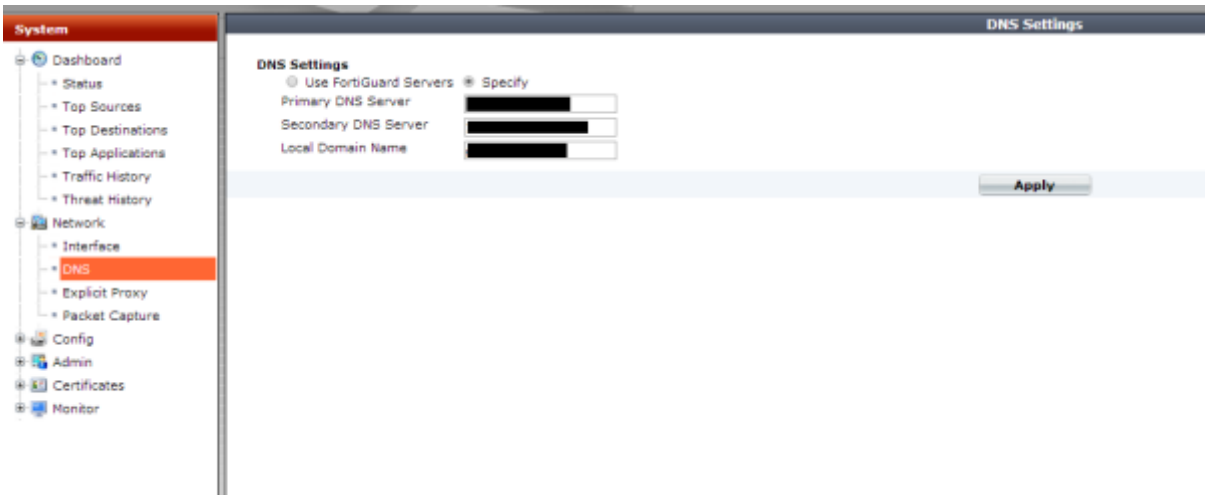
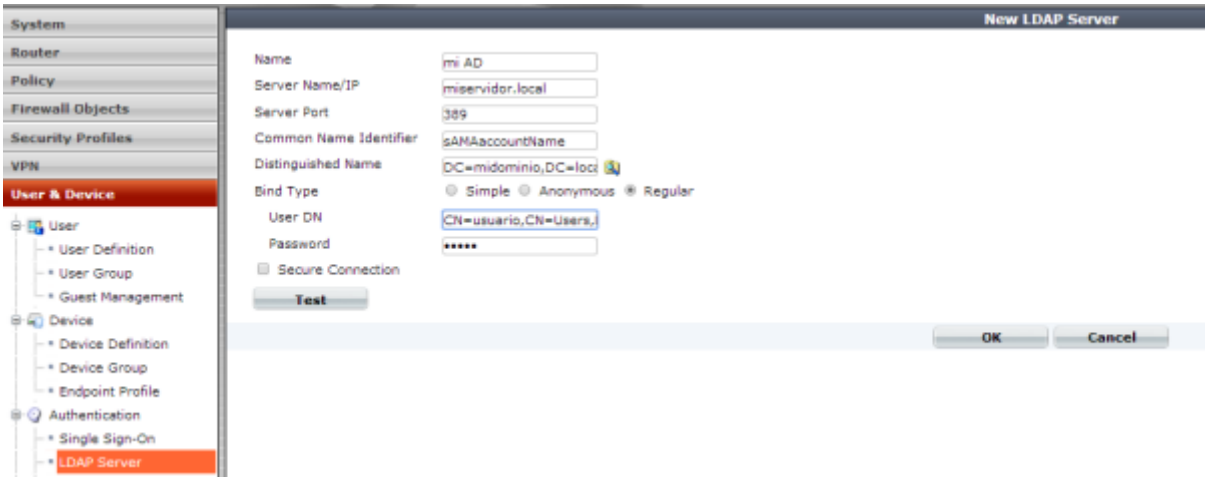
fortigate, validación, directorio activo, ad

Integración del Fortigate con el AD

Lo primero que hay que revisar es que tengamos los DNS bien configurados. System→ Networks → DNS y ponemos los valores correspondientes a nuestros DNS



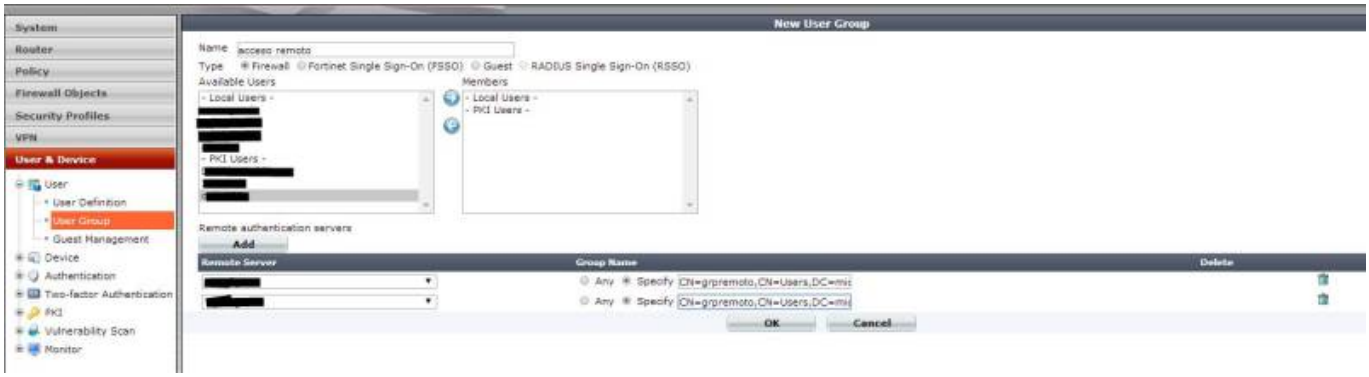
Una vez configurado el DNS, definimos el servidor de con el que nos vamos a conectar para validar usuarios. Para ello vamos a la pestaña User & Device → Authentication → LDAP Server y piulsamos sobre **Create New**



Rellenamos los campos teniendo en cuenta que para la validación con el directorio activo usamos **sAMAccountName** como Common Name Identifier

- En Distinguised Name ponemos el nombre del dominio→DC=midominio,DC=local
- User DN→ CN=usuario, CN=Users, DC=midominio, DC=local (nombre distinguido del usuario que vamos a usar para la validación)

Una vez creada la conexión con el servidor/es del directorio activo vamos a crear un grupo para la validación remota de los usuarios del mismo. Vamos a User & Device → User → User Group.



Creamos un nuevo grupo y le añadimos los servidores de directorio activo de nuestra organización y como cadena de conexión ponemos el nombre distinguido del grupo que queremos usar, en nuestro caso CN=grpremoto,CN=Users,DC=midominio,DC=local

Ahora podemos usar ese grupo para validar usuarios remotos en la VPN . Podemos editar la la fase1 de nuestra vpn y en el apartado XAUTH → marcar Enable as Server. y en UserGroup elegir el grupo que hemos creado.

También podemos crear otro grupo y usarlo para la validación de los administradores . System→ Admin→ Administrators → creamos un administrador nuevo → type= remote y en user Group ponemos el grupo creado en el apartado anterior.