr to 0 to use default session and idle timeouts
'Set the retrAttr to 1 to try to retrieve the session and idle timeouts from LDAP attributes.
Dim retrAttr as String = "1"

'Set useCN=1 to use common name (e.g. "joe levy", non-Active Directory LDAP) for attribute
retrieval (retrAttr).
'Set useCN=0 to use samAccountName (e.g. "jlevy", Active Directory / windows) for attribute
retrieval.
Dim useCN as String = "0"

'If using retrAttr=1, you must define the ldap attributes from which to retrieve the values
optional)
    Dim sessAttr as String = "pager"

    'Set the ldap attribute from which to retrieve the idle timeout value (use is optional)
    Dim idleAttr as String = "mobile"

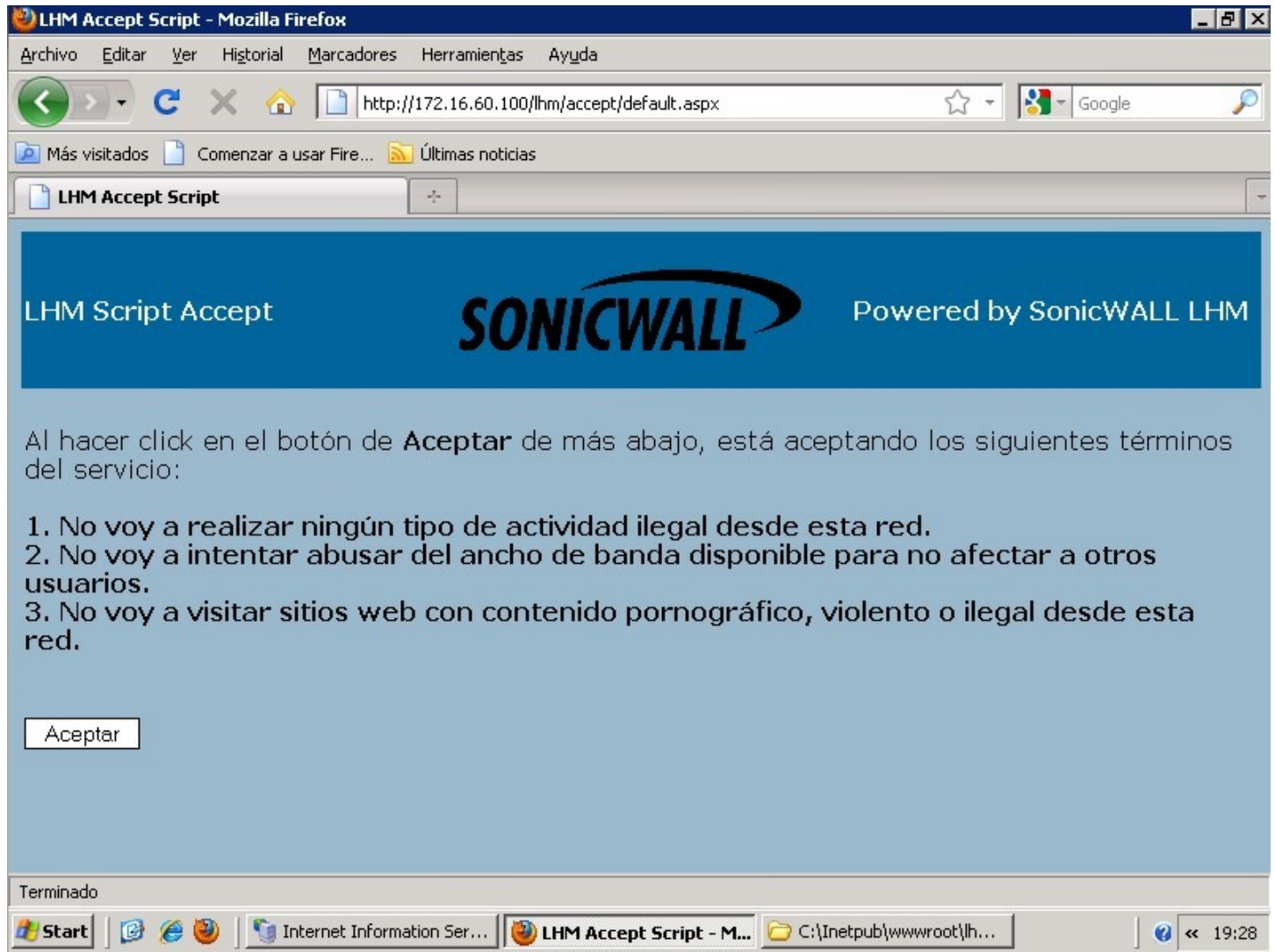
'If retrAttr=0, or if no attributes value can be retrieved, use the following timeout values
'Set the default LHM Session Timeout (for when no attributes is retrieved)
Dim sessTimer as String = "3600"

'Set the default LHM Idle Timeout (for when no attributes is retrieved)
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest Auth config on
the SonicWALL
```

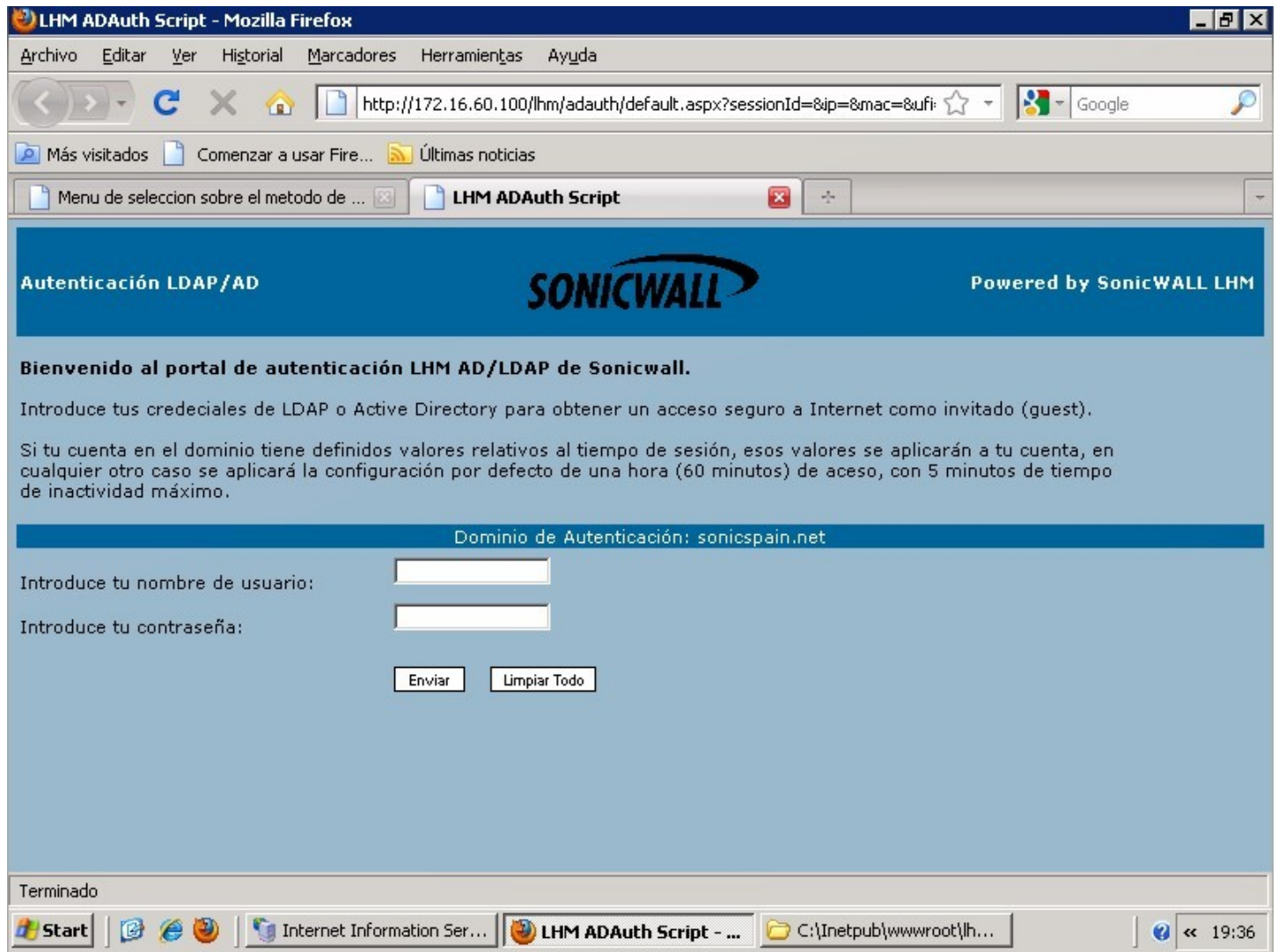
Ejemplos de Portales Cautivos

- Portal cautivo con normas de uso (disclaimer):



Tech Note

- Portal cautivo con autenticación contra servidor Active Directory (adauth):



Tech Note

- Portal cautivo con registro de usuario (Guestbook):

LHM Guestbook Script - Mozilla Firefox

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

http://172.16.60.100/lhm/guestbook/default.aspx?sessionId=&ip=&mac=8

Más visitados Comenzar a usar Fire... Últimas noticias

Menu de seleccion sobre el metodo de ... LHM Guestbook Script

LHM Guestbook **SONICWALL** Powered by SonicWALL LHM

Bienvenido al portal LHM Guestbook de Sonicwall. A cambio de tu información de contacto, así como tu permiso para ponernos en contacto contigo mientras estás en medio de una cena, te proporcionaremos **acceso seguro a Internet durante una hora de manera gratuita.**

Gracias por tu participación.

Introduce tu nombre completo:

Introduce tu dirección:

Introduce tu ciudad:

Introduce tu provincia:

Introduce tu código postal:

Introduce tu número de teléfono:

Introduce tu dirección de correo:

Introduce la URL de tu página web (opcional):

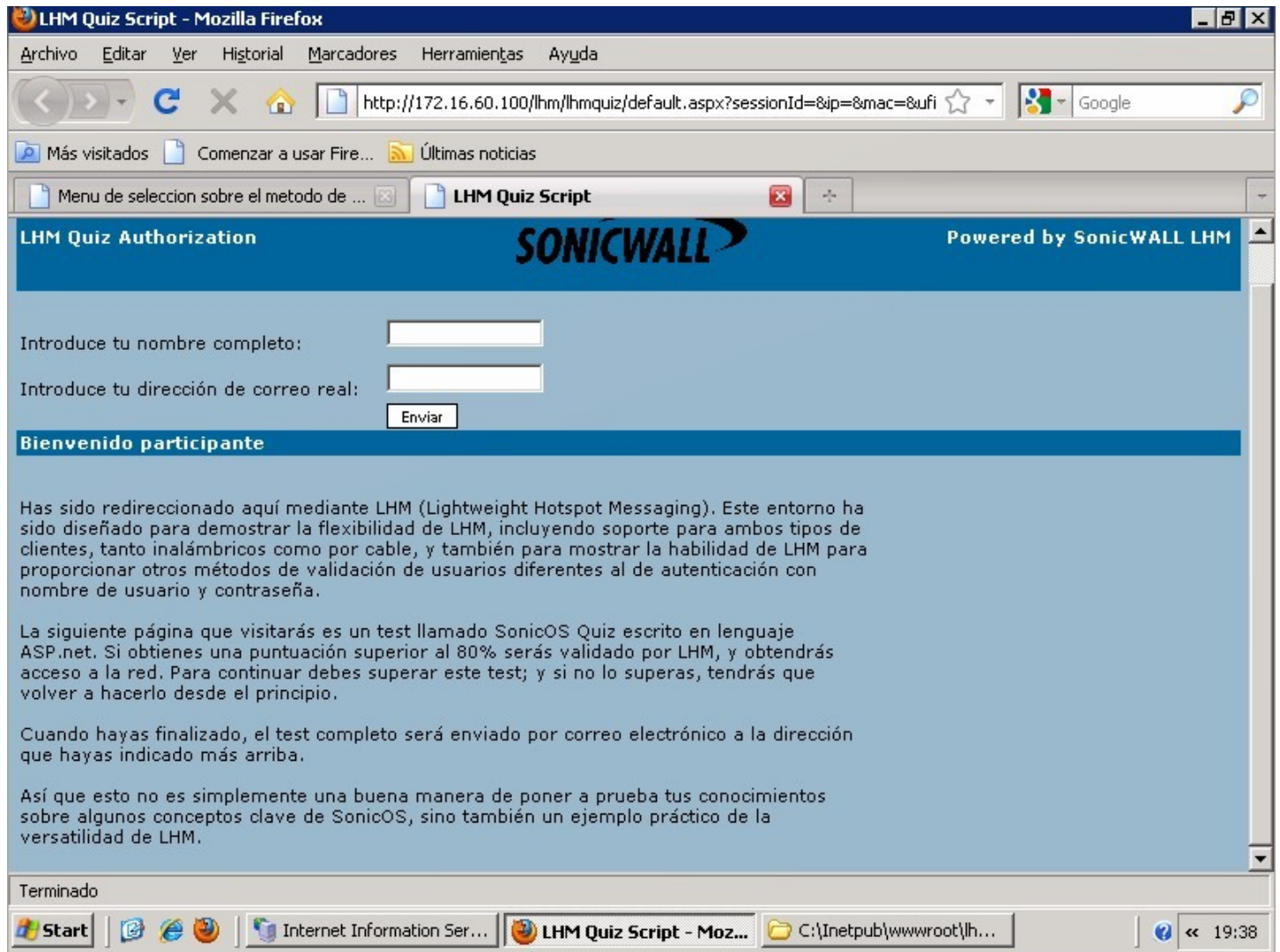
Introduce un comentario (opcional):

Terminado

Start Internet Information Ser... LHM Guestbook Scri... C:\inetpub\wwwroot\lhm... 19:37

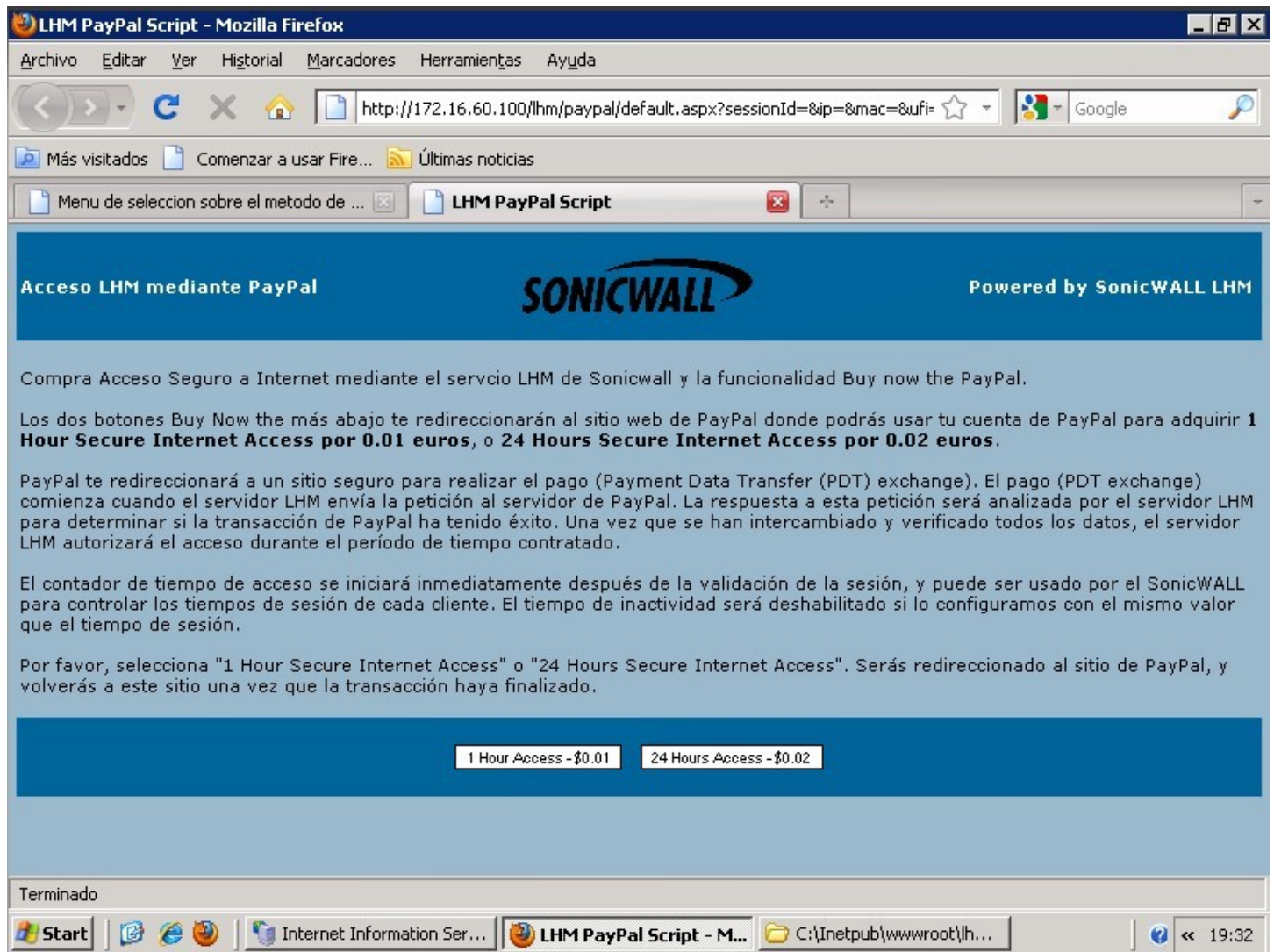
Tech Note

- Portal cautivo con examen (lhmquiz):



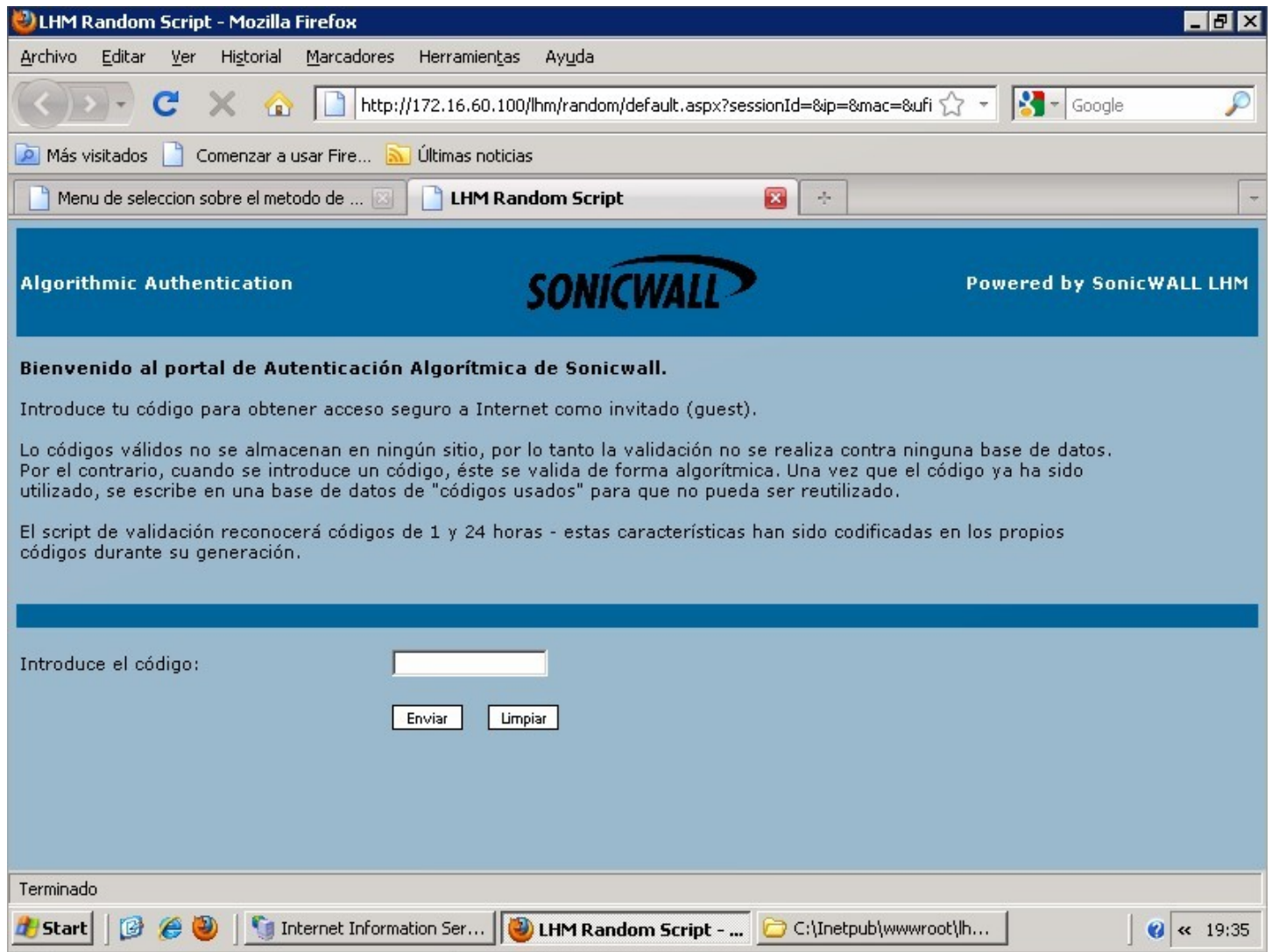
Tech Note

- Portal cautivo con acceso mediante pago a través de Paypal (paypal):



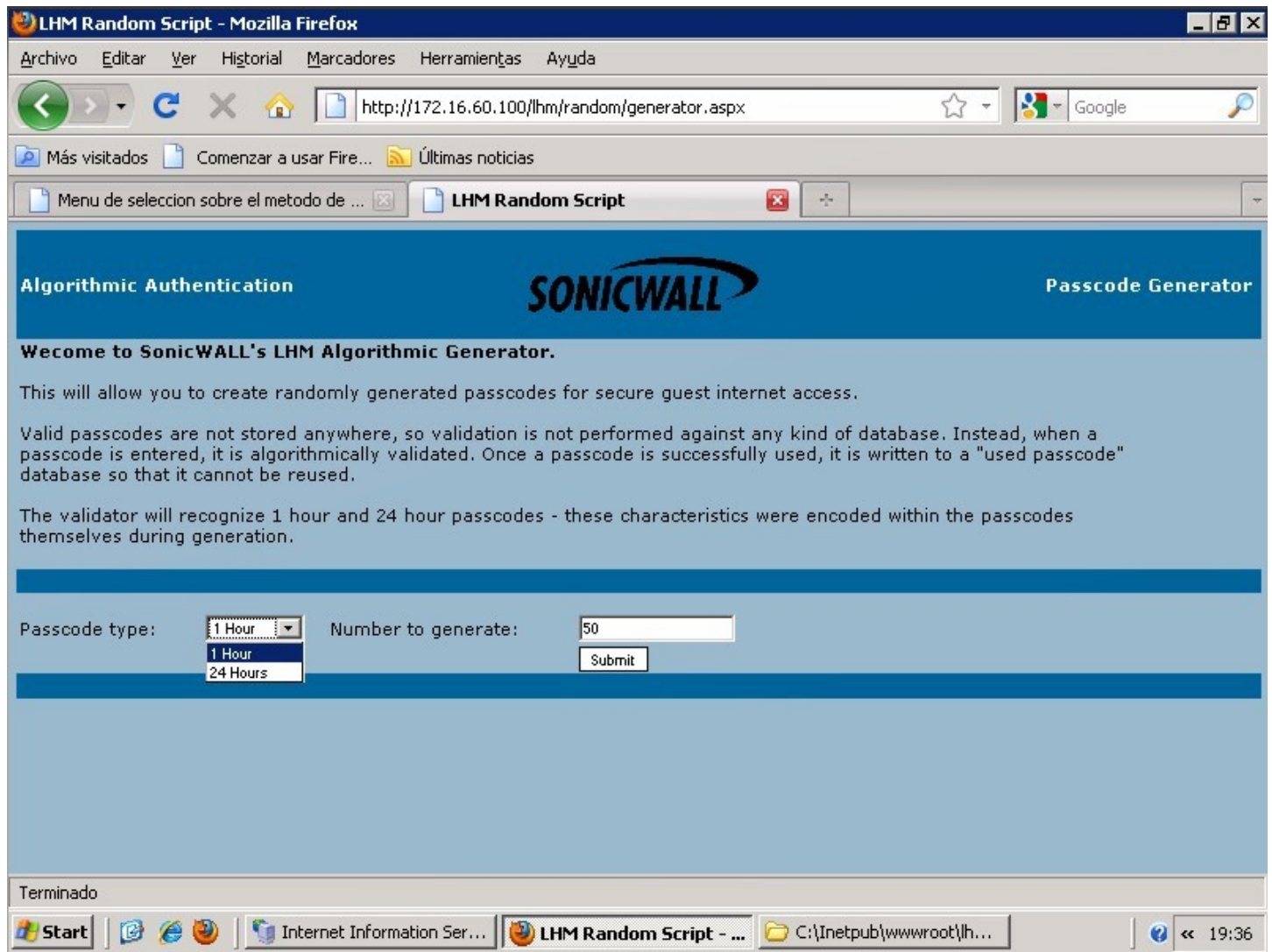
Tech Note

- Portal cautivo con generación aleatoria de claves (random):



Tech Note

- Script de generación de claves para el portal cautivo random (/generator.aspx):



Autor: Alex Vazquez

Fecha: 20/03/2011

Version 1

