fortigate, dns

Fortigate como Servidor DNS

Los cortafuegos Fortigate pueden funcionar como servidores DNS y DHCP, por lo que nos podemos ahorrar el disponer de un servidor en nuestra oficina y además podemor usarlo como caché y optimizar el tráfico originado por dichas peticiones.

El equipo se puede configurar como Maestro (Master) DNS, añadiendo manualmente los registro DNS que necesitemos, o como esclavo (slave).

A su vez el servidor dns puede ser autoritativo o recursivo. La difrencia está en que en el modo recursivo, en caso de no poder resolver un nombre, haría la petición de búsqueda al DNS externo que tengamos configurado..

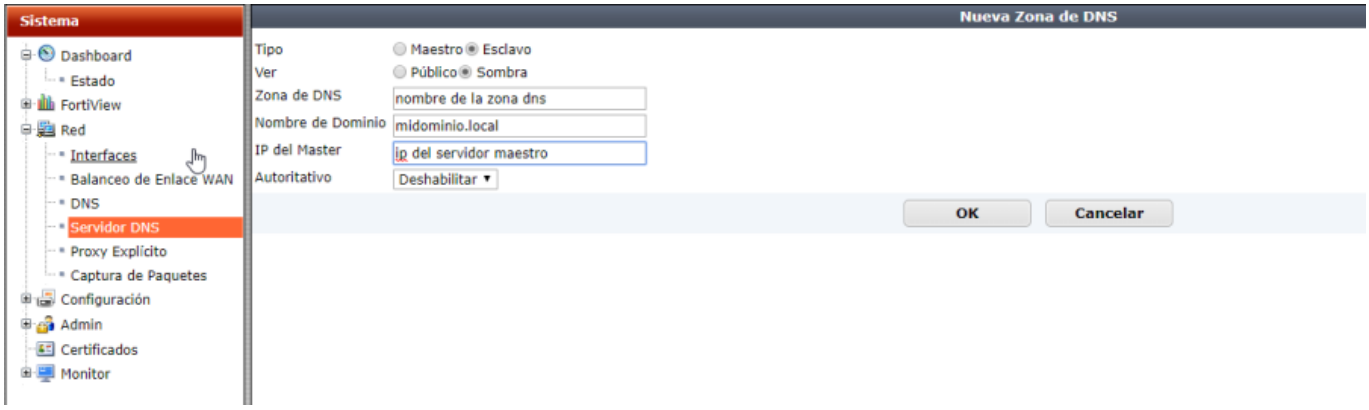
Otra de las opciones que podemos elegir es si queremos que el servidor dns sea **Public** o **Shadow .** Si marcamos como Public los usuarios externos pueden acceder a realizar consultas. Si lo marcamos como **Shadow** sólo los usuario internos pueden usarlo.

Para activar el servidor DNS tenemos que ir Configuración- > Características y pulsar el botón **Mostrar más** para ver todas las opciones disponibles, y activar la opción **Base de Datos DNS**

Al activarlo nos aparecerá una nueva opción **Servidor DNS** dentro del menú de Red

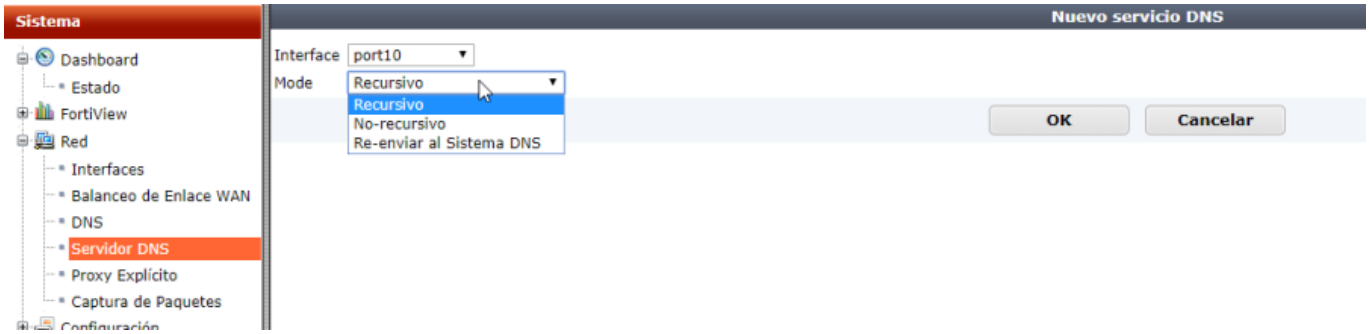
Crear Base de datos DNS

Para crear nuestra Base de datos DNS en el fortigate vamos a red→servidor DNS y en el apartado de Base de Datos DNS pulsamos en crear



Servicio DNS en Interface

Una vez creada nuestra base de datos, lo siguiente es activar el servicio dns en las interfaces que necesitemos. Para ello pulsamos el botón Crear Nuevo en la sección de **Servicio DNS en Interface** Seleccionamos el interface por el que nos van a llegar las peticiones de resolución de nombre y seleccionamos también el modo



Si tenemos varias redes internas que hacen peticiones de resolución de nombre por diferentes interfaces, deberemos a su vez de crear un servicio DNS para cada Interface

Ejemplo de configuración para una oficina remota

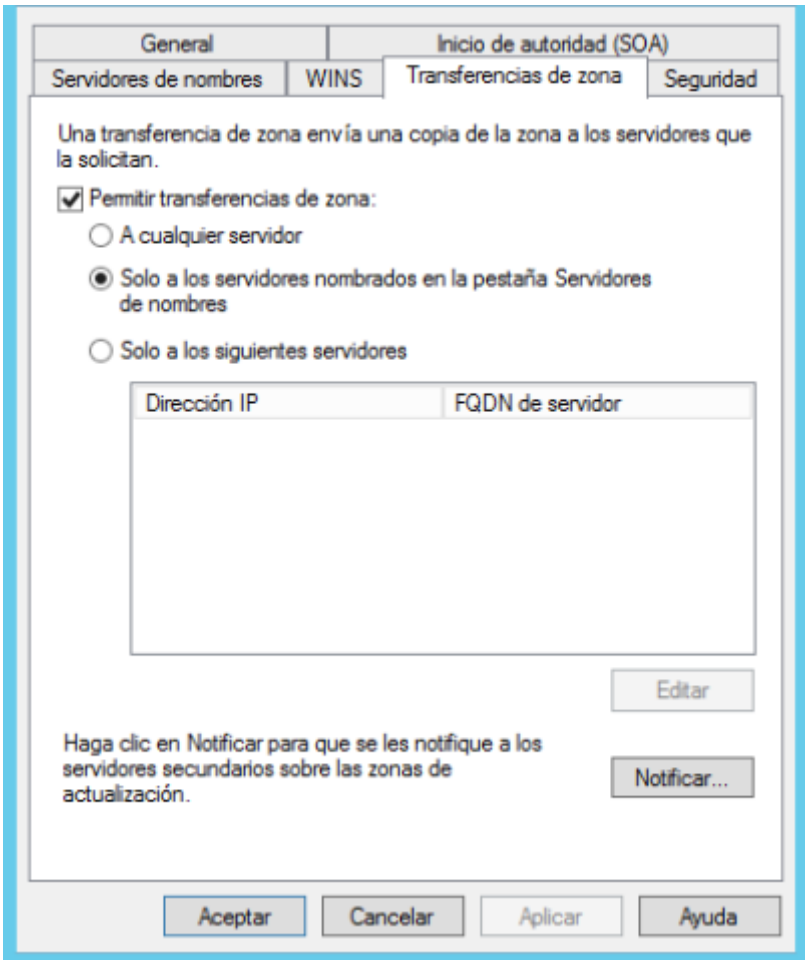
Partimos del supuesto de que tenemos una delegación pequeña que conecta por VPN con la oficina central, y que los equipos están dentro de un dominio con Directorio Activo .

Para la resolución de nombre podríamos simplemente permitir el tráfico DNS desde los equipos clientes a los servidores del dominio, pero eso implicaría desperdiciar ancho de banda y mayores tiempos de respuesta.

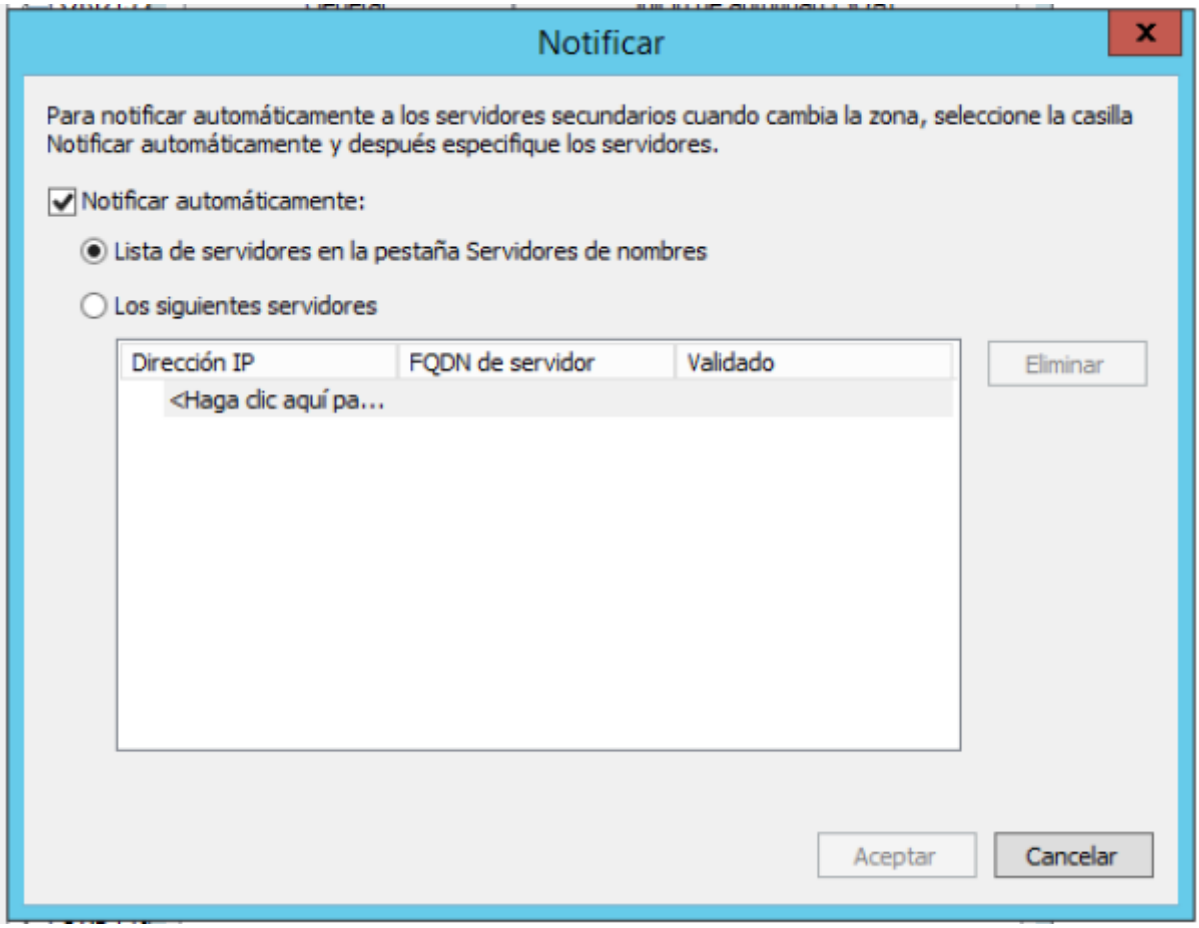
La solución sería desplegar el servico DNS en nuestro cortafuegos y que este a su vez tenga una copia de la base de datos del DNS del AD para no tener que preguntar continuamente a los servidores de la delegación central.

Paso 1

Lo primero es abrir el complemento DNS de nuestro dominio, desplegamos la zona que queremos transferir, buscamos el registro de inicio de autoridad SOA (Start of Authority) y pinchamos botón derecho → propiedades



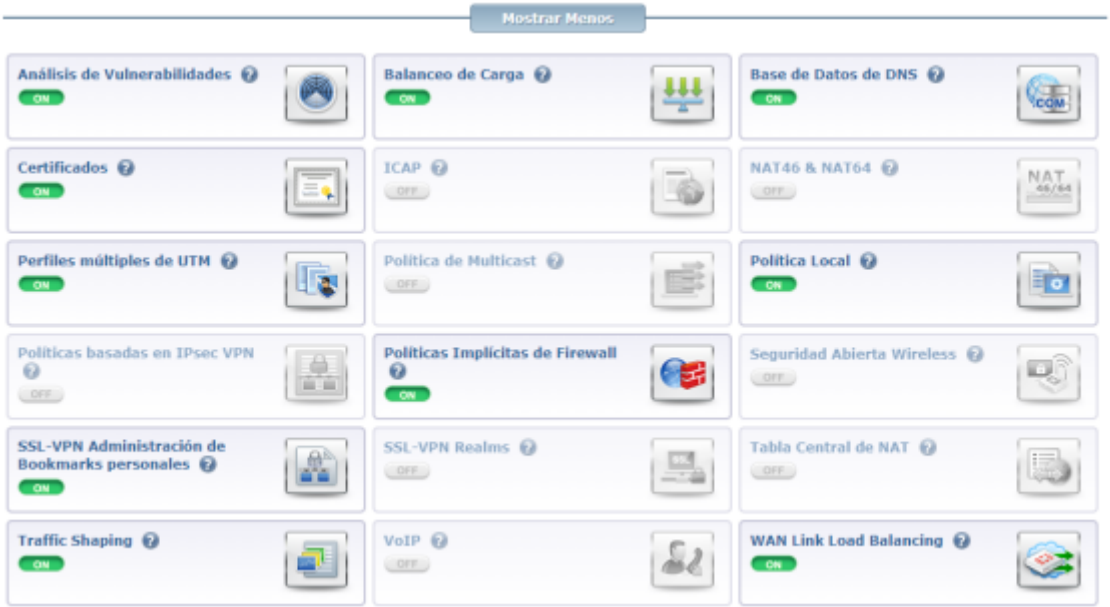
1. Añadimos la ip de nuestro firewall remoto en la pestaña de Servidores de nombre.
2. En la pestaña de Transferencia de zona marcamos la casilla de permitir la transferencias de zona → sólo a los servidores nombrados en la pestaña Servidores y procedemos a pulsar sobre el botón **Notificar**

3. 

también podíamos haber optado por marcar la opción de a cualquier servidor o la de especificar los servidores, en la pestaña de **Transferencias de zona**

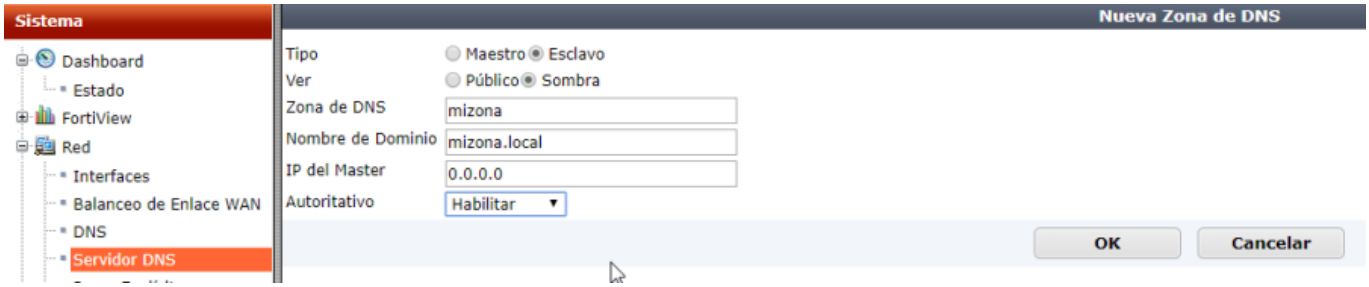
Paso 2

Activamos en nuestro firewall el complemento de la Base de datos de DNS



Paso 3

Vamos a crear el servidor como esclavo, para ello vamos a nuestro fortigate →Sistema → Red → Servidor DNS



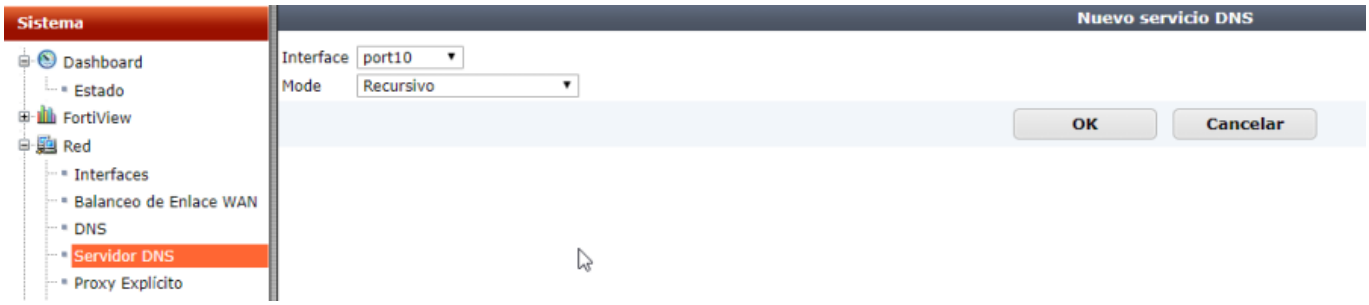
Creamos una nueva base de datos con los siguientes datos:

- tipo→ esclavo
- Ver → Sombra
- Zona de DNS →nombre_zona_empresa
- nombre de dominio →midominio.local
- IP del Master → dirección ip del servidor DNS maestro
- Autoritativo → Deshabilitado para permitir las consultas recursivas

Paso 4

Ahora que tenemos la Base de datos DNS creada vamos a crear un servicio DNS por los interfaces por los que vamos a dar dicho servicio a nuestro equipos. Para ello vamos a Sistema → Red → Servidor DNS → Servicio DNS en Interface → Crear Nuevo

Seleccionamos la interfaz y modo recursivo



Paso 5

Como último paso para la integración con el AD deberemos de crear un registro SRV mediante cli en la BDD de DNS que hemos creado en el fortigate. Abrimos la consola CLI y añadimos los siguientes comandos

```
config system dns-database
edit "nombre_zona_empresa"
set forwarder "ip_servidordns_maestro"
next
end
```

Si la conexión es mediante una VPN deberemos también indicar la ip interna desde la que haremos la petición mediante el comando **set source-ip**

```
config system dns-database
edit "nombre_zona_empresa"
set forwarder "ip_servidordns_maestro"
set source-ip "ip_origen_petición"
next
end
```

Paso 6

Desde la consola CLi podemos realizar las siguientes verificaciones

```
diag test application dnsproxy 8
```

si ponemos sin número el comando anterior **diag test application dnsproxy** nos indicará las opciones que podemos poner como número final

```
1 -> Clear DNS cache
2 -> Show stats
3 -> Dump DNS setting
4 -> Reload FQDN
5 -> Requery FQDN
6 -> Dump FQDN
7 -> Dump DNS cache
8 -> Dump DNS DB
9 -> Reload DNS DB
10 -> Dump secure DNS policy/profile
11 -> Reload Secure DNS setting
12 -> Show Hostname cache
13 -> Clear Hostname cache
14 -> DNS debug bit mask
```

Referencias

- http://kb.fortinet.com/kb/documentLink.do?externalID=FD36649
- https://fortixpert.blogspot.com/2014/05/forwarder-dns-en-fortigate.html
- https://www.fortinetguru.com/2016/12/dns-services/