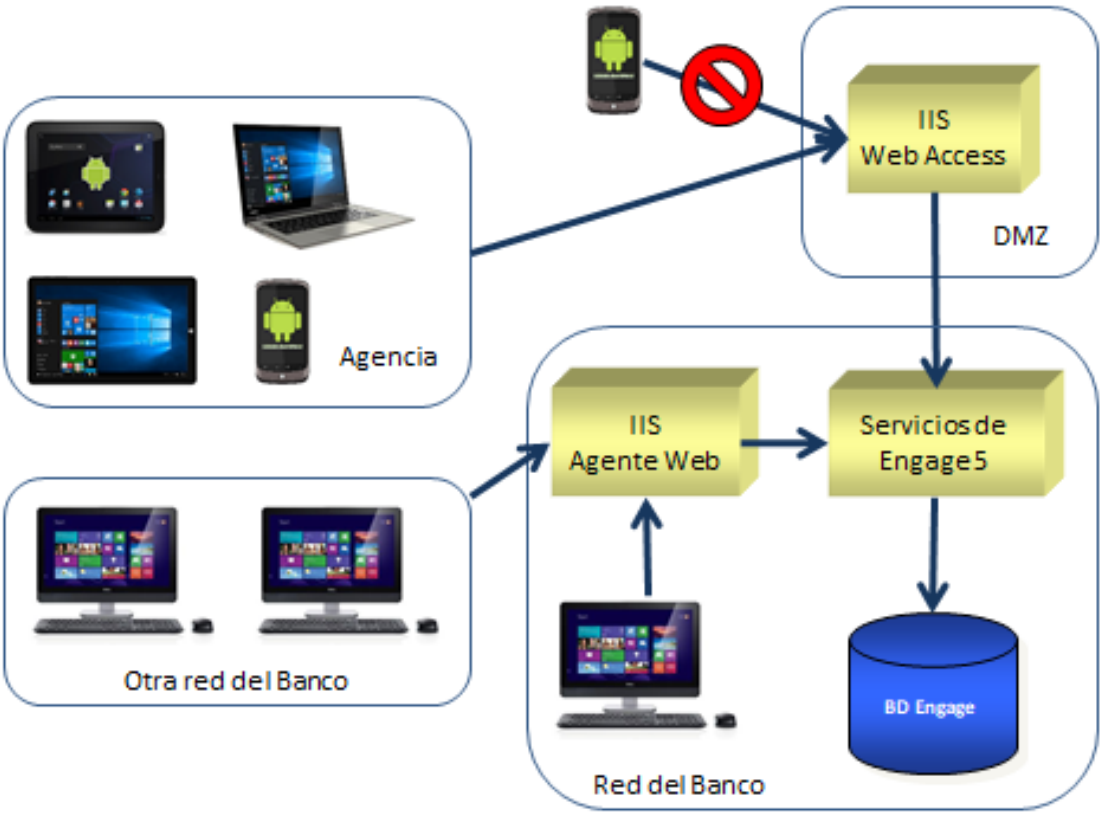
El siguiente es un gráfico ejemplo de un esquema de distribución, y de la situación que se quiere evitar:



El gráfico está muy simplificado, para evitar confusiones, y porque no somos expertos en redes como para detallar todas las posibles variables. La idea es presentar la solución lo más conceptualmente posible, para que luego cualquier experto en el tema pueda determinar su viabilidad o hacer modificaciones.

Los razonamientos que hacemos son los siguientes:

1- Todos los dispositivos que están conectados a la red de la Agencia, llegan al IIS de Web Access con la misma IP. Dicha IP podría ser fija o variar con el tiempo, aunque esto último no debería ser muy habitual.
2- Los dispositivos que acceden por fuera de la red de la Agencia, deberían tener una IP distinta a los que acceden desde adentro. Y además podría variar mucho más seguido.
3- Es más probable que desde adentro de la Agencia se acceda con tablets Windows o Android, aunque nada impide que se haga también desde los mismos celulares con los cuales se ingresa desde afuera. E incluso podría haber notebooks o PCs de escritorio.
4- Es más probable que los dispositivos que acceden desde afuera de la Agencia sean celulares o tablets, aunque cualquiera con una notebook también podría acceder. E incluso las tablets podrían ser las mismas con las que se accede desde adentro.
5- El IIS de Web Access se expone a través de una IP fija y conocida.

En base a estos razonamientos, y de acuerdo a las herramientas o métodos que tenemos para manejar la situación, llegamos a la conclusión de que la solución no será 100% exacta, dadas las siguientes situaciones:

1- La geolocación no puede realizarse vía GPS en todos los dispositivos, y hacerlo por IP no es algo seguro (hay casos en los que se devuelve un radio de hasta casi 50 km), y además depende de servicios de terceros.
2- Los métodos de control del tipo de dispositivo tampoco es seguro. Nosotros desarrollamos un prototipo, pero tanto nuestro prototipo como así otras herramientas más elaboradas pueden ser engañados. Por ejemplo, Chrome en Android tiene la posibilidad de funcionar como un browser de escritorio, y con esta opción activada se detecta como un equipo de escritorio con Linux.
3- E incluso, desde un browser de escritorio también se pueden simular otros dispositivos, con distintos sistemas operativos o tamaños de pantalla.
4- Filtrar por browser tampoco es efectivo, porque cada dispositivo puede tener más de un browser, y cada browser puede funcionar en más de un dispositivo.

Dicho todo esto, la solución que proponemos se basa más que nada en el análisis de la IP remota que llega al IIS de Web Access. Y como dato complementario podemos detectar el tipo de browser, el tamaño de la pantalla del dispositivo, y si este tiene pantalla táctil. Lo primero puede servir como dato guía, y lo segundo como dato estadístico para hacer comparaciones y afinar el procedimiento.

Para determinar si un promotor accede desde una Agencia, la IP remota que llegue al IIS de Web Access debe ser una IP que se haya asociado a esa Agencia, independientemente del tipo de dispositivo que se utilice. Si la IP de la Agencia es fija y es única, es muy fácil de mantener. Si varía con el tiempo o si hay más de una IP de salida válida, puede tomarse una estadística de los usuarios que se registran desde la Agencia y modificar la IP de referencia dinámicamente. Podría utilizarse un mecanismo de autenticación mutua entre la Agencia y el IIS de Web Access, pero esto implicaría un despliegue adicional en la Agencia.

Si el método y las condiciones en las que se aplica logran un nivel adecuado de exactitud, se puede impedir automáticamente el acceso al usuario, presentándole una pantalla de advertencia desde la cual no pueda avanzar. Pero si no se puede lograr una exactitud adecuada, también puede presentársele una pantalla de advertencia al usuario pero dejándolo seguir y dándole alguna manera de hacer un descargo o de registrar un falso positivo.

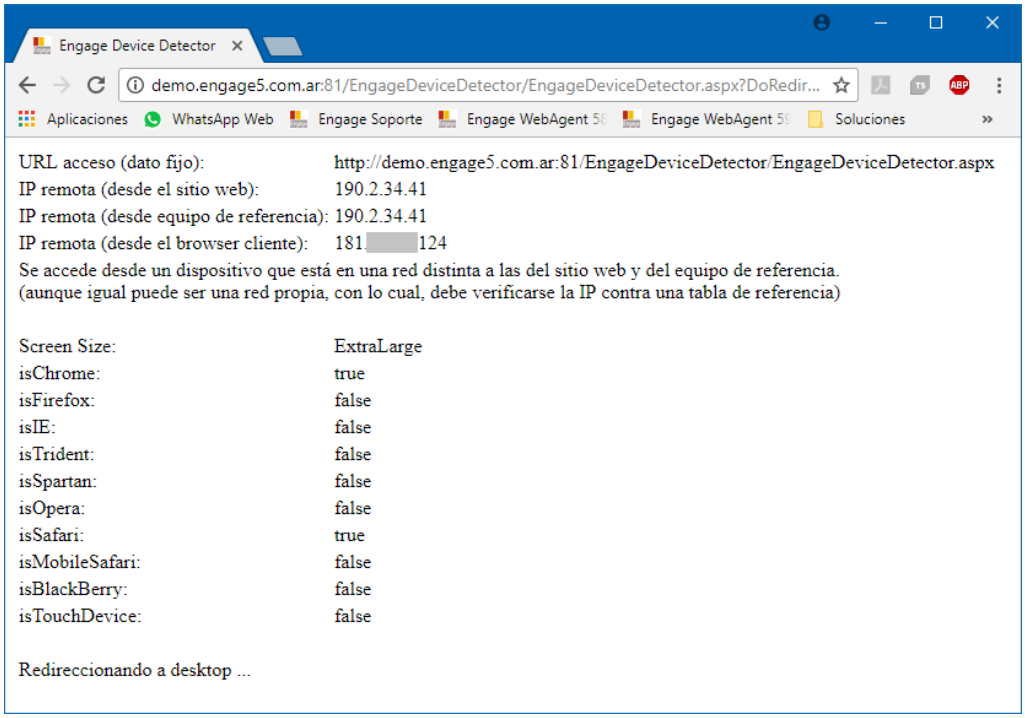
Si se logra una buena exactitud, estimamos que implementar el método de la IP no debería ser algo complicado y sólo habría que hacer una adaptación en el sitio web de Web Access. Pero si la exactitud no es buena, entonces los desarrollos adicionales para analizar estadísticamente la IP y ajustarla dinámicamente van a llevar más esfuerzo.

Nosotros publicamos un pequeño prototipo en la siguiente URL:

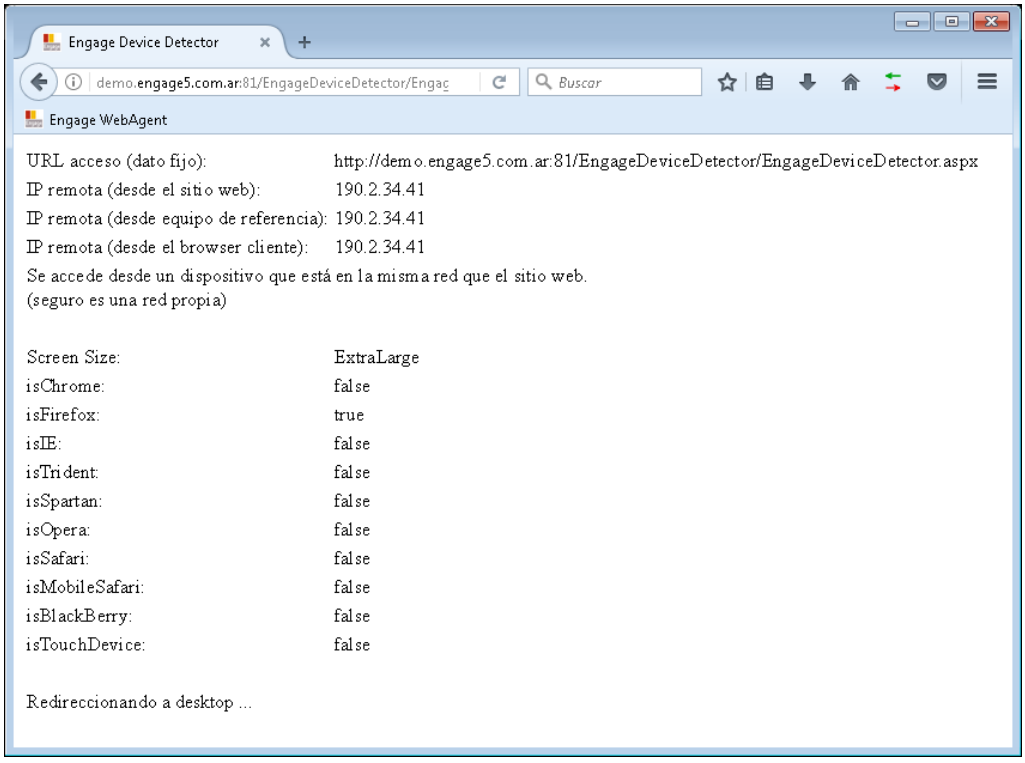
http://demo.engage5.com.ar:81/EngageDeviceDetector/EngageDeviceDetector.aspx?DoRedirect=0

El parámetro DoRedirect es opcional, y si no se informa, luego de un análisis de la información del dispositivo habrá una redirección automática a un Agente Web (orientado a desktop) o a EWA-R (orientado a mobile).

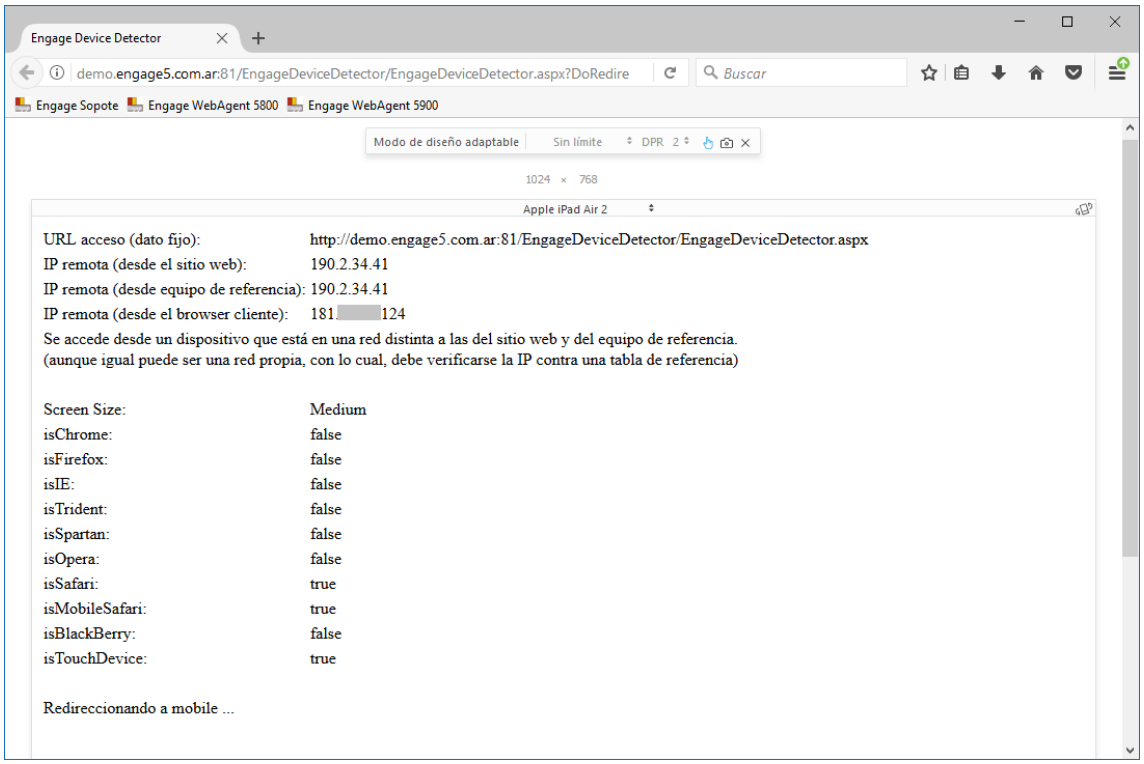
La información que muestra la página si se accede usando Chrome, desde una notebook con Windows 10, ubicada fuera de la red a la que pertenece el sitio web, es la siguiente:



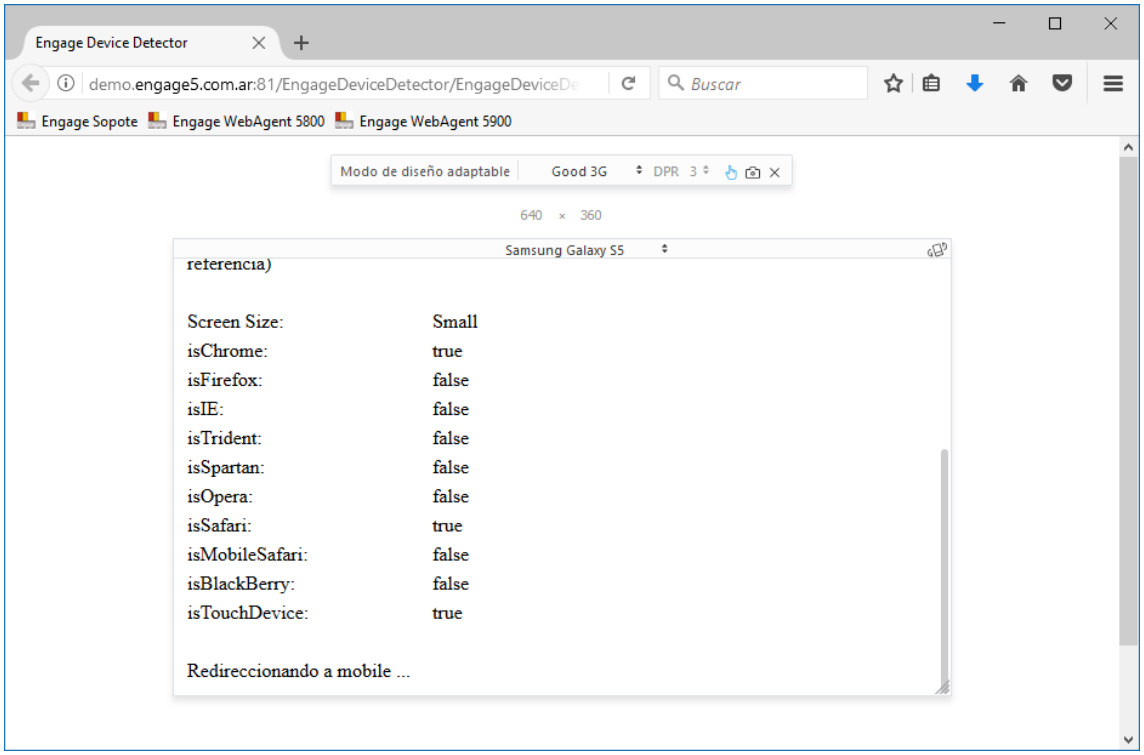
Accediendo con FireFox desde una PC con Windows 7, ubicada en la misma red del sitio web, se muestra lo siguiente:



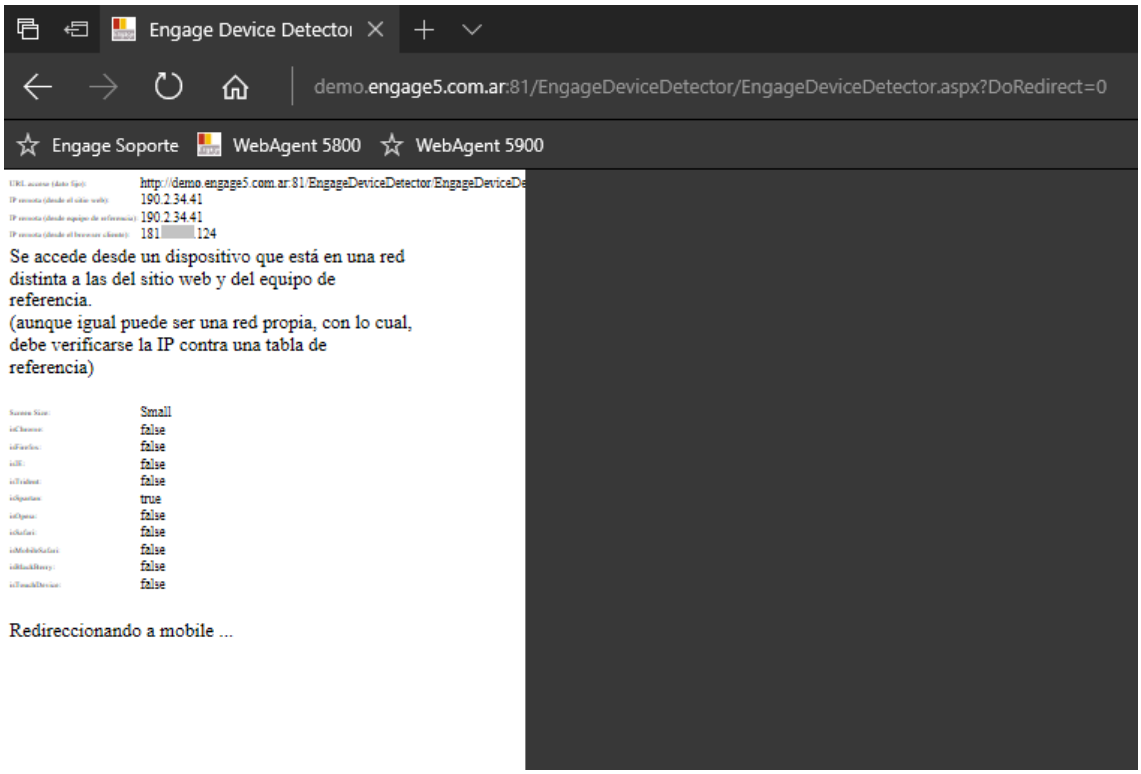
Con FireFox, simulando un iPad, desde fuera de la red:



Con FireFox, simulando un Galaxy S5 apaisado, desde fuera de la red (por el scroll, se muestra sólo la parte que corresponde al tipo de dispositivo y no al análisis de la IP):



Con Edge, simulando Microsoft Lumia 950, desde fuera de la red:



Obviamente, todo es discutible y susceptible de mejoras. Y reiteramos la recomendación de someter la solución propuesta a la opinión de un experto en redes.