SSL EXPLORER – OPENVPN ALS –ADITO VPN

CONENIDOS

1. INTRODUCCIÓN

En este artículo revisaremos la solución Opensource OpenVPN ALS, una bifurcación del SSL Explorer, software que era Opensource y que fue adquirido por Barracuda Networks.

Lo primero es señalar qué puede aportar Open VPN a un entorno empresarial:

- Conexión a la intranet corporativa desde una red externa
- Conexión al servidor de ficheros corporativo desde una red externa
- Conexión para administradores a los servidores del Data Center desde una red externa (vía Putty, WinSCP, RDP o VNC)
- Control Remoto de Equipos de fuera de la red corporativa para el personal de Soporte, iniciado a petición del usuario
- Acceso a determinados servicios internos (mensajería interna) pero cambiando el punto de conexión de la aplicación cliente

Resumiendo, estamos haciendo accesibles los recursos internos de la empresa, de forma segura, a usuarios externos (tele-trabajadores, usuarios móviles, colaboradores, etc.) sin necesidad de instalar ningún software en los equipos. Todo esto sin pagar un duro en licencias de software.

Un aspecto importante de OpenVPN es que valida a los usuarios contra Active Directory (una de las Bases de Datos de usuarios más extendida hoy en día), de forma que lo usuarios no tienen que gestionar otra *password* para acceder a este servicio, y los administradores pueden usar los grupos de Active Directory para controlar el acceso de los usuarios a los recursos publicados, evitando tener que descentralizar la gestión de los accesos a los recursos. Este aspecto es muy importante, ya que si un usuario se da de baja en la empresa, bastaría con darlo de baja en Active Directory para evitar que pueda seguir accediendo desde fuera a la información corporativa. Con múltiples repositorios de usuarios suele suceder que se nos olvida dar de baja los usuarios de alguno de estos repositorios, con el consiguiente agujero de seguridad que se crea…

A continuación se detallan los pasos que hay que seguir para tener este producto listo y funcionando en su organización, y para configurar los servicios más fundamentales, con los cuales empezar a dar acceso a usuarios externos a los recursos internos de la empresa.

Hemos realizado una aportación a la comunidad que consideramos importante, en forma de extensión. Se trata de una extensión que permite publicar aplicaciones para que los usuarios que están fuera de la red corporativa puedan solicitar una sesión de control remoto al personal de Help Desk, que está dentro de la red corporativa. Para ello nos hemos basado en el software UltraVNC, también Opensource, y en una extensión que viene por defecto con Adito y que permite hacer lo contrario (tomar control remoto desde fuera de la red interna a un PC de la red interna). Para nosotros resultaba más importante el inverso, de cara a dar soporte a nuestros usuarios móviles, y por eso hemos desarrollado la extensión.

2. INSTALACIÓN

Instalación de Ubuntu

Instalaremos un servidor Linux, en este caso hemos elegido Ubuntu, como podríamos haber elegido CentOS, ambas soluciones Opensource y con coste en licencias igual a cero.

Concretamente hemos instalado Ubuntu 10.04 LTS

Configuración proxy en apt-get

```
administrador@srvv-ubuntu:/etc/apt$ more apt.conf
Acquire::http::Proxy "http://proxyuser:password@proxy.acme.es:8080";
```

Además de esto editamos `/etc/bash.bashrc`:

```
export http_proxy=http://username:password@proxyserver.net:port/
export ftp_proxy=http://username:password@proxyserver.netport/
```

Instalación de java

```
sudo apt-get install sun-java6-bin sun-java6-jdk
```

En Ubuntu 10.04 por defecto esto no funcionará, por la siguiente razón:

Sun Java moved to the Partner repository

For Ubuntu 10.04 LTS, the `sun-java6` packages have been dropped from the Multiverse section of the Ubuntu archive. It is recommended that you use `openjdk-6` instead.

If you can not switch from the proprietary Sun JDK/JRE to OpenJDK, you can install `sun-java6` packages from the Canonical Partner Repository. You can configure your system to use this repository via command-line:

```
    add-apt-repository "deb http://archive.canonical.com/ lucid partner"
```

Además de esto des-comentamos las líneas siguientes en el `/etc/apt/sources.list`

```
## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
deb http://archive.canonical.com/ubuntu lucid partner
deb-src http://archive.canonical.com/ubuntu lucid partner
```

Configurar Ubuntu para que use el JAVA de SUN y no el OpenJDK

```
sudo update-alternatives --config java
There are 2 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                       Priority   Status
------------------------------------------------------------
* 0            /usr/lib/jvm/java-6-openjdk/jre/bin/java   1061      auto mode
  1            /usr/lib/jvm/java-6-openjdk/jre/bin/java   1061      manual mode
  2            /usr/lib/jvm/java-6-sun/jre/bin/java       63        manual mode

Press enter to keep the current choice[*], or type selection number: 2
update-alternatives: using /usr/lib/jvm/java-6-sun/jre/bin/java to provide /usr/bin/java (java) in manual mode.
```

Instalación apt

```
sudo apt-get install apt-file
sudo apt-file update
```

Instalación de ant

```
sudo apt-get install ant
```

Falla la descarga de algunos componentes, por lo que hacemos lo siguiente:

```
sudo apt-get install ant --fix-missing
```

Instalación de Adito

Descomprimir el zip en un directorio.

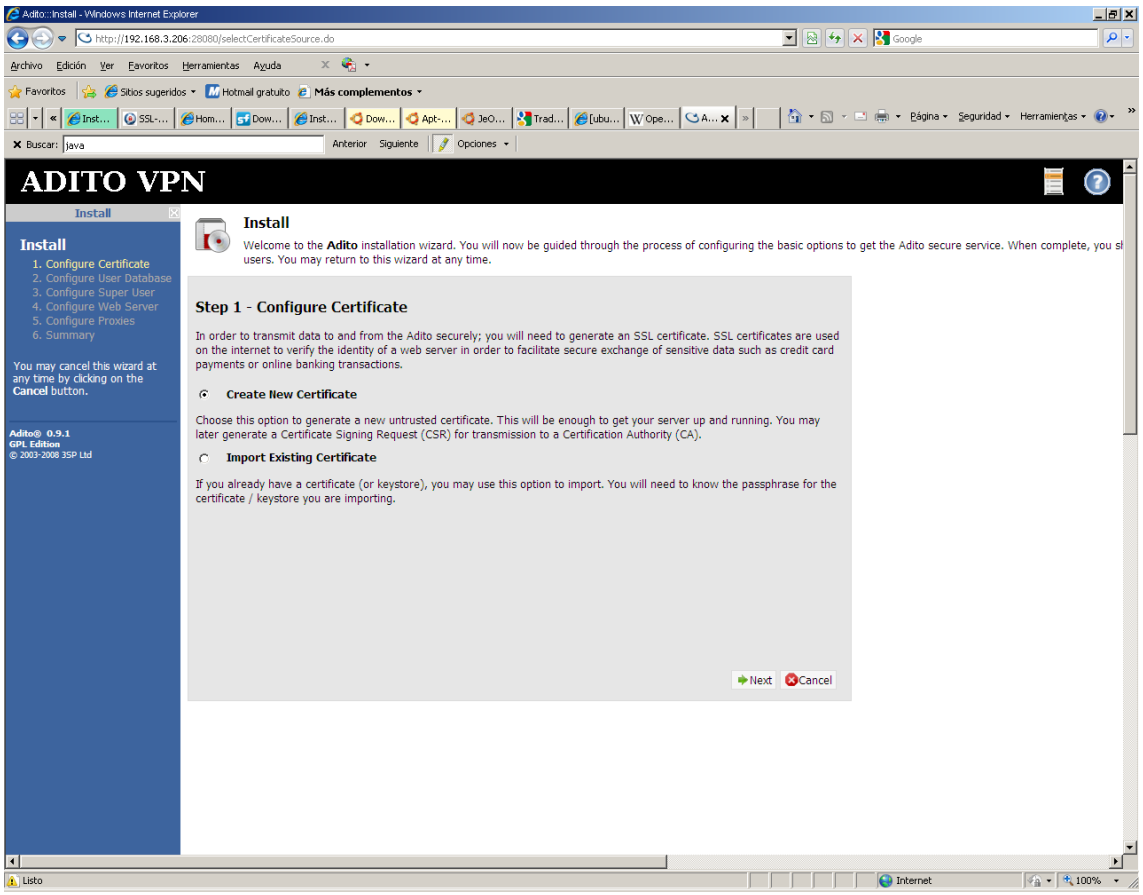
Nos vamos a ese directorio y ejecutamos:

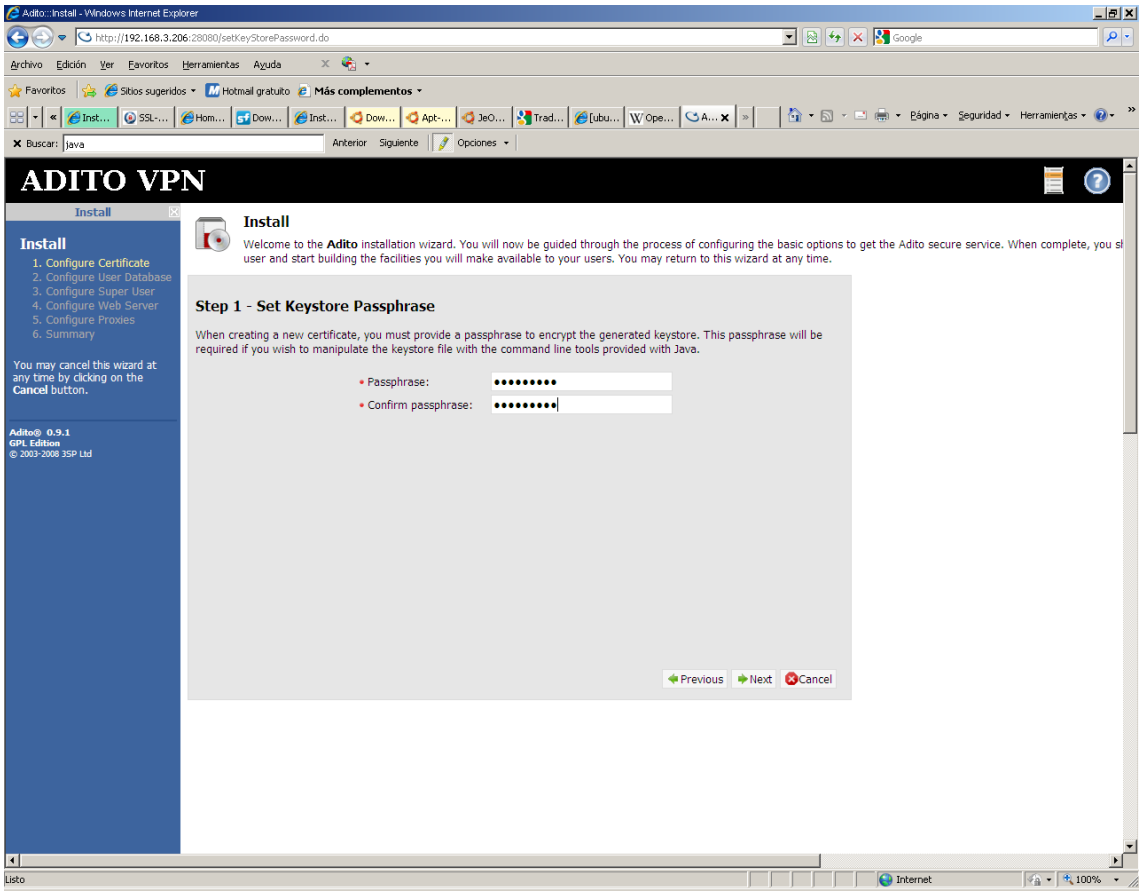
```
sudo apt-get install ant
```

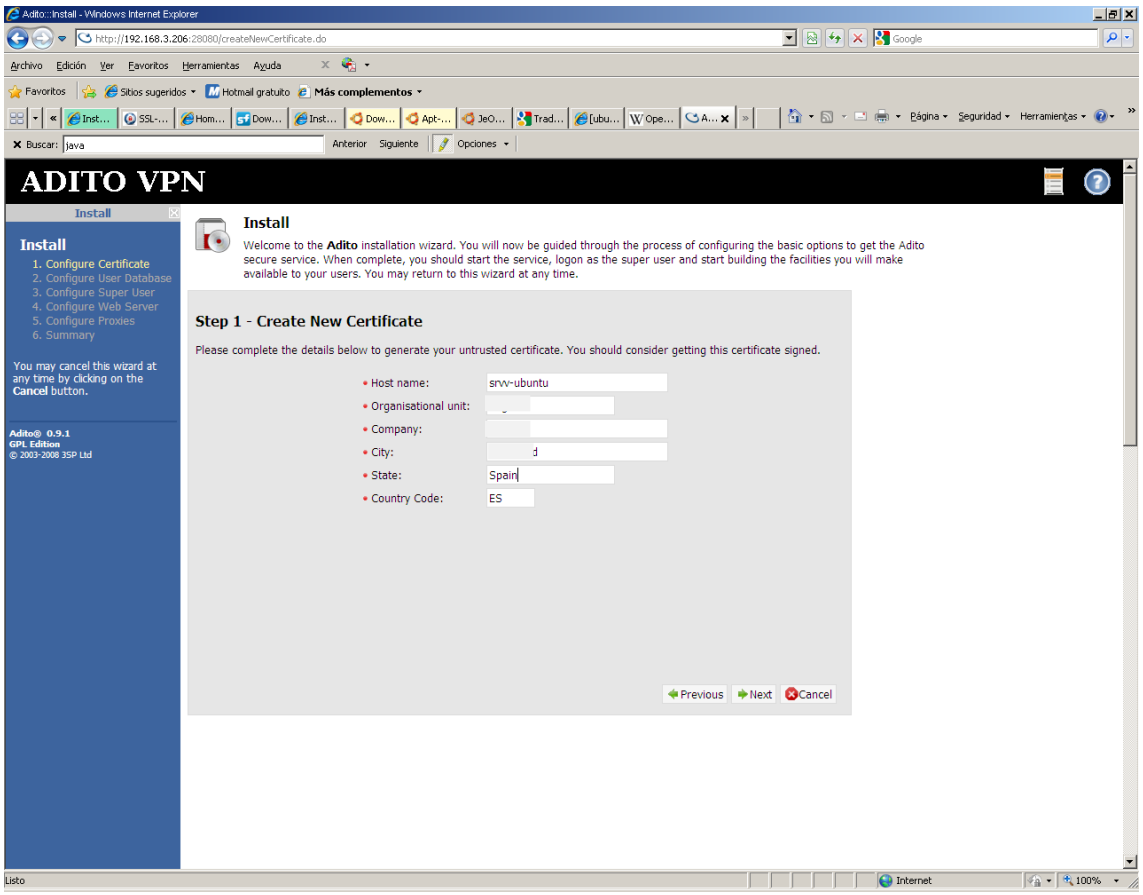
Nos conectamos vía WEB: http://srvv-ubuntu:20080

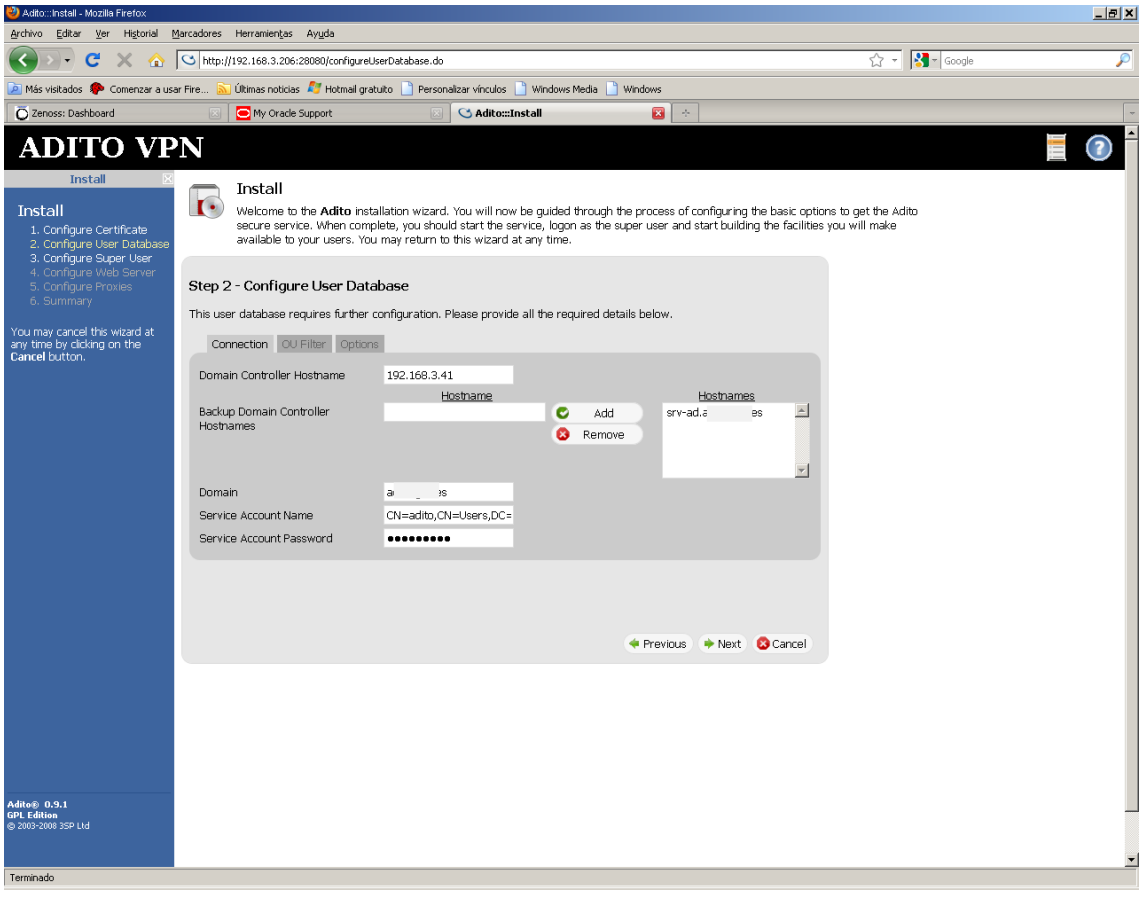
Configuración de Adito

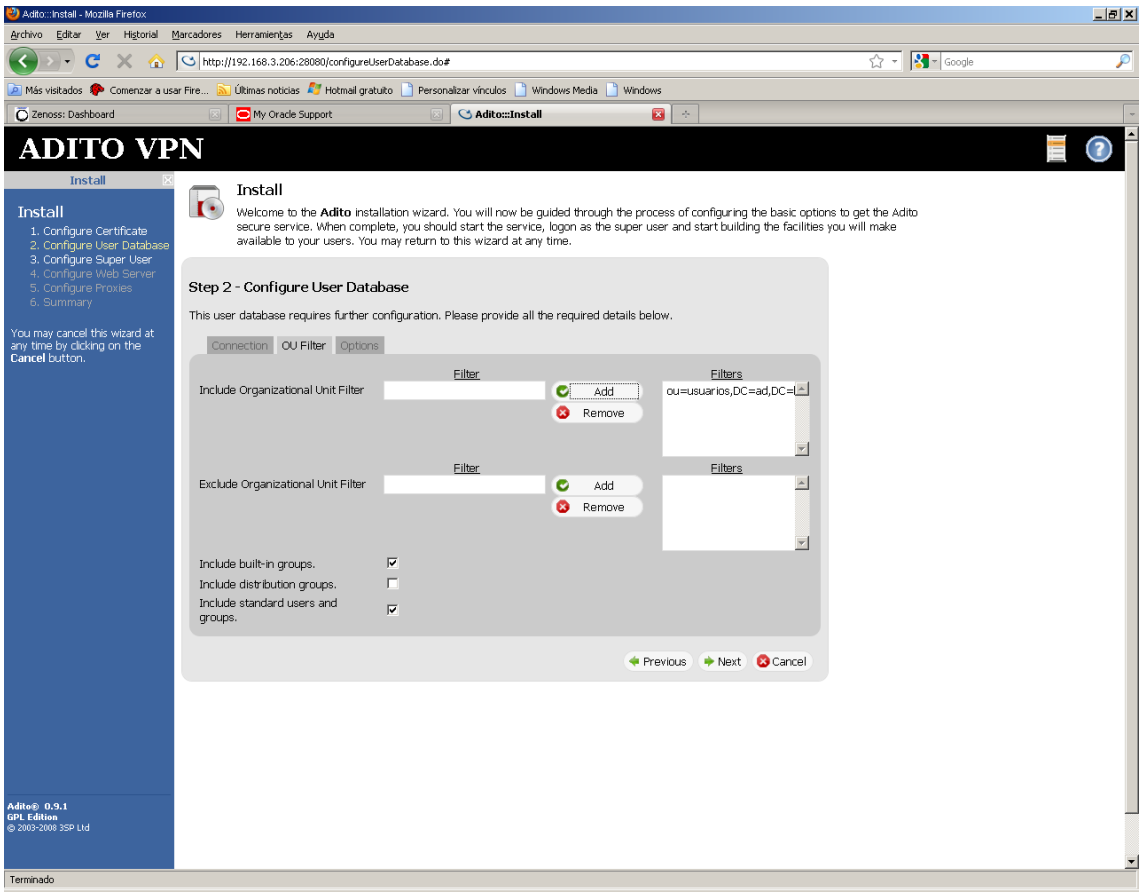
Una vez instalado Adito, tenemos que conectarnos con el navegador para realizar la configuración (Configuración del Certificado Digital, método de autenticación, etc). En nuestro caso hemos elegido las opciones básicas de configuración, salvo en lo que se refiere a la B.D. de usuarios. En este caso, hemos optado por usar la B.D. corporativa (Active Directory de Microsoft). Nos ha dado un poco de guerra pero finalmente hemos conseguido que los usuarios se autentiquen contra esta base de datos.

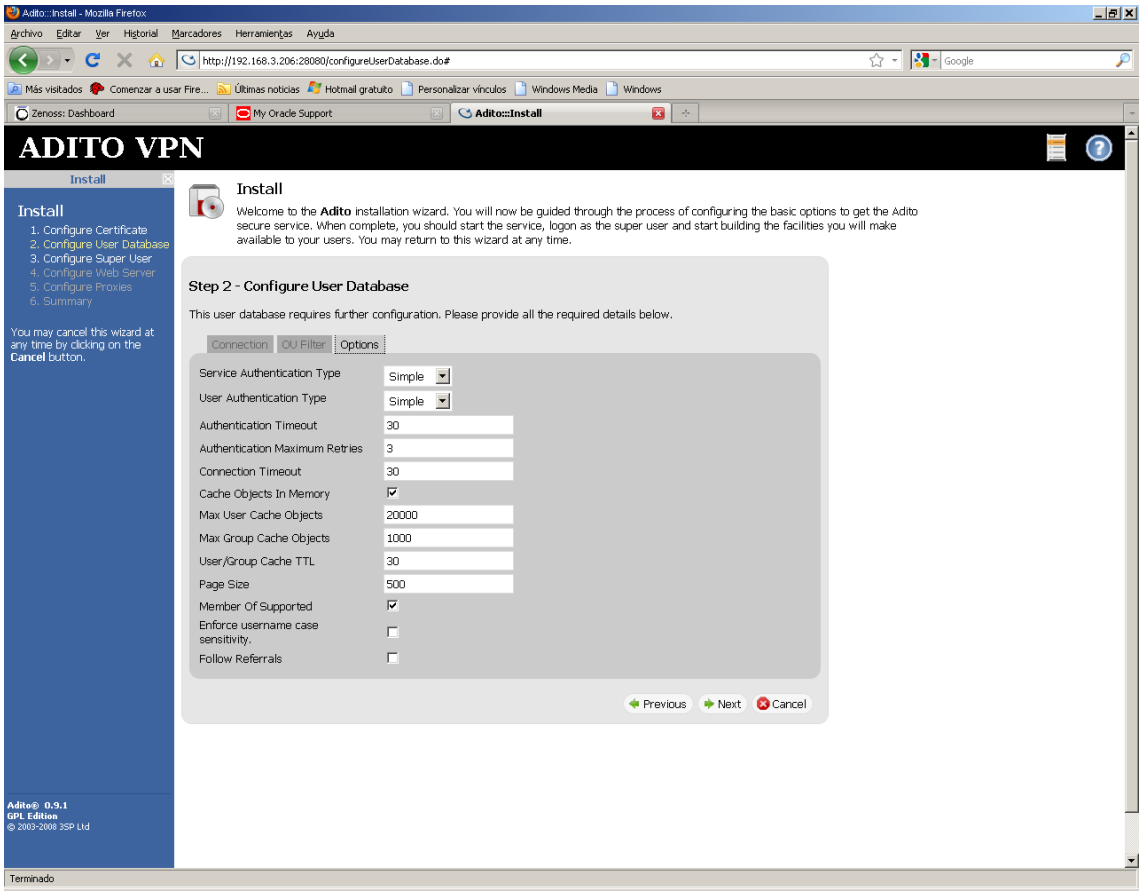

Adito::Install - Windows Internet Explorer
http://192.168.3.206:28080/selectCertificateSource.do
ADITO VPN
Install
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you sh
users. You may return to this wizard at any time.
Step 1 - Configure Certificate
In order to transmit data to and from the Adito securely; you will need to generate an SSL certificate. SSL certificates are used on the internet to verify the identity of a web server in order to facilitate secure exchange of sensitive data such as credit card payments or online banking transactions.
Create New Certificate
Choose this option to generate a new untrusted certificate. This will be enough to get your server up and running. You may later generate a Certificate Signing Request (CSR) for transmission to a Certification Authority (CA).
Import Existing Certificate
If you already have a certificate (or keystore), you may use this option to import. You will need to know the passphrase for the certificate / keystore you are importing.
Next
Cancel
Listo
Internet
100%

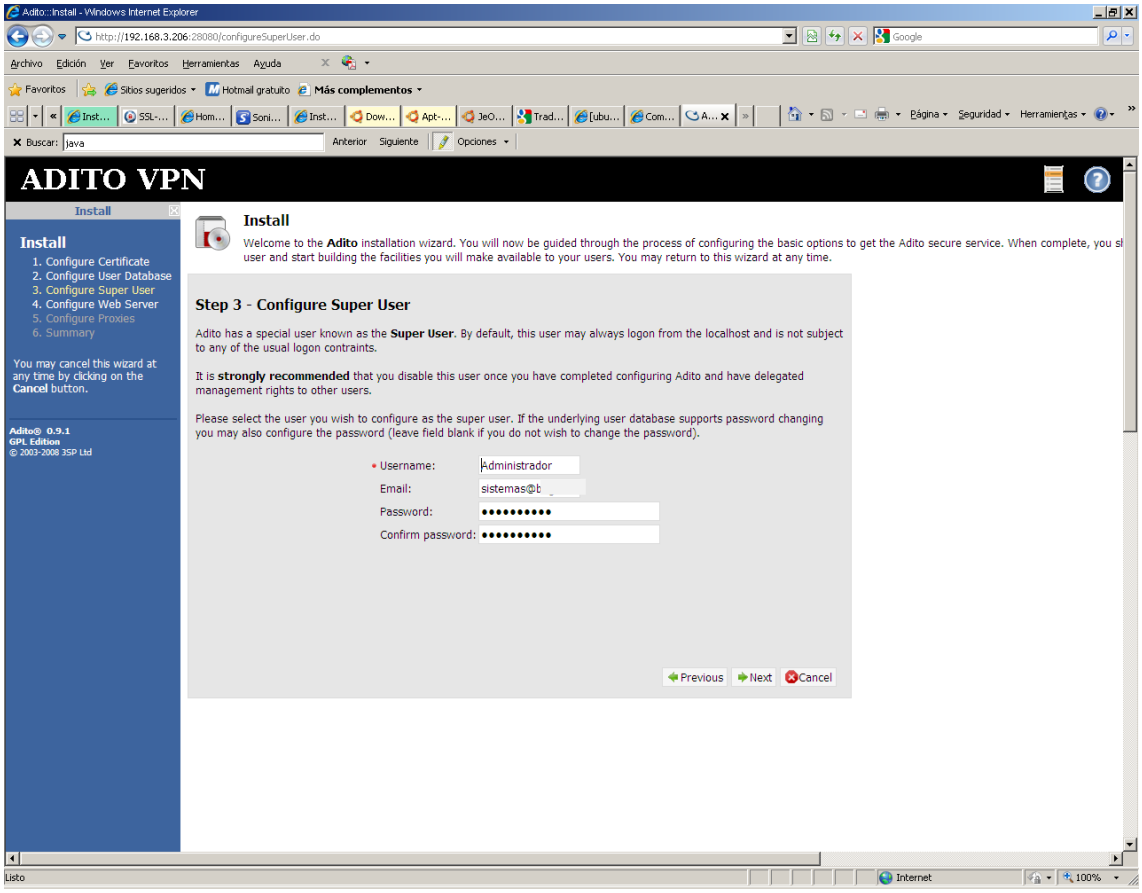

Adito::Install - Windows Internet Explorer
http://192.168.3.206:28080/setKeyStorePassword.do
ADITO VPN
Install
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you sh
user and start building the facilities you will make available to your users. You may return to this wizard at any time.
Step 1 - Set Keystore Passphrase
When creating a new certificate, you must provide a passphrase to encrypt the generated keystore. This passphrase will be required if you wish to manipulate the keystore file with the command line tools provided with Java.
Passphrase:
Confirm passphrase:
Previous
Next
Cancel
Listo
Internet
100%

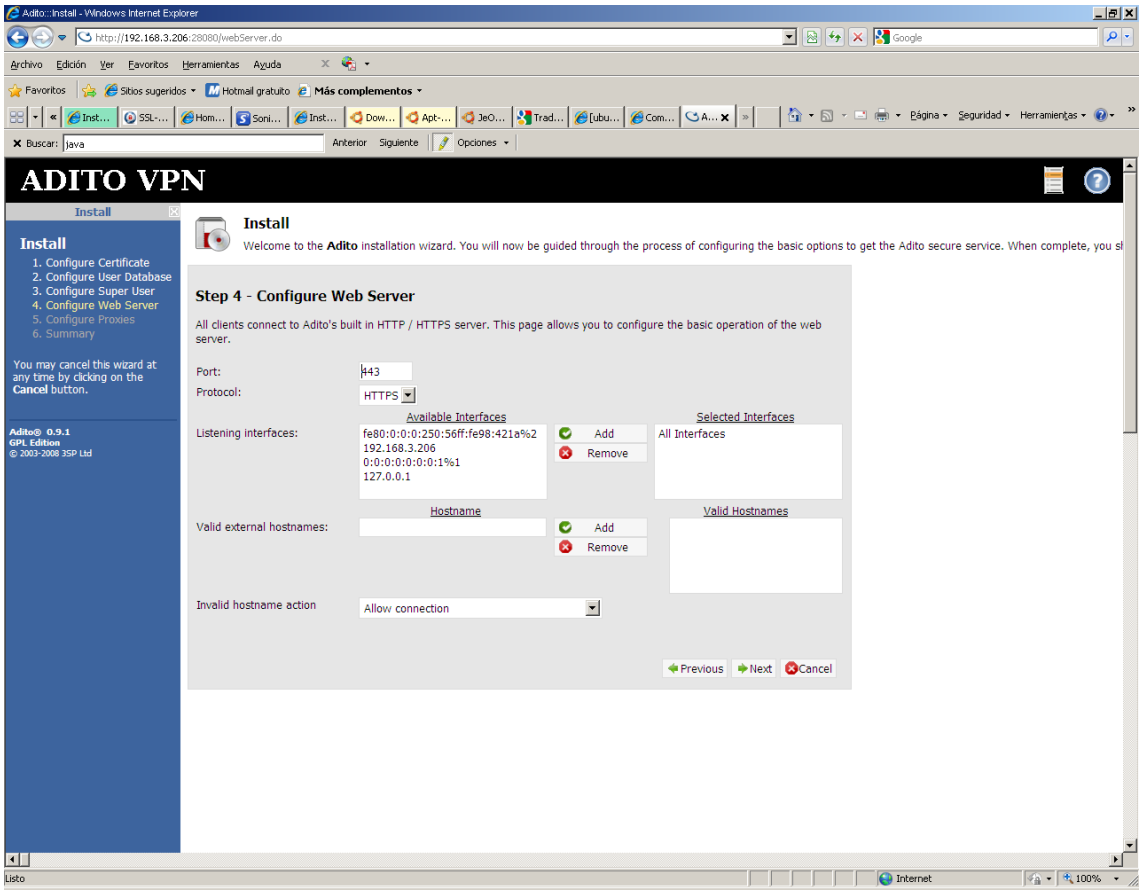

Adito:::Install - Windows Internet Explorer
http://192.168.3.206:28080/createNewCertificate.do
ADITO VPN
Install
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you should start the service, logon as the super user and start building the facilities you will make available to your users. You may return to this wizard at any time.
Step 1 - Create New Certificate
Please complete the details below to generate your untrusted certificate. You should consider getting this certificate signed.
Host name: srvv-ubuntu
Organisational unit:
Company:
City:
State: Spain
Country Code: ES
Previous
Next
Cancel

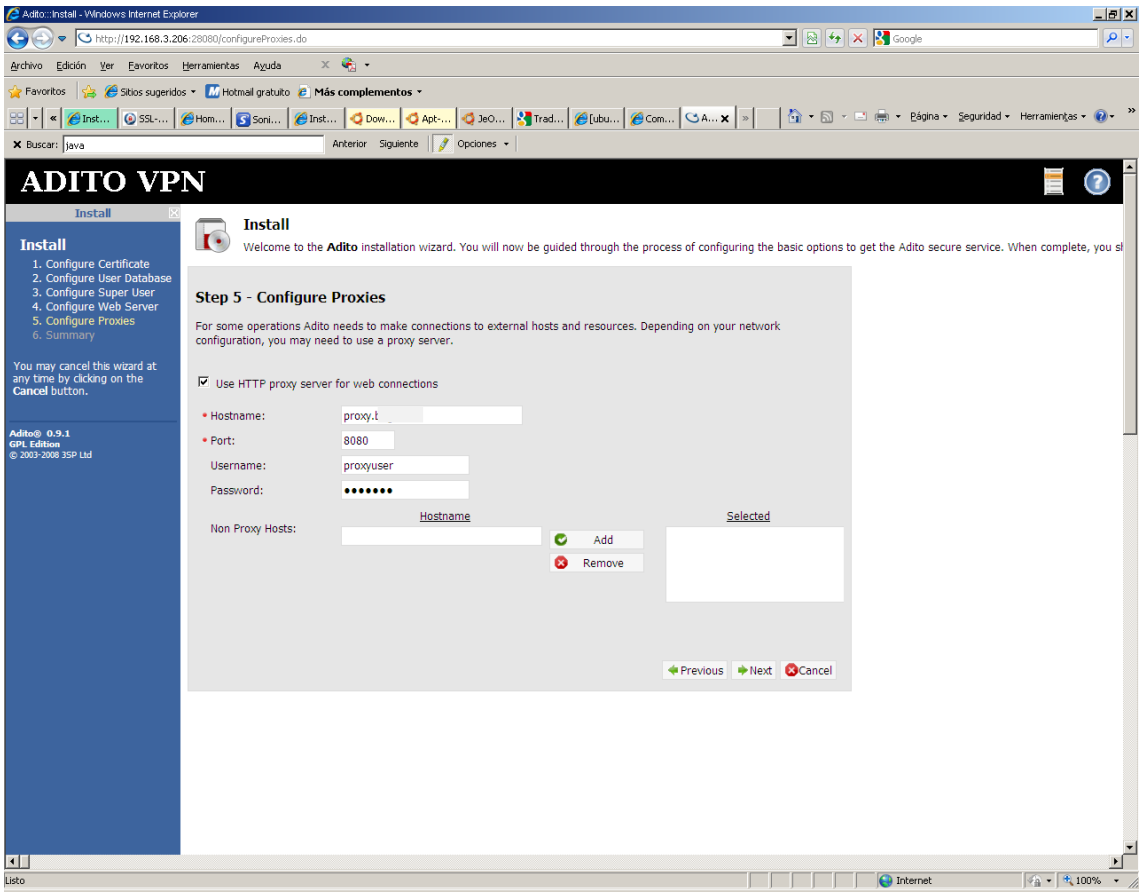

Adito:::Install - Mozilla Firefox
http://192.168.3.206:28080/configureUserDatabase.do
ADITO VPN
Install
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you should start the service, logon as the super user and start building the facilities you will make available to your users. You may return to this wizard at any time.
Step 2 - Configure User Database
This user database requires further configuration. Please provide all the required details below.
Connection
OU Filter
Options
Domain Controller Hostname: 192.168.3.41
Backup Domain Controller Hostnames
Hostname
Add
Remove
Hostnames
Domain
Service Account Name: CN=adito,CN=Users,DC=
Service Account Password
Previous
Next
Cancel


Adito:::Install - Mozilla Firefox
http://192.168.3.206:28080/configureUserDatabase.do#
ADITO VPN
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you should start the service, logon as the super user and start building the facilities you will make available to your users. You may return to this wizard at any time.
Step 2 - Configure User Database
This user database requires further configuration. Please provide all the required details below.
Connection
OU Filter
Options
Filter
Filters
Include Organizational Unit Filter
Add
Remove
ou=usuarios,DC=ad,DC=l
Exclude Organizational Unit Filter
Include built-in groups.
Include distribution groups.
Include standard users and groups.
Previous
Next
Cancel
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Terminado


Adito:::Install - Mozilla Firefox
http://192.168.3.206:28080/configureUserDatabase.do#
ADITO VPN
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Install
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you should start the service, logon as the super user and start building the facilities you will make available to your users. You may return to this wizard at any time.
Step 2 - Configure User Database
This user database requires further configuration. Please provide all the required details below.
Connection
OU Filter
Options
Service Authentication Type
Simple
User Authentication Type
Simple
Authentication Timeout
30
Authentication Maximum Retries
3
Connection Timeout
30
Cache Objects In Memory
Max User Cache Objects
20000
Max Group Cache Objects
1000
User/Group Cache TTL
30
Page Size
500
Member Of Supported
Enforce username case sensitivity.
Follow Referrals
Previous
Next
Cancel
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Terminado


Adito:::Install - Windows Internet Explorer
http://192.168.3.206:28080/configureSuperUser.do
ADITO VPN
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you
Step 3 - Configure Super User
Adito has a special user known as the Super User. By default, this user may always logon from the localhost and is not subject to any of the usual logon contraints.
It is strongly recommended that you disable this user once you have completed configuring Adito and have delegated management rights to other users.
Please select the user you wish to configure as the super user. If the underlying user database supports password changing you may also configure the password (leave field blank if you do not wish to change the password).
Username:
administrador
Email:
Password:
Confirm password:
Previous
Next
Cancel


Adito:::Install - Windows Internet Explorer
http://192.168.3.206:28080/webServer.do
ADITO VPN
Install
1. Configure Certificate
2. Configure User Database
3. Configure Super User
4. Configure Web Server
5. Configure Proxies
6. Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options to get the Adito secure service. When complete, you
Step 4 - Configure Web Server
All clients connect to Adito's built in HTTP / HTTPS server. This page allows you to configure the basic operation of the web server.
Port:
443
Protocol:
HTTPS
Available Interfaces
Selected Interfaces
Listening interfaces:
fe80:0:0:0:250:56ff:fe98:421a%2
192.168.3.206
0:0:0:0:0:0:0:1%1
127.0.0.1
Add
Remove
All Interfaces
Hostname
Valid Hostnames
Valid external hostnames:
Add
Remove
Invalid hostname action
Allow connection
Previous
Next
Cancel



Instalar el servicio

```
sudo ant install-service
Buildfile: build.xml

set-tools:

check-tools:

check-permissions:

install-service:
     [echo] Installing Adito as Linux service
     [exec] Detecting Java
     [exec]      Using /usr/lib/jvm/java-6-sun-1.6.0.20/jre
     [exec] Detected OS debian (x86)
     [exec] update-rc.d: warning: /etc/init.d/adito missing LSB information
     [exec] update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
     [exec]  Adding system startup for /etc/init.d/adito ...
     [exec]    /etc/rc0.d/K20adito -> ../init.d/adito
     [exec]    /etc/rc1.d/K20adito -> ../init.d/adito
     [exec]    /etc/rc6.d/K20adito -> ../init.d/adito
     [exec]    /etc/rc2.d/S20adito -> ../init.d/adito
     [exec]    /etc/rc3.d/S20adito -> ../init.d/adito
     [exec]    /etc/rc4.d/S20adito -> ../init.d/adito
     [exec]    /etc/rc5.d/S20adito -> ../init.d/adito
```

```
     [exec] /home/administrador/adito-0.9.1/install/platforms/linux/install-service: line 12: /home/administrador/adito-
0.9.1/conf/wrapper.conf: No such file or directory
     [exec] Service installed
     [echo] Adito installed as Linux service

BUILD SUCCESSFUL
Total time: 0 seconds
```

Arrancar el servicio

```
sudo ant start
```

Reconfigurar Adito SSL

Parar los servicios y ejecutar de nuevo `sudo ant install` desde el directorio de Adito. Se puede hacer sin perder los parámetros que ya tenemos configurados bien.

3. CONFIGURACIÓN DE SERVICIOS

Publicar una aplicación binaria: VNCVIEWER

Siguiendo los pasos que encontramos en la WEB de 3sp, vamos a tratar de crear una nueva extensión en Adito, y publicar una nueva aplicación.

http://3sp.com/en/kb/idx.php/67/178/article/Creating-your-own-extensions.html

Como ejemplo de extensión podemos tomar el fichero ZIP que encontramos en la WEB de Lars Werner

http://lars.werner.no/adito-application-ultravnc.zip

Básicamente, se trata de empaquetar en este ZIP los ejecutables y DLLs que necesita nuestra aplicación, y editar el fichero `extensions.xml`. En este fichero es donde indicamos:

- los ficheros que hay que descargar en el cliente
- los parámetros que necesitamos recoger para ejecutar la aplicación
- el túnel que vamos a crear para conectar nuestra aplicación a los servidores internos (si hace falta)

En el caso de UltraVNC, vamos a describir un poco lo que conseguimos. UltraVNC tiene dos ejecutables:

- el server (`winvnc.exe`) que es el que tiene que estar ejecutándose en el equipo del que queremos tomar control remoto
- el cliente o visor (`vnviewer.exe`) que es el que ejecutamos en la maquina desde donde vamos a tomar el control remoto

Lo que hace la extensión de VNC server, que además viene por defecto con Adito VPN, es descargar el Viewer en el PC del equipo y establecer una sesión de control remoto contra una maquina de la red local.

Pero antes de establecer esta sesión, se establece un túnel entre la IP `localhost:localport` y la IP `remotehost:5900`. El ejecutable `vncviewer` atacará a `localhost:localport` y sus paquetes se tunelizan y se llevan a través de la maquina donde tenemos instalado ADITO VPN, hasta la maquina remota: `remotehost:5900`

De esta manera nos logramos conectar de forma segura a un servicio corporativo de la red interna, desde un equipo en internet.

Pero normalmente, el problema es el contrario. El personal de soporte, dentro de la red interna corporativa, es el que tiene que tomar control remoto de equipos que se encuentran fuera de esta red. En el siguiente apartado explicamos cómo hemos creado una nueva extensión para poder hacer esto.

Publicar una aplicación binaria: VNCSERVER

El VNC Server (`winvnc.exe`) tiene la posibilidad de solicitar que un cliente (`vnviewer`) establezca una sesión remota contra él. Lo bueno de esto es que el server es el que inicia la conexión, y por tanto podemos aprovechar y establecer antes un túnel desde el equipo remoto antes de solicitar la sesión de control remoto.

Una vez que vncserver está ejecutándose, si ejecutamos `winvnc -connect helpdeskhost`, haremos que helpdeskhost inicie una sesión de control remoto contra el vncserver. Para ello el helpdeskhost tiene que estar ejecutando el vncviewer en modo "listen": `vncviewer /listen`

Por tanto necesitamos modificar en cierto modo la extensión tradicional que trae Adito para el VNC, porque lo que tenemos que descargar al cliente es el `winvnc.exe` y lo que tenemos que ejecutar es `winvnc.exe -connect`

Vamos a explicar los pasos que hemos seguido para que esto funcione:

Basándonos en el fichero http://lars.werner.no/adito-application-ultravnc.zip vamos a realizar algunos cambios. En primer lugar, cambiamos el nombre de la extensión para que nos cree una nueva:

```
<bundle version="2.0.1"
                        requiredHostVersion="0.9.0"
                        type="executable"
                        id="adito-application-win-vnc"
                        licenseAgreement="License.html"
                        name="win-vnc"
                        license="GPL"
                        order="99999"
                        productURL="http://www.ultravnc.com/">
```

```
<extension type="executable" extension="adito-application-win-vnc" name="win-vnc" smallIcon="UltraVNC16x16.jpg"
largeIcon="UltraVNC32x32.jpg">
```

Como vemos, hemos cambiado el nombre de la extensión, y la hemos llamado **win-vnc**

A continuación, ponemos algunos ficheros más para descargar en el cliente:

```
<files>
                                    <file>vncviewer.exe</file>
                                    <file>winvnc.exe</file>
                                    <file>UnZip32.dll</file>
                                    <file>Zip32.dll</file>
                                    <file>authadmin.dll</file>
                                    <file>authSSP.dll</file>
                                    <file>ldapauth.dll</file>
                                    <file>logging.dll</file>
                                    <file>logmessages.dll</file>
                                    <file>vnchooks.dll</file>
                                    <file>workgrpdomnt4.dll</file>
                                    <file>LaunchUltraVNC.cmd</file>
                        </files>
```

Definimos nuestro túnel:

```
<tunnel name="win-vnc" hostname="${shortcut:hostname}" port="${shortcut:port}" usePreferredPort="true" />
```

Notese que ponemos - `usePreferredPort="true"`; esto es importante, hay que poner true para que el puerto origen del túnel sea el 5500, y no uno aleatorio al azar.

A continuación definimos lo que queremos ejecutar y cómo:

```
<executable program="${client:installDir}/LaunchUltraVNC.cmd">
                                <arg>-connect</arg>
                                <arg>${tunnel:win-vnc.hostname}::${tunnel:win-vnc.port}</arg>
                                <arg>${client:installDir}</arg>
                        </executable>
```

Como vemos, no ejecutamos `winvnc.exe –connect` directamente, sino que llamamos a un cmd que previamente hemos descargado, porque necesitamos hacer algunas cosas más. A este cmd le pasamos tres argumentos:

- La opción: –connect
- Donde nos tenemos que conectar
- El directorio de descarga donde vamos a encontrar `winvnc.exe`

Veamos lo que hacemos dentro del cmd:

```
reg add HKLM\SOFTWARE\ORL\WinVNC3 /v AllowLoopback /t REG_DWORD /d 0000001 /f > %temp%\LaunchUltraVNC.log
cd %3
REM arrancamos el VNC Server, si no lo está ya
REM /SEPARATE   Start in separate memory space (more robust)
REM usar start y no esperar a que termine
REM /B         : Start application without creating a new window
tasklist /FI "IMAGENAME eq winvnc.exe" 2>NUL | find /I /N "winvnc.exe">NUL
if "%ERRORLEVEL%"=="1" start "winvnc.exe" /B /SEPARATE winvnc.exe
REM Levantamos el VIEWEr en la maquina remota
REM Parametro 1: -connect
REM Parametro 2: host::puerto
REM Parametro 3: Path al winvnc.exe
echo "Ejecutando winvnc.exe -connect %2 en el direcotrio %3" >> %temp%\LaunchUltraVNC.log
timeout 2
winvnc.exe -connect %2 >> %temp%\LaunchUltraVNC.log
```

Lo primero es añadir una clave en el registro para permitir Conexiones Loopback (Allow Loopback Connections). Esto es necesario, si no lo hacemos, recibiremos un error en el PC de Help Desk (un pequeño lio que se trae el viewer al ver que se está conectando a localhost, y que nos trajo de cabeza algunos días…)

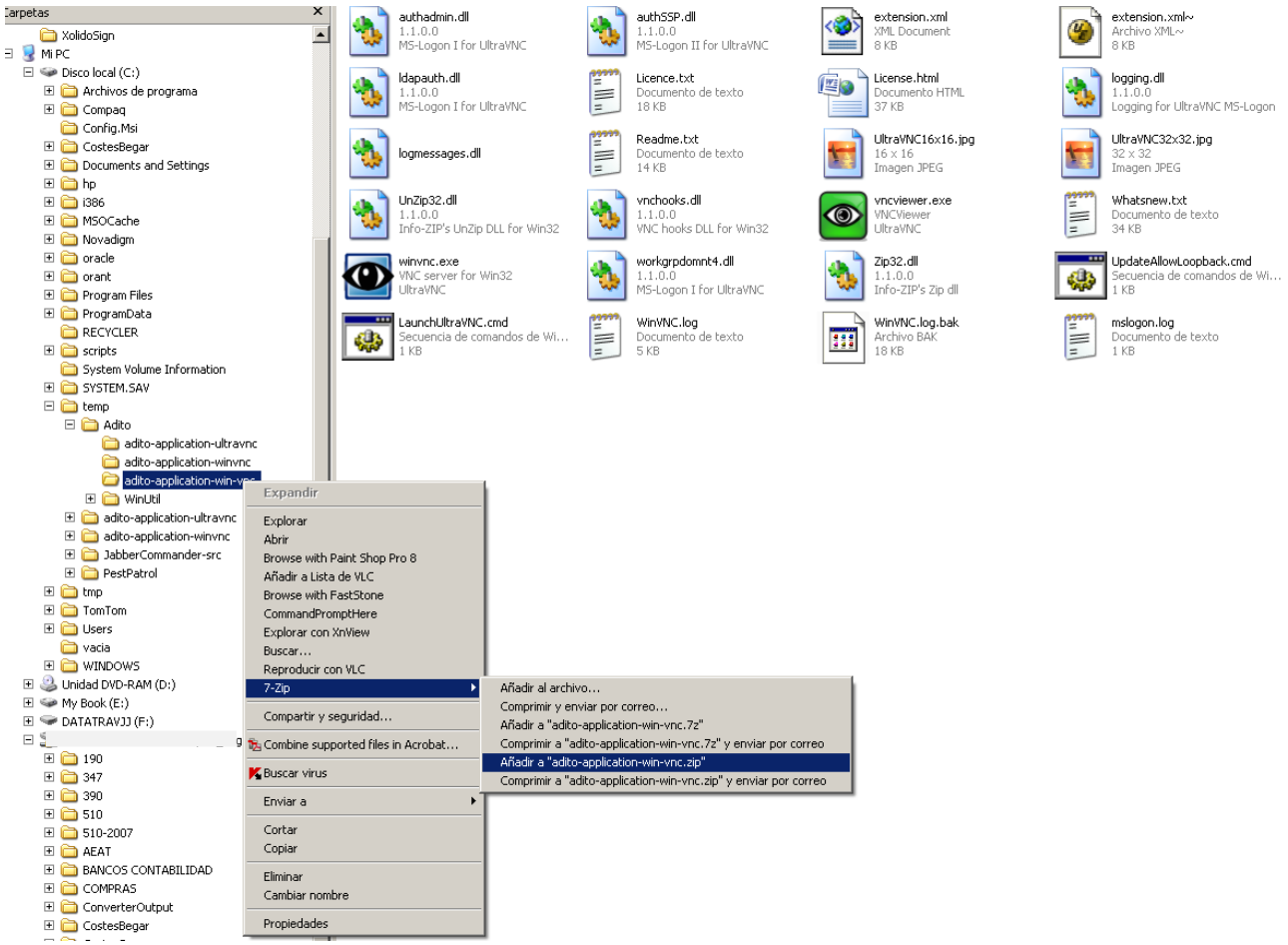
Lo segundo es ver si el VNC server está arrancado, y en caso contrario, arrancarlo.

En tercer lugar y último, ejecutamos `winvnc.exe` con la opción `–connect`

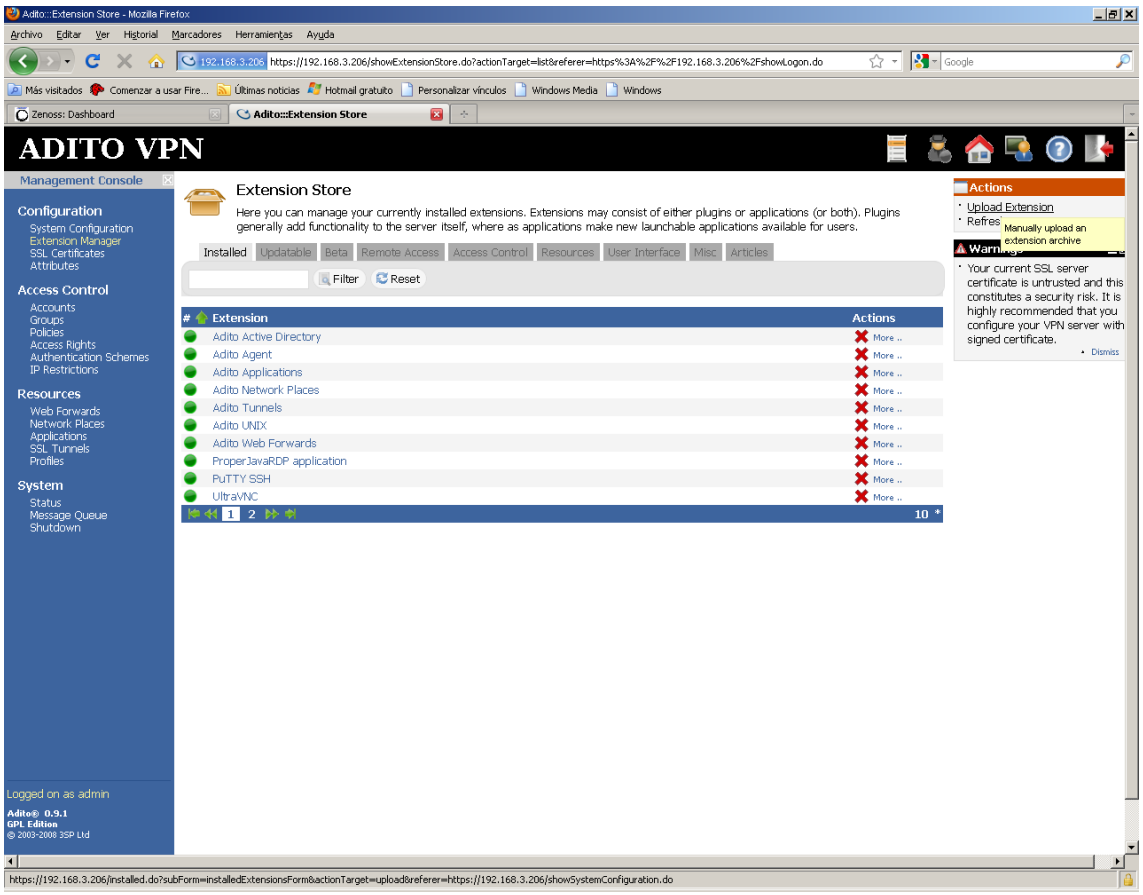
El parámetro %2 nos dirá donde nos vamos a conectar (localhost:5500). Si, nos conectamos a localhost, pero el túnel nos llevará hasta la maquina remota que especificaremos al definir la aplicación.

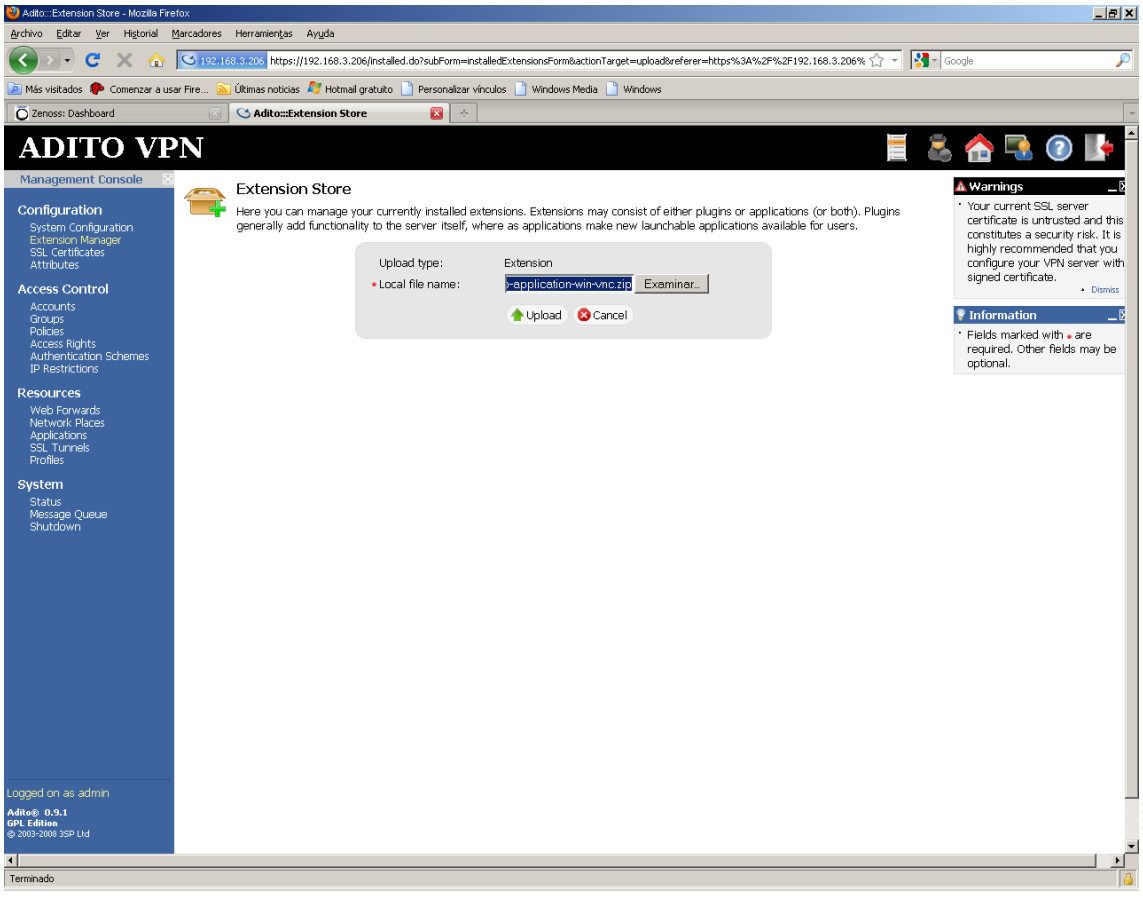
Con el fichero `extensions.xml` y el `LaunchUltraVNC` preparados, construimos un ZIP que se tiene que llamar adito-application-win-vnc.zip y descomprimir en una carpeta llamada adito-application-win-vnc (tiene que coincidir con el nombre que aparece en el fichero extensions.xml):

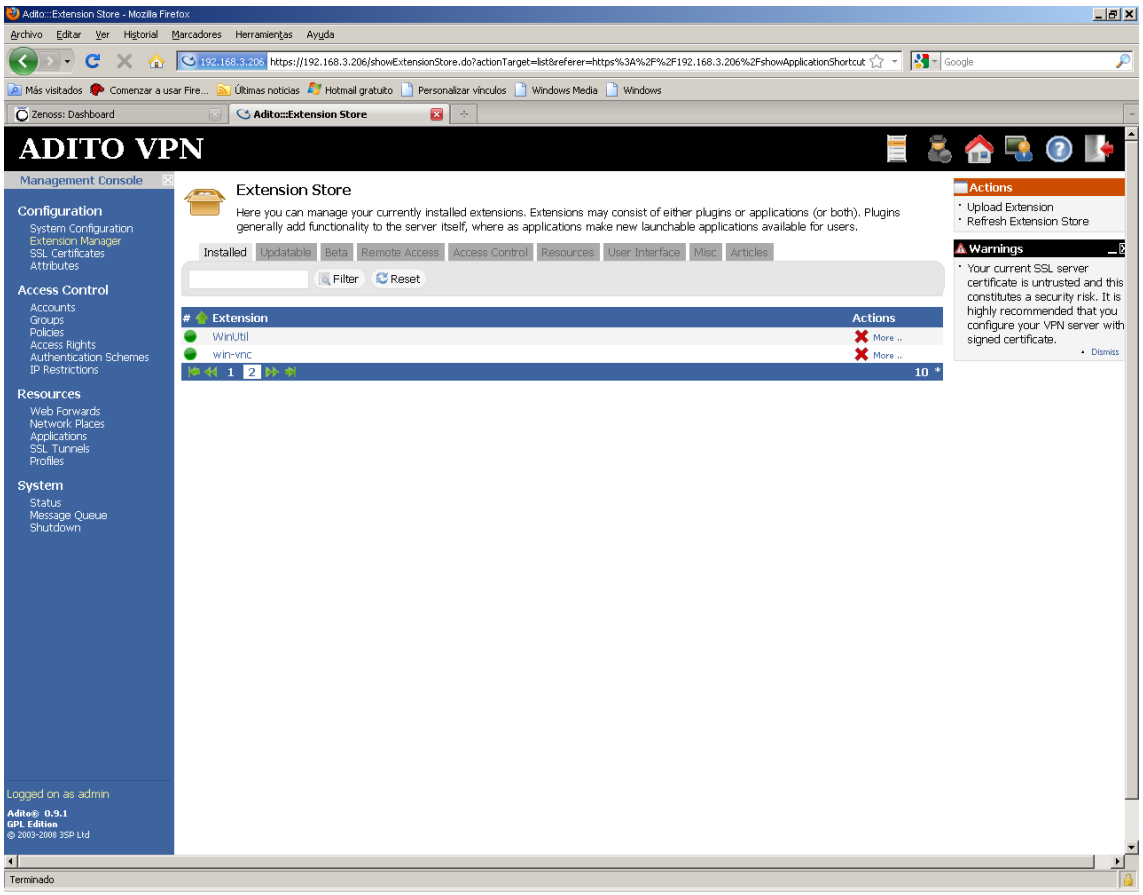
```
                        id="adito-application-win-vnc"
```



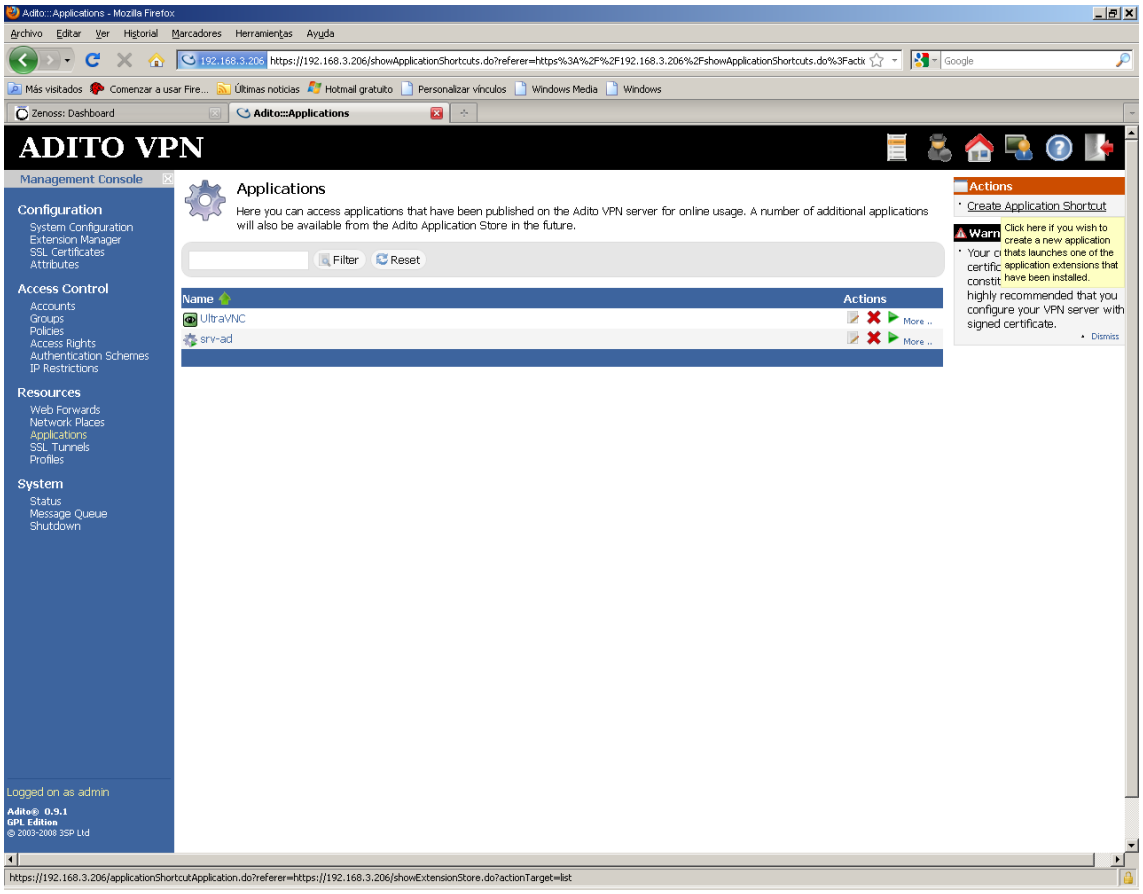
Con este ZIP ya preparado, nos vamos a ADITO VPN y añadimos una extensión:

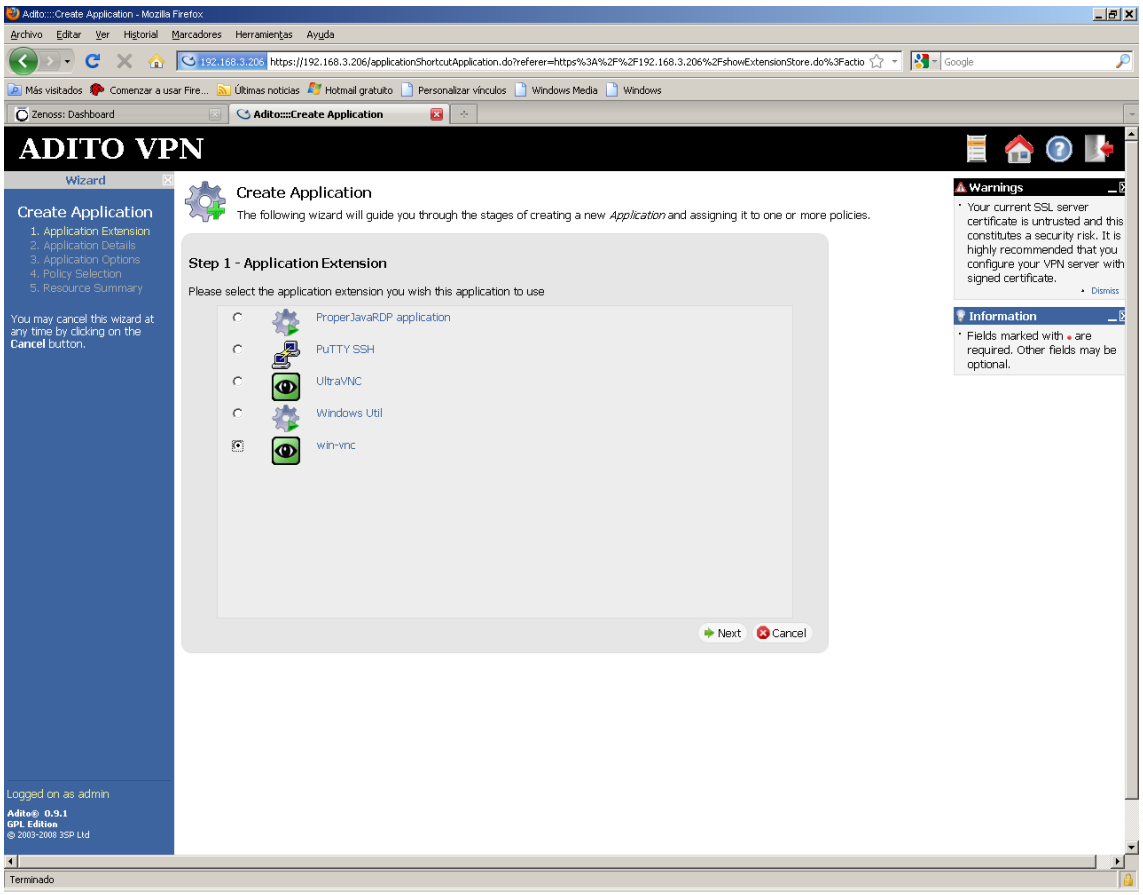

Adito:::Extension Store - Mozilla Firefox
ADITO VPN
Management Console
Configuration
System Configuration
Extension Manager
SSL Certificates
Attributes
Access Control
Accounts
Groups
Policies
Access Rights
Authentication Schemes
IP Restrictions
Resources
Web Forwards
Network Places
Applications
SSL Tunnels
Profiles
System
Status
Message Queue
Shutdown
Logged on as admin
Extension Store
Here you can manage your currently installed extensions. Extensions may consist of either plugins or applications (or both). Plugins generally add functionality to the server itself, where as applications make new launchable applications available for users.
Installed
Updatable
Beta
Remote Access
Access Control
Resources
User Interface
Misc
Articles
Filter
Reset
Extension
Actions
Adito Active Directory
Adito Agent
Adito Applications
Adito Network Places
Adito Tunnels
Adito UNIX
Adito Web Forwards
ProperJavaRDP application
PuTTY SSH
UltraVNC
More ..
Actions
Upload Extension
Refres
Manually upload an extension archive
Your current SSL server certificate is untrusted and this constitutes a security risk. It is highly recommended that you configure your VPN server with signed certificate.
Dismiss

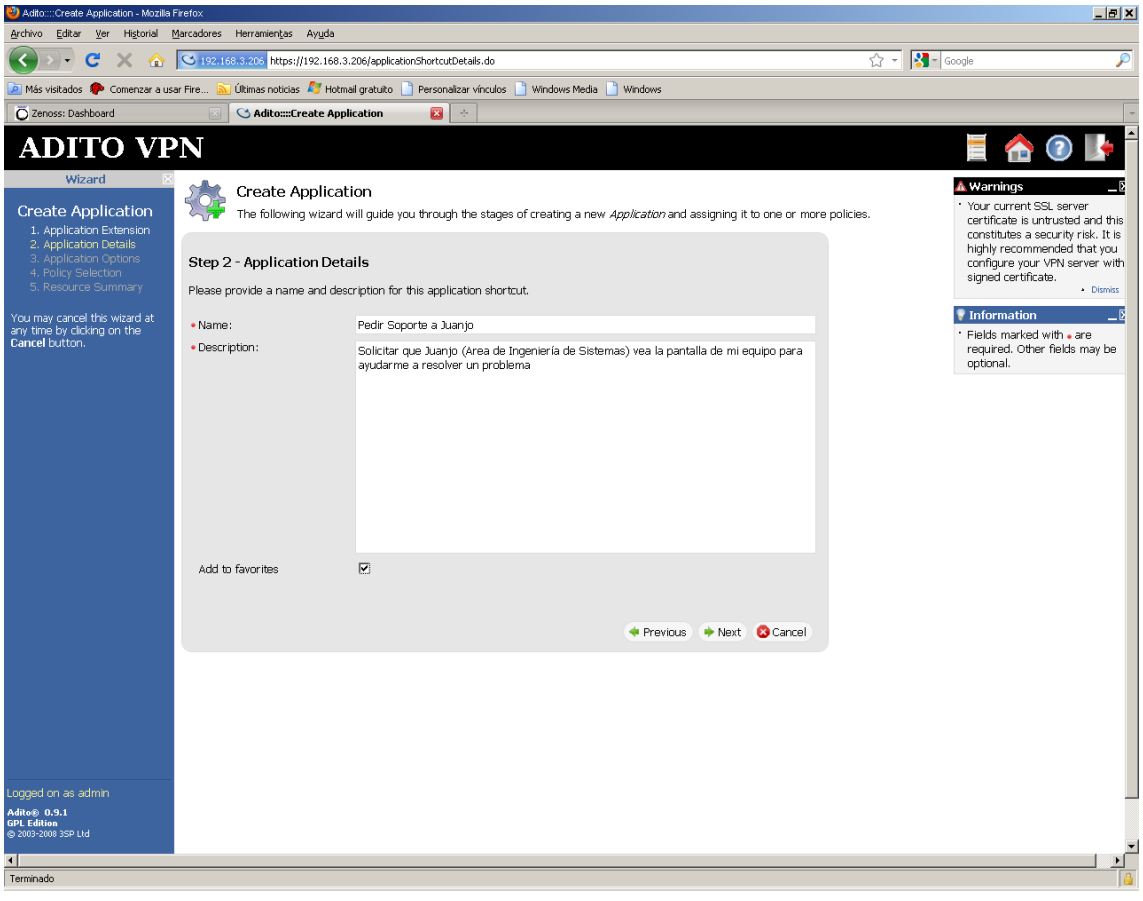

Adito:::Extension Store - Mozilla Firefox
ADITO VPN
Management Console
Configuration
System Configuration
Extension Manager
SSL Certificates
Attributes
Access Control
Accounts
Groups
Policies
Access Rights
Authentication Schemes
IP Restrictions
Resources
Web Forwards
Network Places
Applications
SSL Tunnels
Profiles
System
Status
Message Queue
Shutdown
Logged on as admin
Extension Store
Here you can manage your currently installed extensions. Extensions may consist of either plugins or applications (or both). Plugins generally add functionality to the server itself, where as applications make new launchable applications available for users.
Upload type:
Extension
Local file name:
-application-win-vnc.zip
Examinar..
Upload
Cancel
Warnings
Your current SSL server certificate is untrusted and this constitutes a security risk. It is highly recommended that you configure your VPN server with signed certificate.
Dismiss
Information
Fields marked with * are required. Other fields may be optional.
Terminado

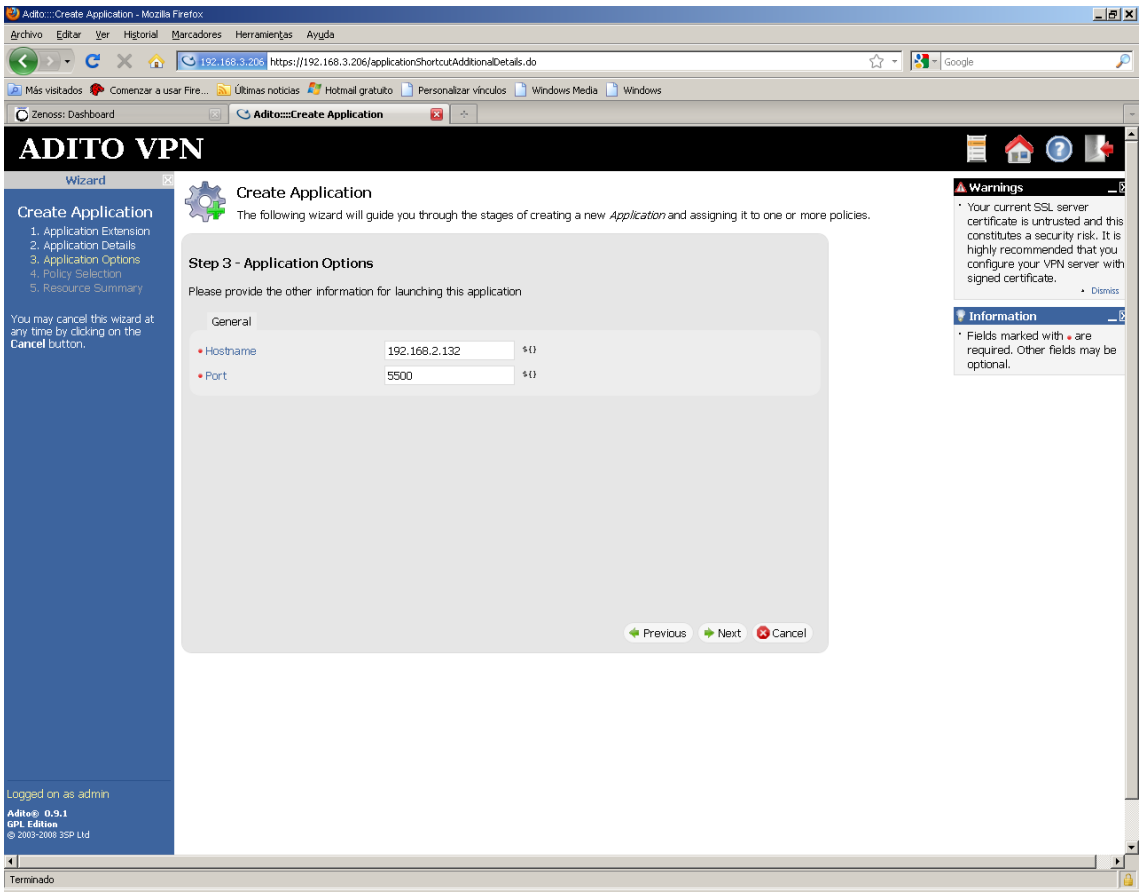


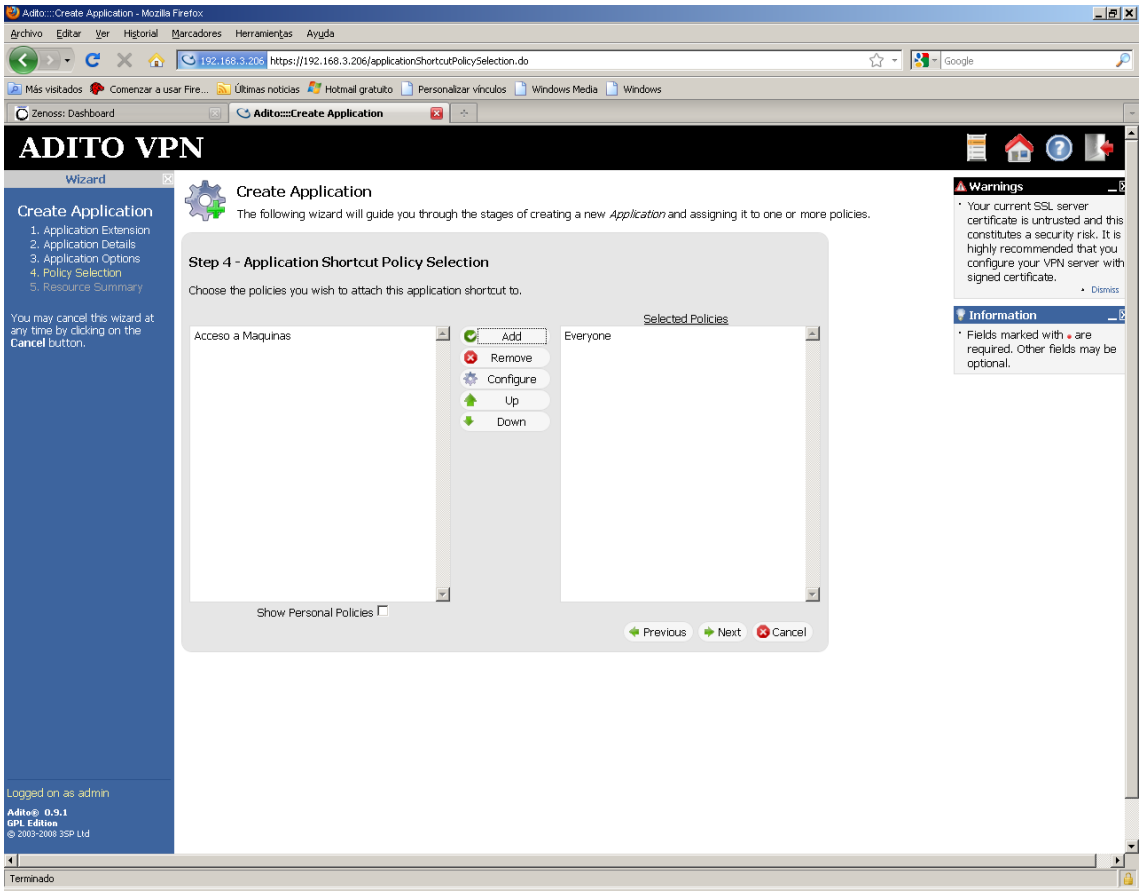
Ahora tenemos que crear nuestra aplicación basándonos en esta extensión:



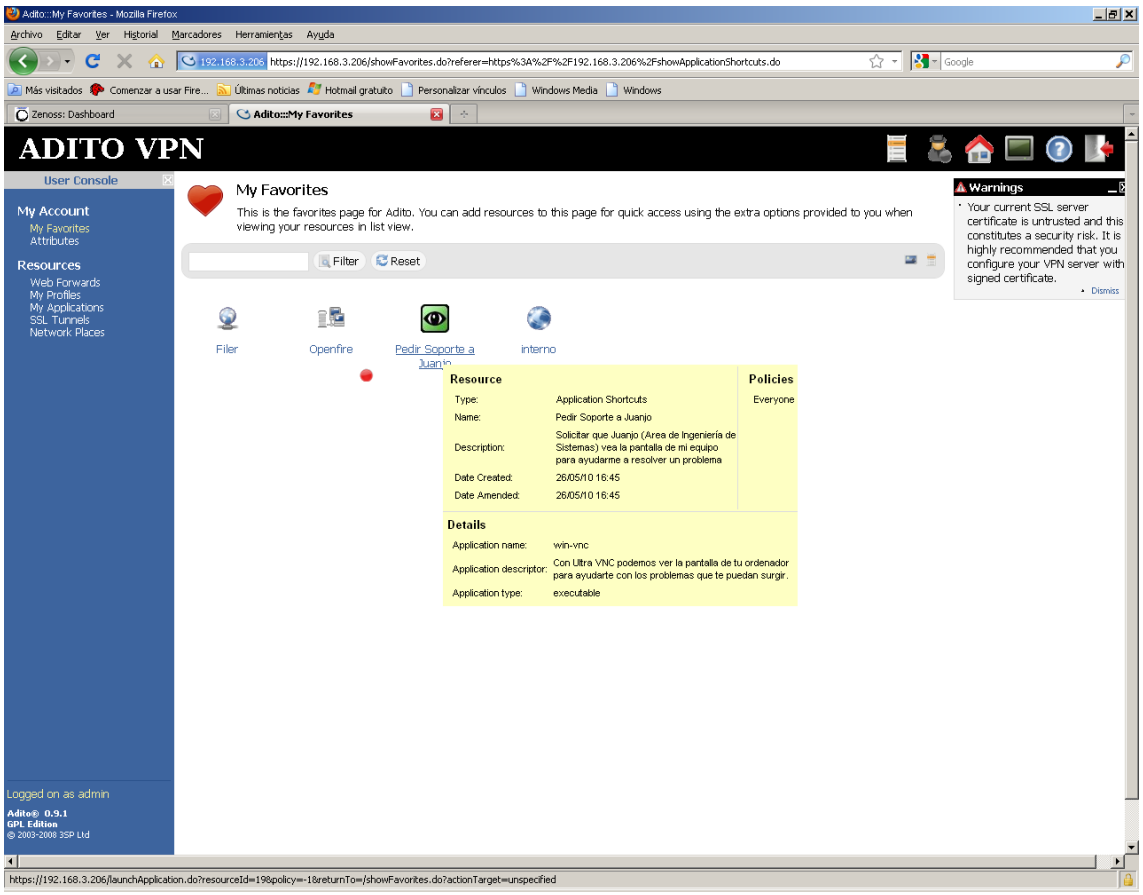

Adito::::Create Application - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
https://192.168.3.206/applicationShortcutApplication.do?referer=https%3A%2F%2F192.168.3.206%2FshowExtensionStore.do%3Factio
Zenoss: Dashboard
Adito::::Create Application
ADITO VPN
Wizard
Create Application
1. Application Extension
2. Application Details
3. Application Options
4. Policy Selection
5. Resource Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Create Application
The following wizard will guide you through the stages of creating a new Application and assigning it to one or more policies.
Step 1 - Application Extension
Please select the application extension you wish this application to use
ProperJavaRDP application
PuTTY SSH
UltraVNC
Windows Util
win-vnc
Next
Cancel
Warnings
Your current SSL server certificate is untrusted and this constitutes a security risk. It is highly recommended that you configure your VPN server with signed certificate.
Dismiss
Information
Fields marked with * are required. Other fields may be optional.
Logged on as admin
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Terminado


Adito::::Create Application - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
https://192.168.3.206/applicationShortcutDetails.do
Zenoss: Dashboard
Adito::::Create Application
ADITO VPN
Wizard
Create Application
1. Application Extension
2. Application Details
3. Application Options
4. Policy Selection
5. Resource Summary
You may cancel this wizard at any time by clicking on the Cancel button.
Create Application
The following wizard will guide you through the stages of creating a new Application and assigning it to one or more policies.
Step 2 - Application Details
Please provide a name and description for this application shortcut.
Name:
Pedir Soporte a Juanjo
Description:
Solicitar que Juanjo (Area de Ingeniería de Sistemas) vea la pantalla de mi equipo para ayudarme a resolver un problema
Add to favorites
Previous
Next
Cancel
Warnings
Your current SSL server certificate is untrusted and this constitutes a security risk. It is highly recommended that you configure your VPN server with signed certificate.
Dismiss
Information
Fields marked with * are required. Other fields may be optional.
Logged on as admin
Adito® 0.9.1
GPL Edition
© 2003-2008 3SP Ltd
Terminado





Una vez finalizado el asistente, los usuarios ya pueden ver en sus favoritos la nueva aplicación publicada:



Establecer un túnel contra un servidor local

Imaginemos que tenemos un cliente de mensajería instantánea que se conecta contra un servidor de mensajería corporativo, situado en nuestra red privada.

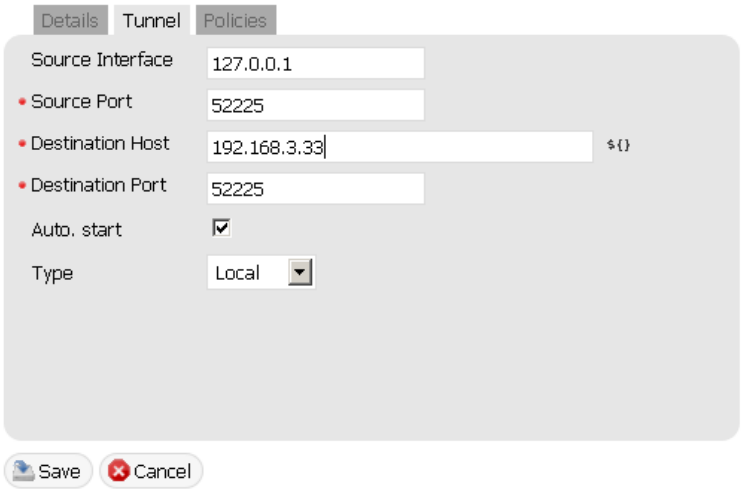
El problema es que los equipos que estén fuera de nuestra red, en principio no podrán conectarse al servidor

Para solucionar este problema, podemos establecer un túnel entre nuestro PC y el servidor de mensajería.

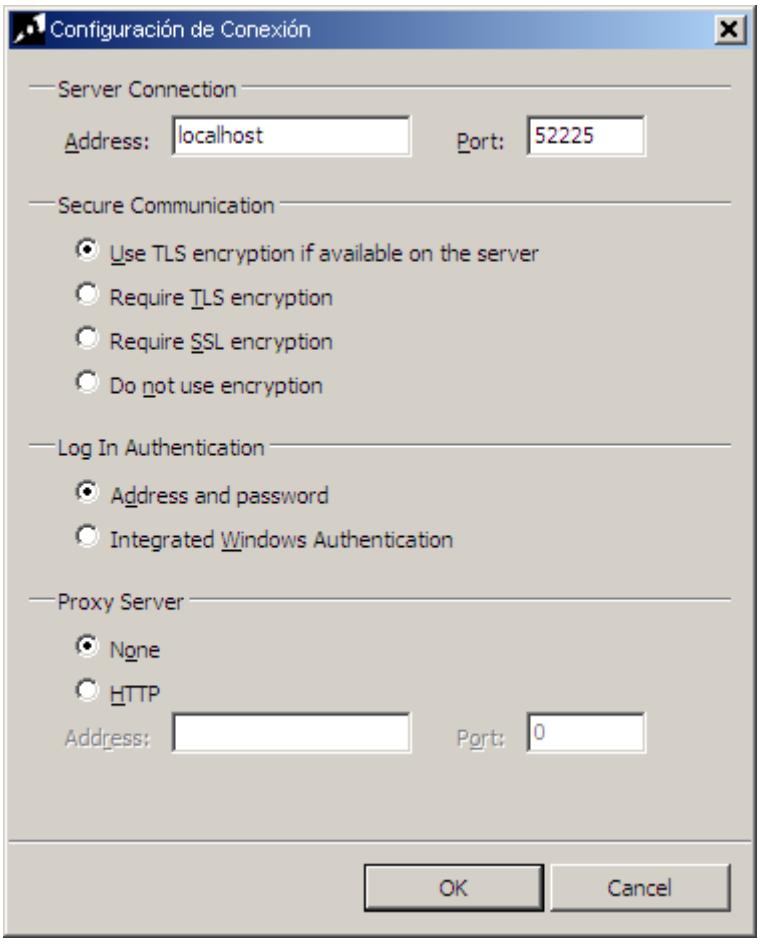
Si nuestro cliente se conecta por ejemplo a la IP privada 192.168.3.33 puerto 52225, podemos hacer que se conecte a localhost puerto 52225 (por no cambiar el puerto, aunque podríamos poner otro)

Para que esto funcione, el agente de SSL Explorer tiene que tener establecido el túnel en cuestión.

En el siguiente pantallazo vemos la definición del túnel:



El inconveniente de este tipo de túneles frente a otros túneles tradicionales como los establecidos por el Cliente Cisco VPN, es que hay que reconfigurar la aplicación cliente para que se conecte a localhost:



Con el Cliente Cisco VPN esto sería transparente, y el cliente Cisco encuentra la ruta hacia la IP Privada, porque el equipo realmente tiene una interfaz de red adicional que pertenece a esta red privada.

La ventaja del SSL Explorer es que no hace falta instalar nada en los equipos cliente.