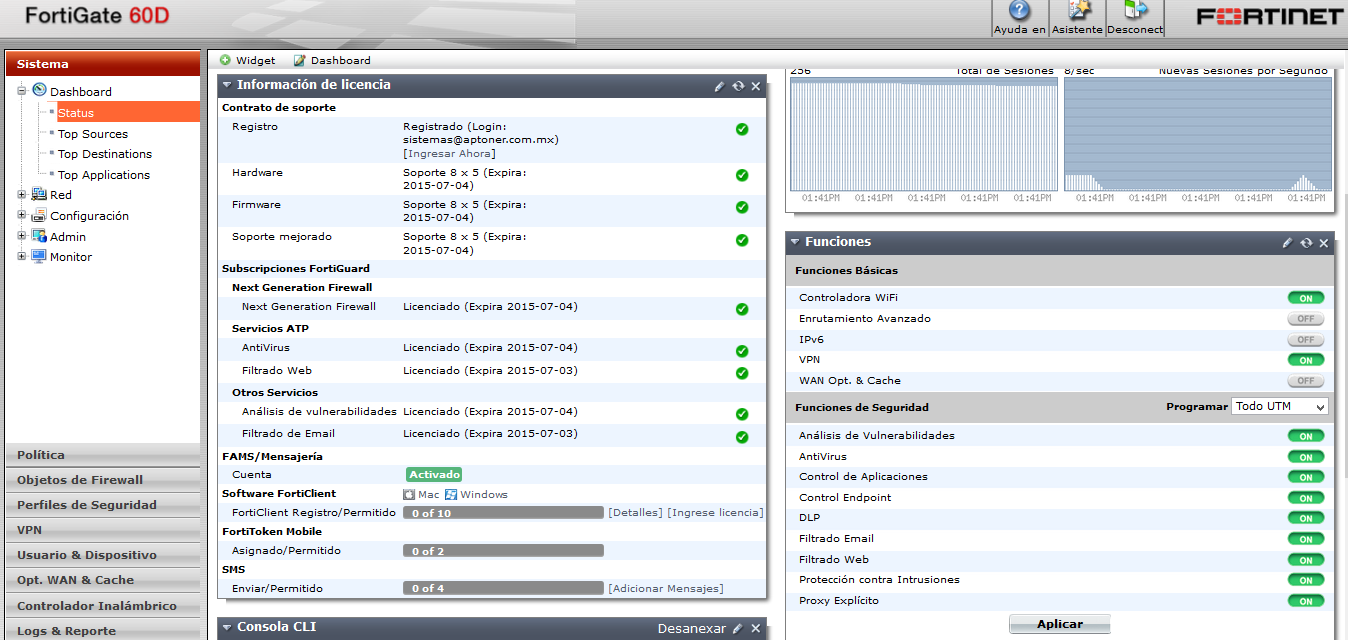
**CONFIGURACION DE FORTINET 60D**

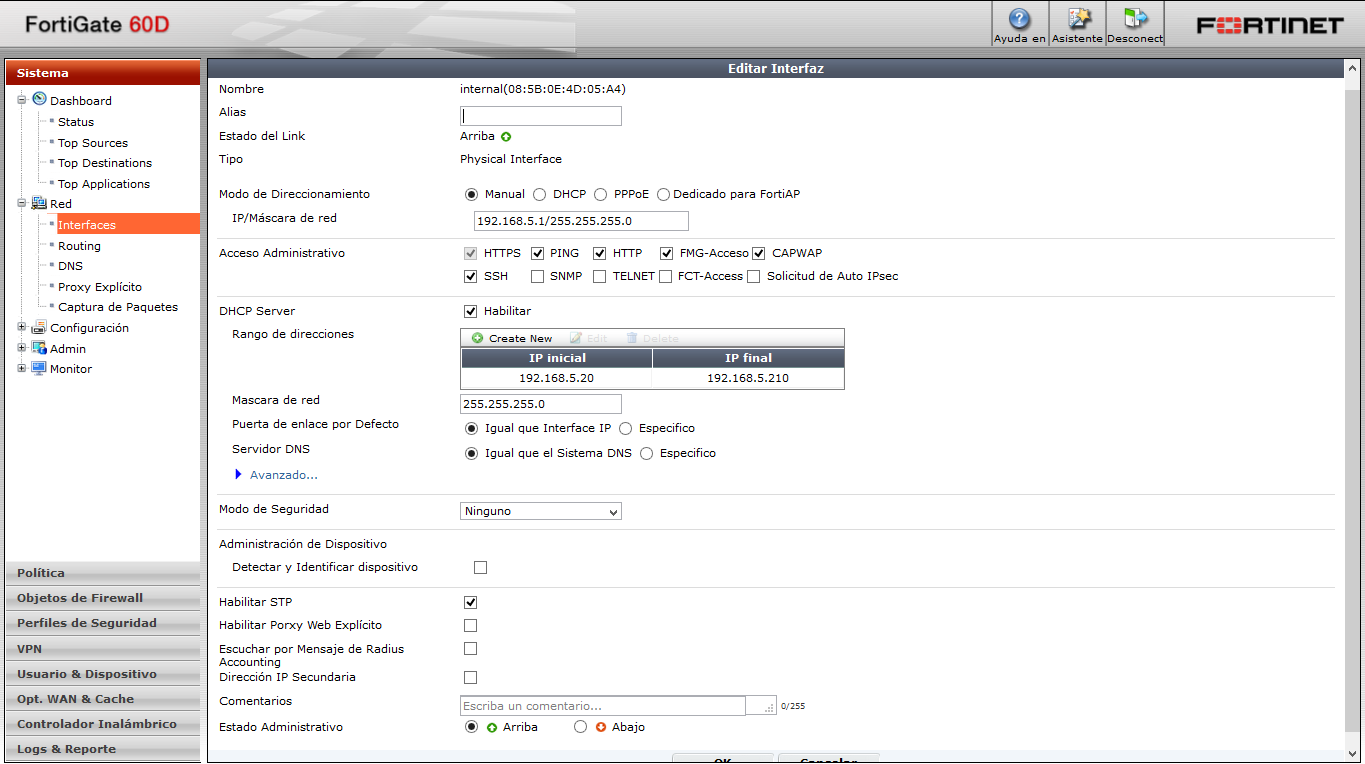
**IP DE ACCESO: 192.168.5.1**

**USUARIO: Admin**

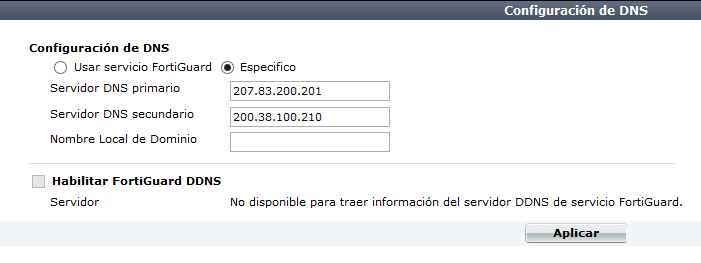
**PASSWORD: “ *@pt040201KA5.* “**

**TODAS LAS LICENCIAS ESTAN ACTIVAS**

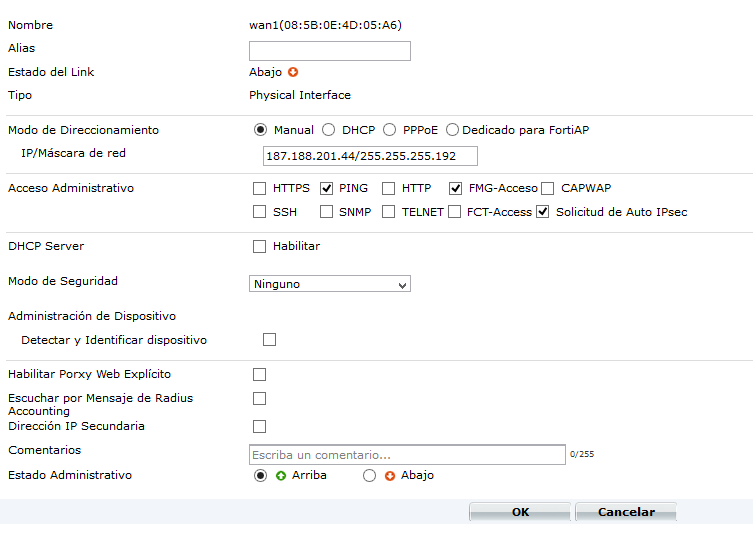


**CONFIGURACION DE RED/INTERFACES/ INTERNAL**

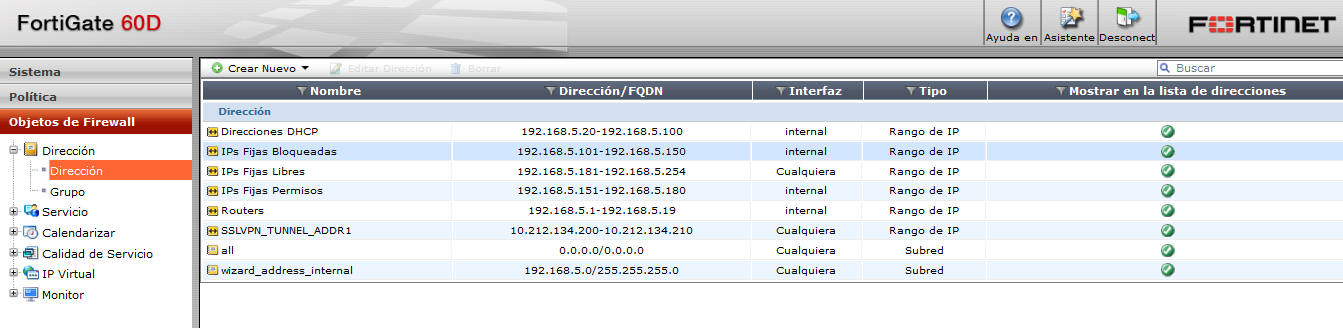
**CONFIGURACION RED/DNS**



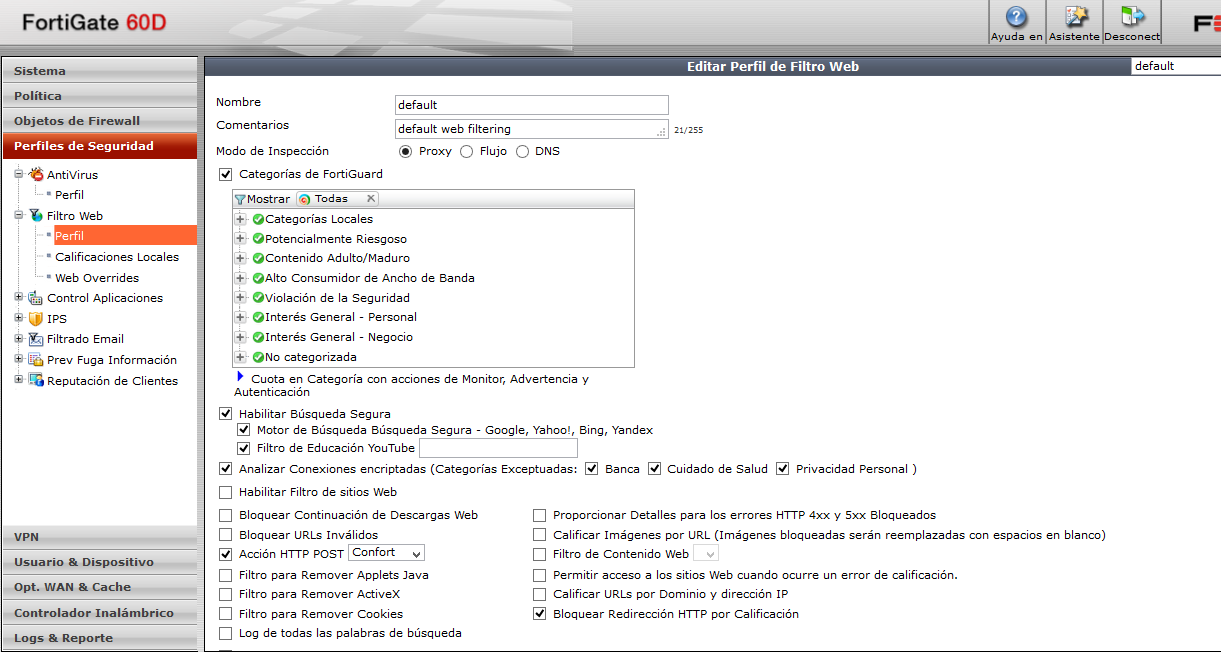
**CONFIGURACION DE RED/INTERFACES/WAN 1**



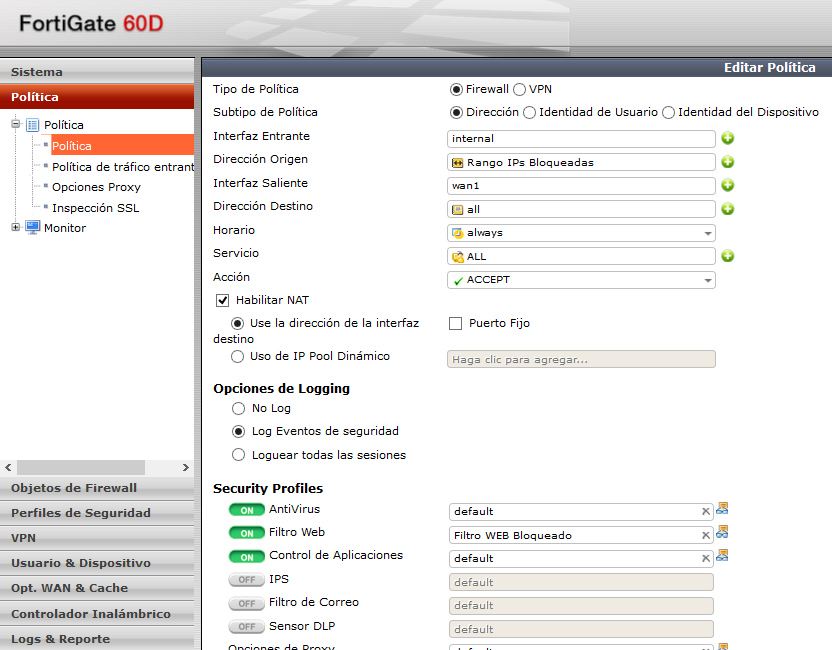
**CONFIGURACION DE OBJETOS DE FIREWALL**



**CREAR UN FILTRO WEB**

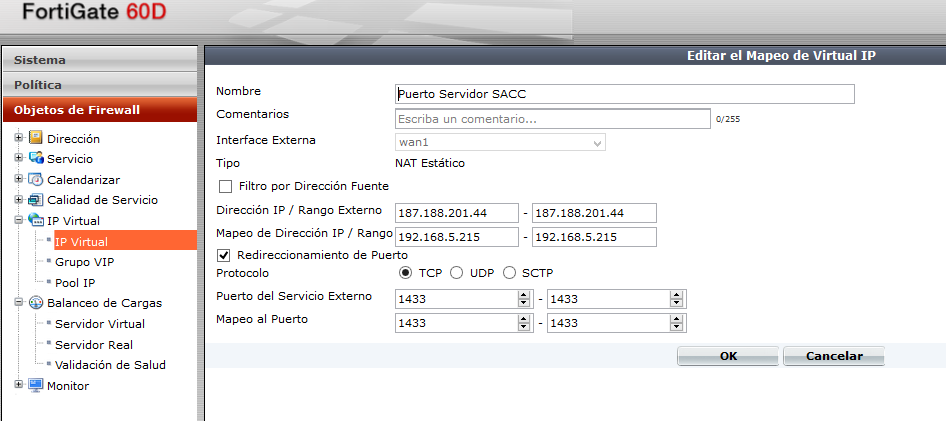


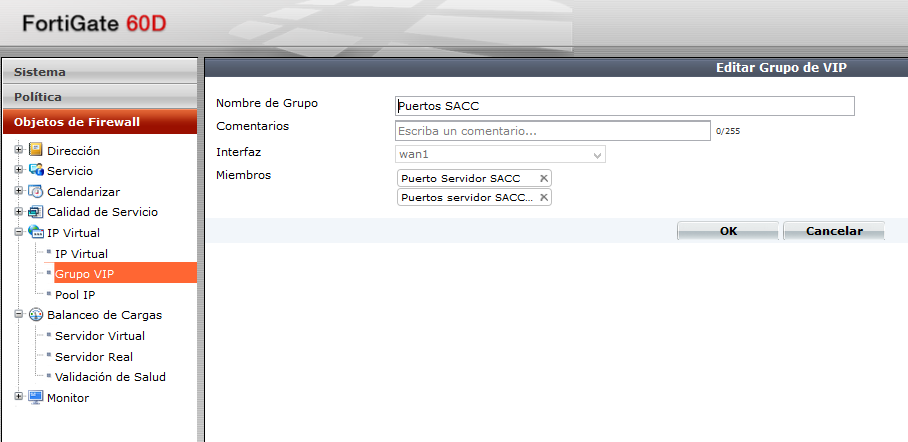
**CREAR POLITICAS PARA EL BLOQUEO DE INTERNET**

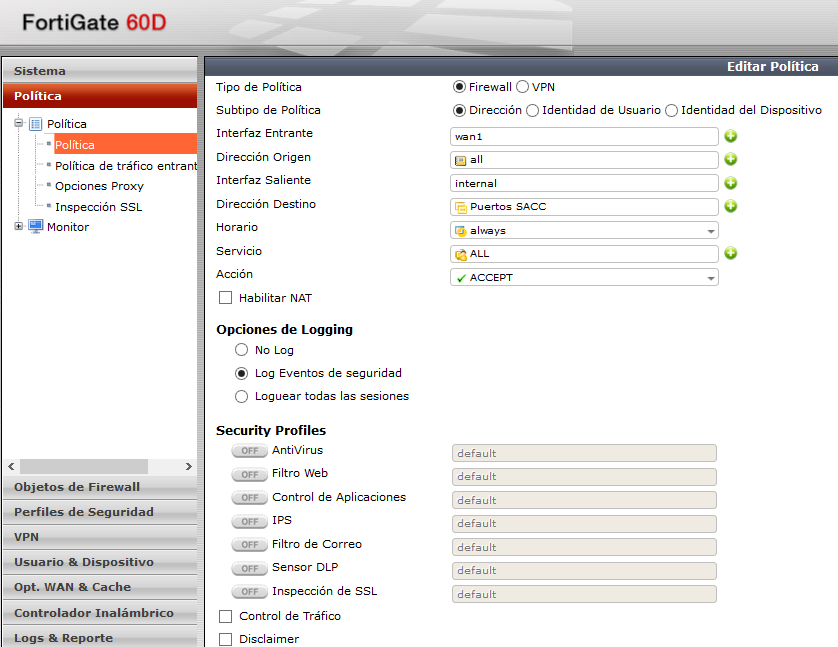


**ABRIR PUERTOS PARA CONEXIÓN DE SUCURSALES**

1. **CREAR IP VIRTUAL PARA MAPEO DE PUERTOS 1433**



1. **Crear un Grupo y asignar las IP Virutales Creadas**
2. **Crear una política con los siguientes parámetros**



**ABRIR PUERTOS PARA SACC**

The solution involves creating multiple VIPs that map sessions from the wan1 IP address to the PC IP address and adding the VIPs to a VIP group and adding that VIP group to a wan1 to internal security policy.

1 Go to Firewall Objects > Virtual IP > Virtual IP and select Create New to add a virtual IP that maps connections to the wan1 interface on ports 7882 to 7999 to the server.

|  |  |
| --- | --- |
| Name | Port Range VIP |
| External Interface | wan1 |
| Type | Static NAT |
| External IP Address/Range | 172.20.120.14-172.20.120.14 |
| Mapped IP Address/Range | 192.168.1.110-192.168.1.110 |

2 Select Port Forwarding and configure the following port forwarding settings:

|  |  |
| --- | --- |
| Protocol | TCP |
| External Service Port | 7882 - 7999 |
| Map to Port | 7882 - 7999 |

3 Select OK to save the VIP.

4 Select Create New to add a virtual IP that maps connections to the wan1 interface on UDP port 2119 to the server.

|  |  |
| --- | --- |
| Name | First UDP Port VIP |
| External Interface | wan1 |
| Type | Static NAT |
| External IP Address/Range | 172.20.120.14-172.20.120.14 |
| Mapped IP Address/Range | 192.168.1.110-192.168.1.110 |

5 Select Port Forwarding and configure the following port forwarding settings:

|  |  |
| --- | --- |
| Protocol | UDP |
| External Service Port | 2119 |
| Map to Port | 2119 |

6 Select OK to save the VIP.

7 Select Create New to add a virtual IP that maps connections to the wan1 interface on UDP port 2995 to the server.

|  |  |
| --- | --- |
| Name | Second UDP Port VIP |
| External Interface | wan1 |
| Type | Static NAT |
| External IP Address/Range | 172.20.120.14-172.20.120.14 |
| Mapped IP Address/Range | 192.168.1.110-192.168.1.110 |

8 Select Port Forwarding and configure the following port forwarding settings:

|  |  |
| --- | --- |
| Protocol | UDP |
| External Service Port | 2995 |
| Map to Port | 2995 |

9 Select OK to save the VIP.

10 Go to Firewall Objects > Virtual IP > VIP Group and select Create New to add a VIP Group that includes all three VIPs.

|  |  |
| --- | --- |
| Group Name | Server VIP Group |
| Interface | wan1 |

11 Add Server Port Range, First UDP Port VIP, and Second UDP Port VIP to the Members list.

12 Go to Policy > Policy > Policy and select Create New to add a policy that accepts includes the VIP Group.

|  |  |
| --- | --- |
| Source Interface/Zone | wan1 |
| Source Address | all |
| Destination Interface/Zone | internal |
| Destination Address | Server VIP Group |
| Schedule | always |
| Service | ANY |
| Action | ACCEPT |

13 Select OK to save the security policy.

|  |  |
| --- | --- |
|  | If you select NAT, the source address is changed to the internal interface address. Normally, you would not want to perform source NAT since this has the affect of hiding the actual source address of the sessions. |