DISICO

Instalación y Configuración RADIUS

Manual

¿Que es Radius?

Remote Authentication Dial In User Service. Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP.

- **Autenticación**
  - La confirmación de que el usuario es quien dice ser. La autenticación se realiza mediante la presentación de credenciales.
- **Autorización**
  - Permitir el acceso a determinados tipos de servicio o recursos.
- **Administración**
  - El seguimiento del consumo de recursos.

Como funciona RADIUS

Muchos ISP (proveedores de acceso a internet por dial up, DSL, cable módem, Ethernet, WiFi, etc.) requieren que se ingrese un nombre de usuario y contraseña para conectarse a la red. Antes de que el acceso a la red sea concedido, los datos de acceso son pasados por un dispositivo NAS (Network Access Server) sobre un protocolo de capa de enlace (como PPP, para muchos dialups y DSL), luego hacia un servidor RADIUS sobre un protocolo RADIUS. El servidor RADIUS chequea que esa información sea correcta usando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP, parámetros L2TP, etc.

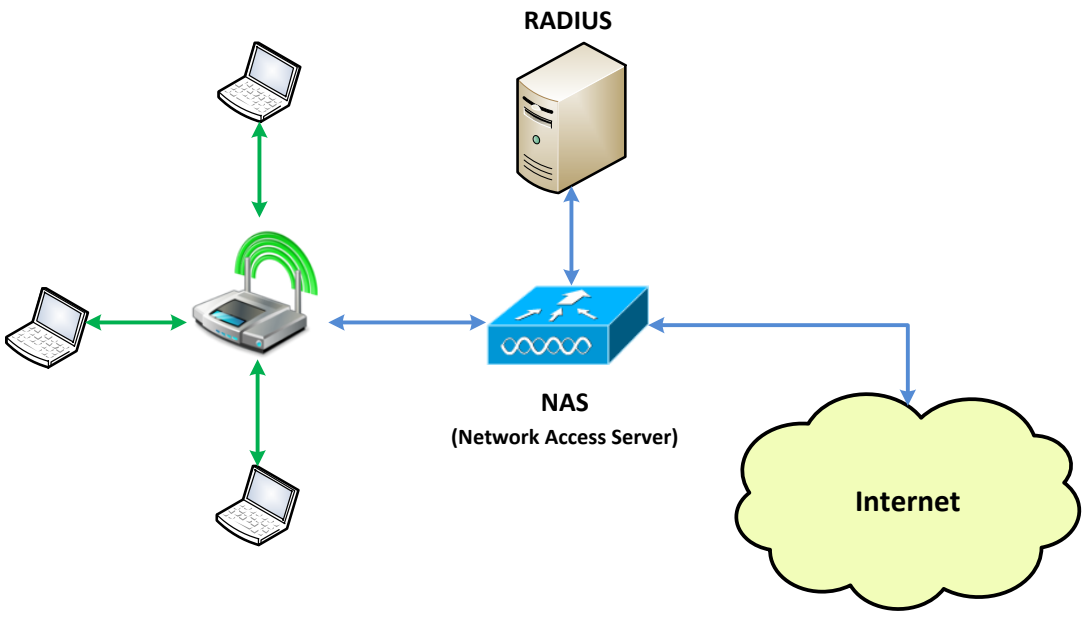


Ilustración 1: Esquema de funcionamiento

Esquema de Implementación

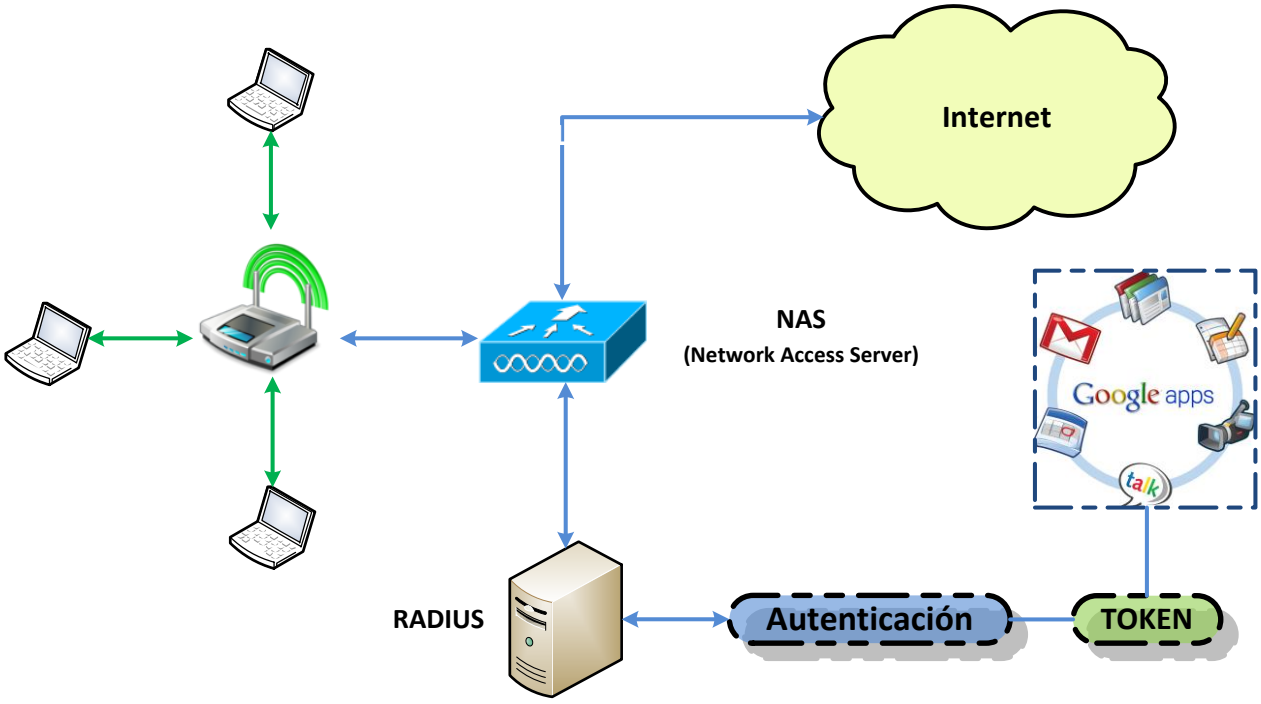


Ilustración 2: Esquema implementación

Instalación y configuración de FreeRADIUS

- **Instalación:**
  - Para instalar FreeRADIUS deberá de dirigirse a la siguiente dirección:
    - **# cd /usr/ports/net/freeradius2/**
  - Luego deberá de ejecutar el siguiente comando:
    - **# make config**
      - *enable-LDAP*
      - *enable-MySQL*
  - Finalmente se procede a instalar la aplicación

 # make && make install && make clean

- **Configuración Test:**
  - Posterior a la instalación de FreeRadius deberá de configurar el archivo **users** como se muestra a continuación:
    - Hacer una copia del archivo original
      - **# cp /usr/local/etc/raddb/users /usr/local/etc/raddb/users_original**
    - Ingresar usuario de prueba para FreeRADIUS
      - **#ee /usr/local/etc/raddb/users**
        - **jnnader Cleartext-Password := "jn_javac"**
      - **#ee /etc/rc.conf**
        - **radiusd_enable="YES"**
      - **#radiusd –X**
      - **#radtest jnnader jn_javac 127.0.0.1 0 testing123**
        - **Access-Accept**

- **Configuración Script Perl**
  - Posterior a las pruebas de usuario se deberá de editar el archivo example.pl para permitir la autenticación por cuentas Google Apps
    - Hacer una copia del archivo original
      - # **cp /usr/local/etc/raddb/example.pl /usr/local/etc/raddb/example.pl.resp_original**
    - Agregar código de autenticación, para ello deberá reemplazar el bloque de la función authentica te como se muestra a continuación.
      - **#ee /usr/local/etc/raddb/example.pl**
        - **sub authenticate {**
        -
        - **my $response = $lwp_object->post($url,**
        - **['accountType' => 'HOSTED',**
        - **'Email' => $RAD_REQUEST{'User-Name'}.'@uv.cl',**
        - **'Passwd' => $RAD_REQUEST{'User-Password'},**
        - **'service' => 'apps'**
        - **]**
        - **);**
        -
        - **if($response->is_success)**
        - **{**

- **$RAD_REPLY{'h323-credit-amount'} = "100";**
- **return RLM_MODULE_OK;**
- **}**
- **else**
- **{**
- **$RAD_REPLY{'Reply-Message'} = "Denied access by rlm_perl function".$RAD_REQUEST{'User-Name'};**
- **return RLM_MODULE_REJECT;**
- **}**
- **}**

- Para permitir la autenticación de los usuarios mediante perl editar el archivo de configuración user
  - #ee /usr/local/etc/raddb/users
    - **DEFAULT Auth-Type = Perl**
- Habilitar perl en default y inner-tunnel
  - #ee /usr/local/etc/raddb/site_enable/default
    - **authorize {**
    - **#preprocess**
    - **#chap**
    - **#mschap**
    - **#digest**
    - **#suffix**
    - **eap**
    - **files**
    - **perl**
    - **expiration**
    - **logintime**
    - **pap**
    - **}**
    -
    - **authenticate {**
    - **Auth-Type PAP {**
    - **pap**
    - **}**
    - **Auth-Type CHAP {**
    - **chap**
    - **}**

- **perl**
- **Auth-Type MS-CHAP {**
- **mschap**
- **}**
- **digest**
- **unix**
- **eap**
- **}**
-
- **accounting {**
- **detail**
- **unix**
- **radutmp**
- **perl**
- **exec**
- **}**

- ee /usr/local/etc/raddb/site_enable/inner-tunneling
  - **authorize {**
  -
  - **#chap**
  - **#mschap**
  - **#suffix**
  - **update control {**
  - **Proxy-To-Realm := LOCAL**
  - **}**
  - **eap**
  - **files**
  - **perl**
  - **expiration**
  - **logintime**
  - **pap**
  - **}**
  -
  - **authenticate {**
  - **Auth-Type PAP {**
  - **pap**
  - **}**
  -

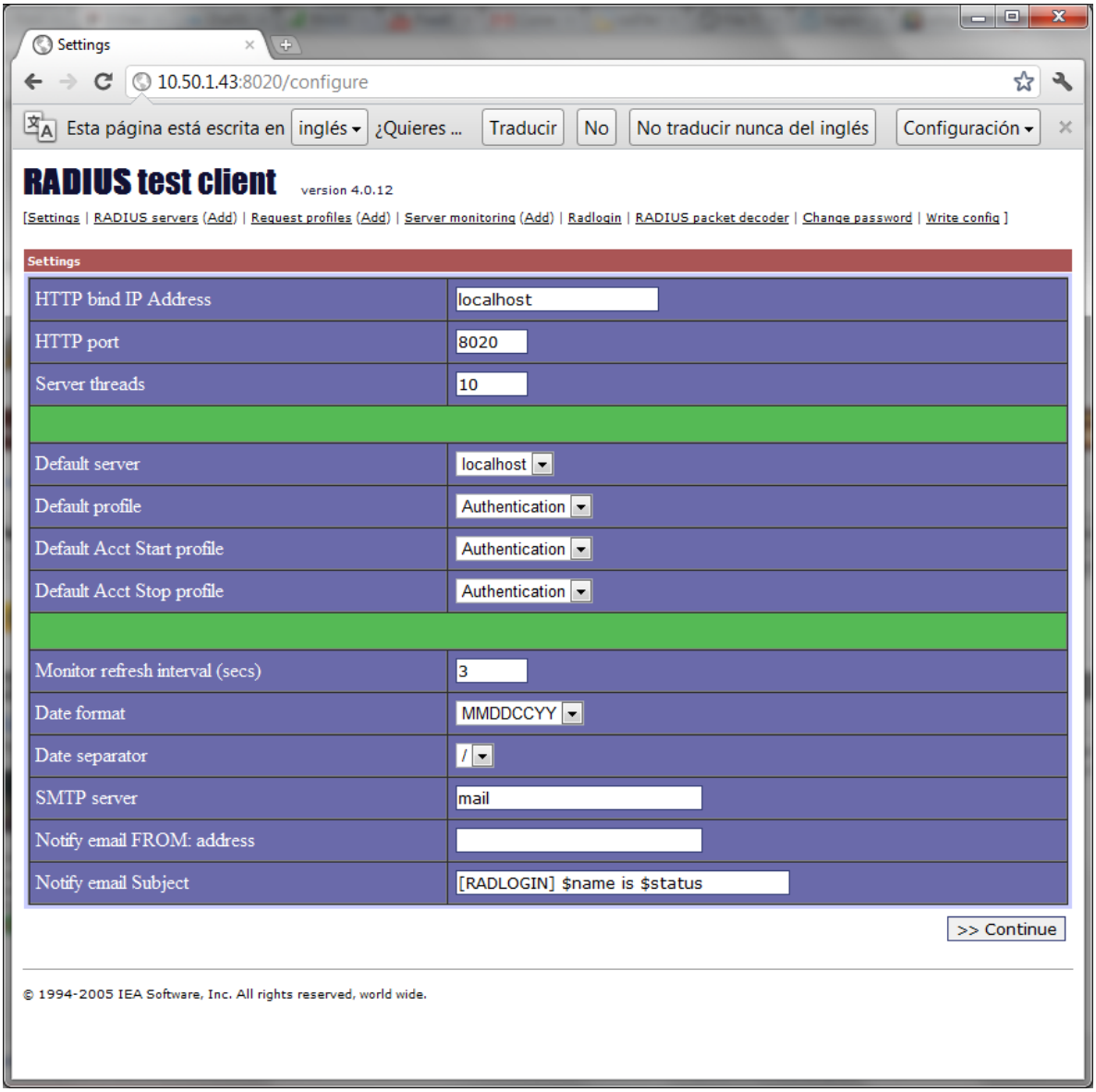
- **Auth-Type CHAP {**
- **chap**
- **}**
- **Auth-Type Perl {**
- **perl**
- **}**
-
-
- **Auth-Type MS-CHAP {**
- **mschap**
- **}**
- **unix**
- **eap**
- **}**

- Instalar modulos perl mediante cpan
  - #cpan> Install LWP::UserAgent
  - #cpan> Install LWP::Protocol::https
- Pruebas mediante radius con googleapps
  - /usr/local/bin/radtest nader128 mypassword 127.0.0.1 0 testing123
- Verificar la carga del script
  - #ee /usr/local/etc/raddb/modules/perl
    - perl {
    - #
    - # The Perl script to execute on authorize, authenticate,
    - # accounting, xlat, etc. This is very similar to using
    - # 'rlm_exec' module, but it is persistent, and therefore
    - # faster.
    - #
    - module = ${confdir}/example.pl

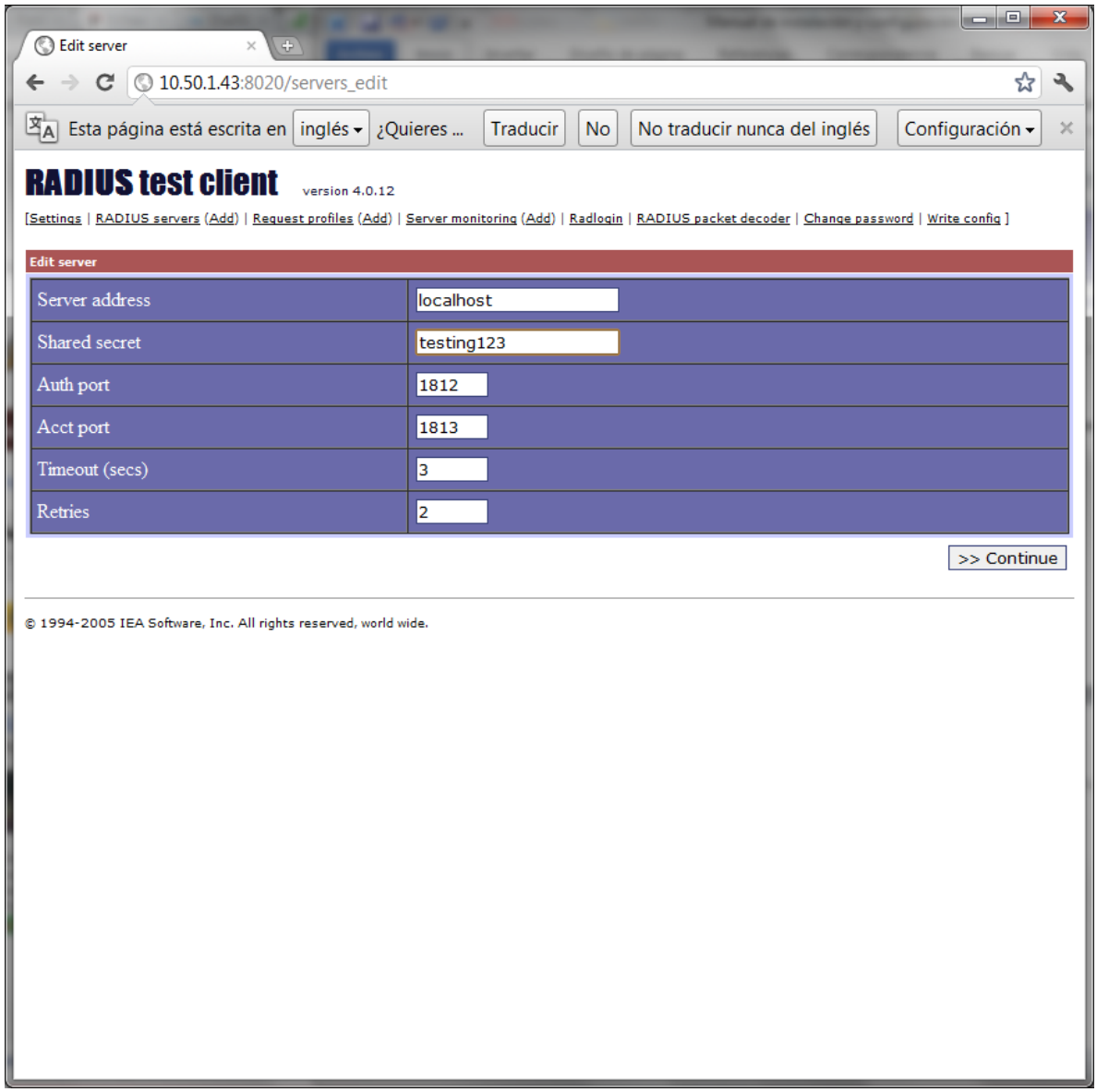
Instalación y Configuración de Radlogin from IE

- **Qué es**
- **Instalación**
    - Deberá descargar el paquete de radlogin desde http://www.iea-software.com/ftp/radiusv5/freebsd/radlogin4_freebsd.tar.gz, una vez descargado el archivo se procederá con su instalación
        - #tar –xvf radlogin4_freebsd.tar.gz
        - # cd /usr/ports/misc/compat4x
        - #make install clean
        - # cd /usr/ports/misc/compat5x
        - #make install clean
        - #cd /usr/local/etc/radiuslogin
        - #./install.pl
            - Teclear C y luego enter
        - Iniciar el servicio radlogin
            - #/usr/local/radius/radlogin
        - Ingresar al navegador web para ver el servicio
            - Ip_maquina:8020

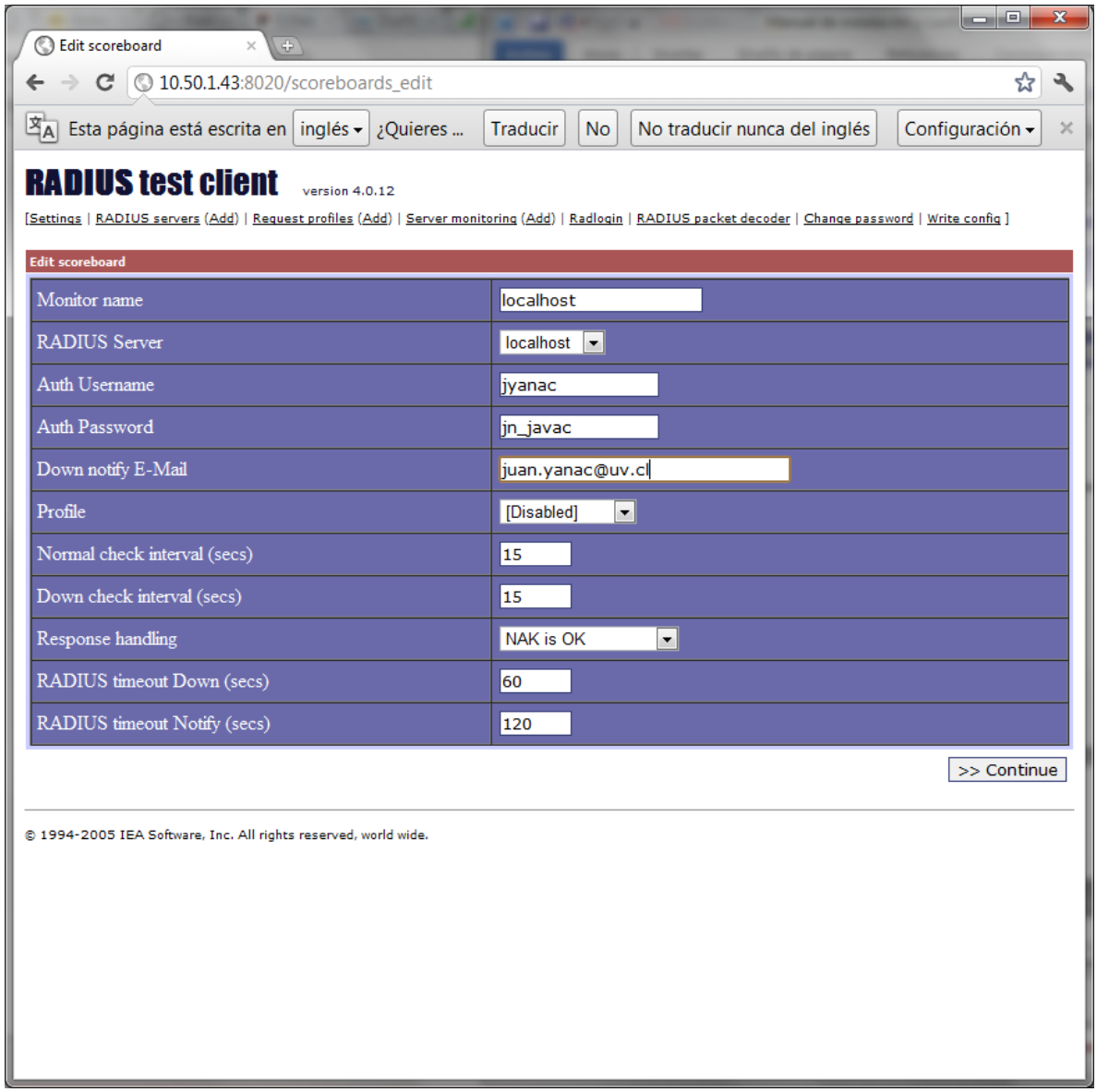
- **Configuración**
  - Ingresar a http://10.50.1.43:8020
    - Configurar Settings

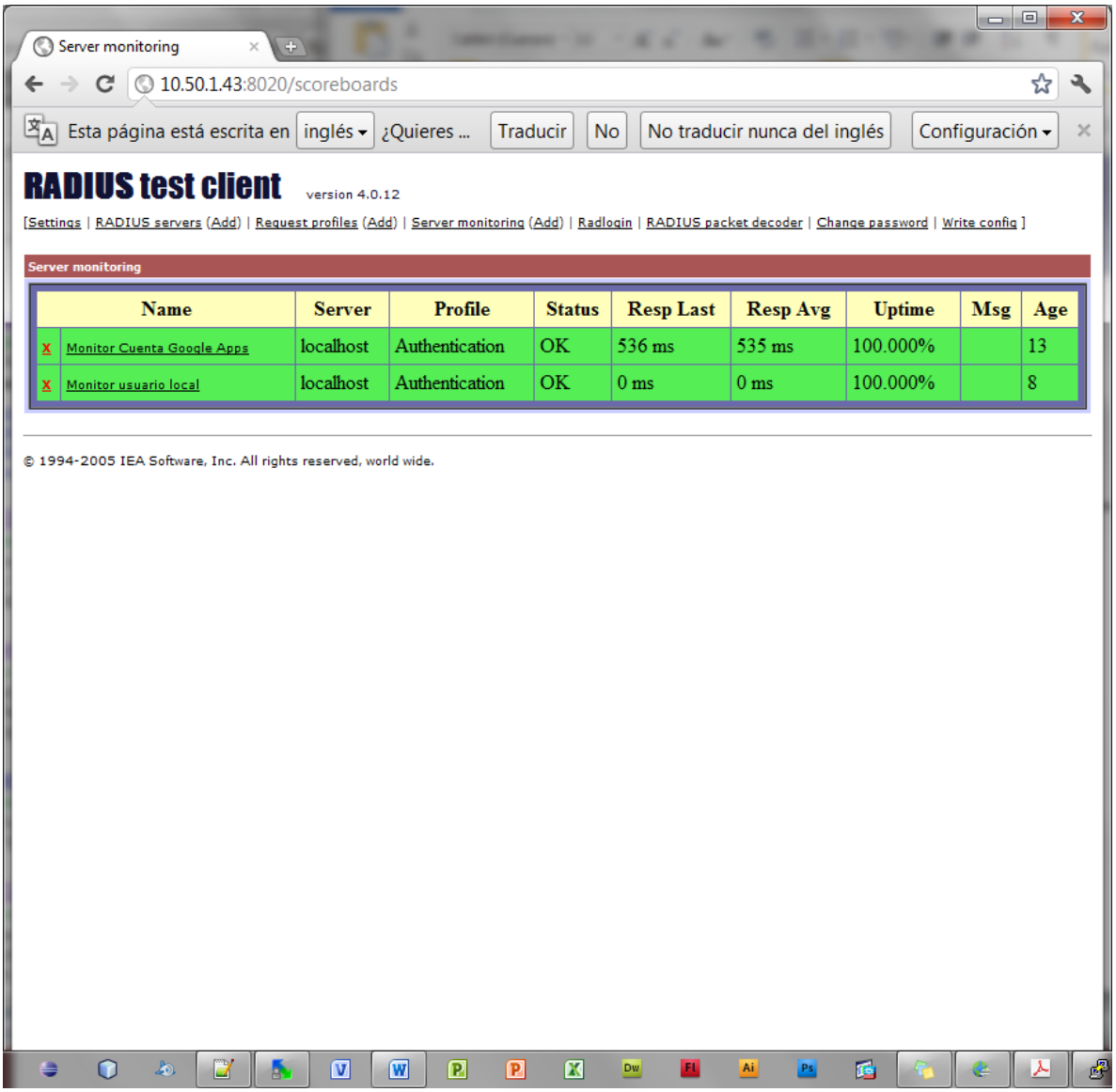


- **Radius Server**

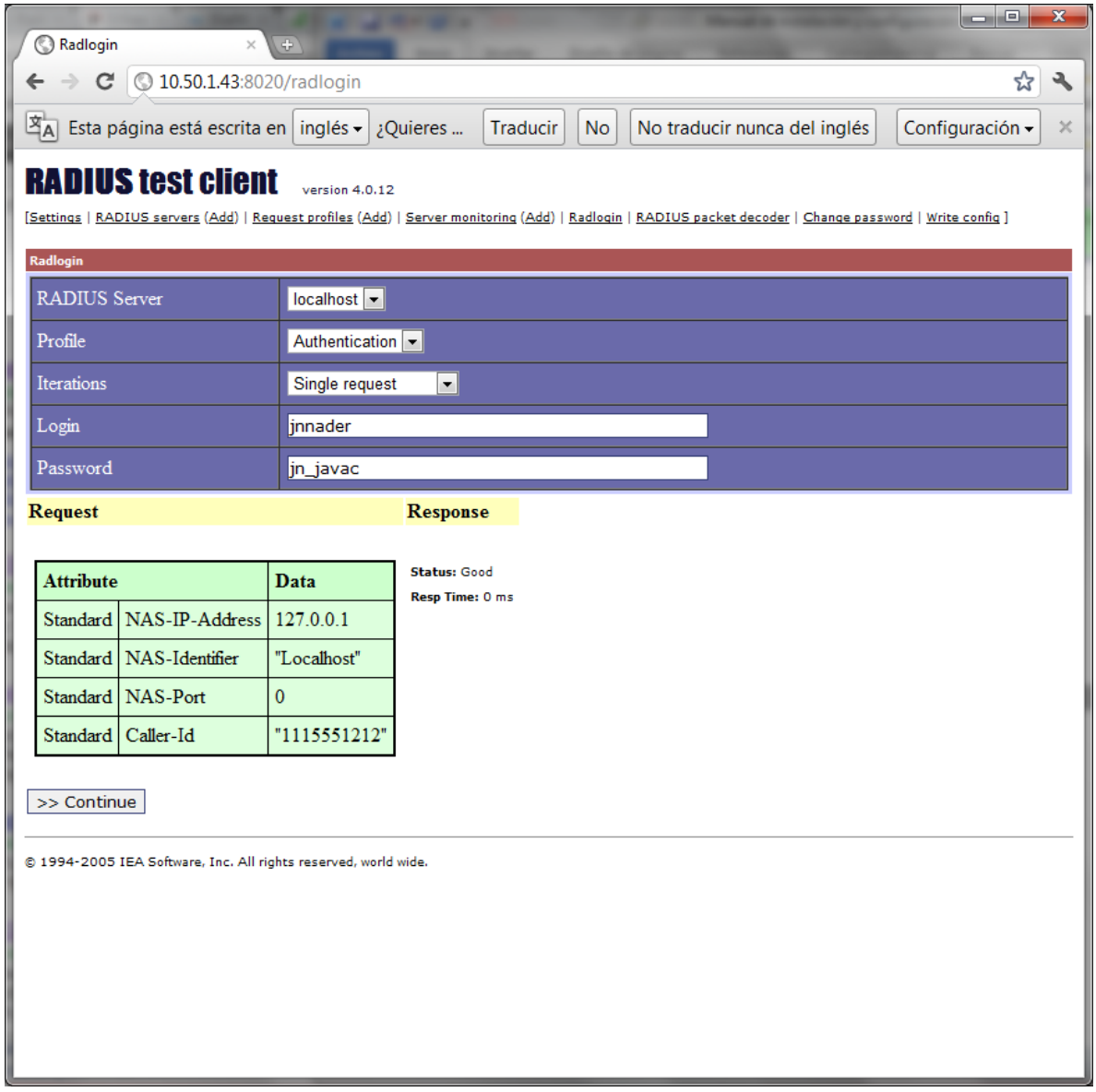


- **Server monitoring**




Server monitoring
10.50.1.43:8020/scoreboards
Esta página está escrita en inglés ¿Quieres ... Traducir No No traducir nunca del inglés Configuración
RADIUS test client version 4.0.12
[Settings | RADIUS servers (Add) | Request profiles (Add) | Server monitoring (Add) | Radlogin | RADIUS packet decoder | Change password | Write config]
Server monitoring
Name Server Profile Status Resp Last Resp Avg Uptime Msg Age
x Monitor Cuenta Google Apps localhost Authentication OK 536 ms 535 ms 100.000% 13
x Monitor usuario local localhost Authentication OK 0 ms 0 ms 100.000% 8
© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

- **Radlogin**


Radlogin
10.50.1.43:8020/radlogin
Esta página está escrita en inglés ¿Quieres ... Traducir No No traducir nunca del inglés Configuración
RADIUS test client version 4.0.12
[Settings | RADIUS servers (Add) | Request profiles (Add) | Server monitoring (Add) | Radlogin | RADIUS packet decoder | Change password | Write config]
Radlogin
RADIUS Server localhost
Profile Authentication
Iterations Single request
Login jnnader
Password jn_javac
Request
Response
Attribute Data
Standard NAS-IP-Address 127.0.0.1
Standard NAS-Identifier "Localhost"
Standard NAS-Port 0
Standard Caller-Id "1115551212"
Status: Good
Resp Time: 0 ms
>> Continue
© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

Para monitorear otro freeradius, se beberá de habilitar el cliente en el server que se quiere monitorear

A – B

Donde A es el server

Donde B es el ciente

En B deberá editar el archivo clients.conf y agregar las siguiente línea

```
client 10.50.1.43{ //ip del server – Permite conexión
  secret         = testing123
 shortname       = localhost
}
```

Para monitorea con la ip del equipo agregar client localhost {

```
 # Allowed values are:
 # dotted quad (1.2.3.4)
 # hostname    (radius.example.com)
#ipaddr = 127.0.0.1
 ipaddr  = 10.50.1.43
```

Para habilitar el correo instalar snmp en el equipo