

POLÍTICAS DE FIREWALL DEL SERVIDOR

Resumen Ejecutivo

El servidor GameCenter utiliza **UFW (Uncomplicated Firewall)** con políticas restrictivas por defecto y **fail2ban** para protección contra ataques de fuerza bruta.

Políticas Generales

Política por Defecto

- ENTRADA (Incoming): DENY - Todo bloqueado por defecto
- SALIDA (Outgoing): ALLOW - Todo permitido
- REENVÍO (Forward): DENY - Bloqueado por defecto

Filosofía de seguridad:

- **Denegar todo** lo que entra
- **Permitir solo** los servicios necesarios
- **Permitir todo** lo que sale (el servidor puede conectarse a internet)

Puertos Abiertos

1. SSH (Puerto 22/TCP)

```
Puerto:      22/TCP
Protocolo:   TCP
Servicio:    OpenSSH Server
Política:    LIMIT (Rate limiting)
Comentario:  SSH con rate limiting
```

Protección especial:

- Rate limiting activado (máximo 6 conexiones en 30 segundos)
- Fail2ban monitoreando intentos fallidos
- Bloqueo automático después de 5 intentos fallidos

Comando aplicado:

```
ufw limit 22/tcp comment 'SSH con rate limiting'
```

2. DNS (Puerto 53/TCP y UDP)

```
Puerto:      53/TCP y 53/UDP
Protocolo:   TCP y UDP
Servicio:    BIND9 DNS Server
Política:    ALLOW
Comentario: DNS TCP y DNS UDP
```

Propósito:

- Resolución de nombres de dominio
- DNS64 para traducción IPv4 → IPv6
- Consultas DNS desde clientes de la red

Comandos aplicados:

```
ufw allow 53/tcp comment 'DNS TCP'
ufw allow 53/udp comment 'DNS UDP'
```

3. HTTP (Puerto 80/TCP)

```
Puerto:      80/TCP
Protocolo:   TCP
Servicio:    Nginx Web Server
Política:    ALLOW
Comentario: HTTP Web Server
```

Propósito:

- Servidor web para página de bienvenida
- Portal de información del servidor
- Acceso HTTP desde clientes

Comando aplicado:

```
ufw allow 80/tcp comment 'HTTP Web Server'
```

4. DHCPv6 (Puertos 546-547/UDP)

```
Puerto:      546/UDP (Cliente)
              547/UDP (Servidor)
```

```
Protocolo: UDP
Servicio: ISC DHCP Server v6
Política: ALLOW
Comentario: DHCPv6 Server y Client
```

Propósito:

- Asignación automática de direcciones IPv6
- Configuración de DNS en clientes
- Gestión de leases DHCP

Comandos aplicados:

```
ufw allow 547/udp comment 'DHCPv6 Server'
ufw allow 546/udp comment 'DHCPv6 Client'
```

5. FTP Pasivo (Puertos 21000-21010/TCP)

```
Puerto: 21000-21010/TCP
Protocolo: TCP
Servicio: FTP Passive Mode
Política: ALLOW
Comentario: FTP Passive Ports
```

Propósito:

- Transferencia de archivos en modo pasivo
- Rango de puertos para conexiones de datos FTP

Comando aplicado:

```
ufw allow 21000:21010/tcp comment 'FTP Passive Ports'
```

🚫 Puertos Bloqueados (Ejemplos)

Todos los demás puertos están **bloqueados por defecto**, incluyendo:

- ✗ **Telnet (23)** - Inseguro, usar SSH
- ✗ **FTP Control (21)** - Solo modo pasivo permitido
- ✗ **SMTP (25)** - No es servidor de correo
- ✗ **MySQL (3306)** - Base de datos no expuesta
- ✗ **PostgreSQL (5432)** - Base de datos no expuesta
- ✗ **RDP (3389)** - No es servidor Windows

- ✗ **VNC (5900)** - No se usa acceso remoto gráfico
-

🔒 Fail2ban - Protección contra Ataques

Servicios Monitoreados

1. SSH

```
Servicio: sshd
Filtro: sshd
Puerto: 22
Intentos: 5 fallos
Tiempo ban: 10 minutos
Acción: Bloqueo de IP
```

Protección:

- Detecta intentos de login fallidos
- Bloquea IP después de 5 intentos
- Desbloqueo automático después de 10 minutos

2. Nginx (HTTP)

```
Servicio: nginx-http-auth
Filtro: nginx-http-auth
Puerto: 80
Intentos: 5 fallos
Tiempo ban: 10 minutos
```

Protección:

- Detecta intentos de autenticación HTTP fallidos
 - Protege contra ataques de fuerza bruta web
-

📊 Tabla Resumen de Puertos

Puerto	Protocolo	Servicio	Estado	Protección Extra
22	TCP	SSH	<input checked="" type="checkbox"/> LIMIT	Rate limiting + fail2ban
53	TCP/UDP	DNS (BIND9)	<input checked="" type="checkbox"/> ALLOW	-
80	TCP	HTTP (Nginx)	<input checked="" type="checkbox"/> ALLOW	fail2ban
546	UDP	DHCPv6 Client	<input checked="" type="checkbox"/> ALLOW	-
547	UDP	DHCPv6 Server	<input checked="" type="checkbox"/> ALLOW	-

Puerto	Protocolo	Servicio	Estado	Protección Extra
21000-21010	TCP	FTP Pasivo	<input checked="" type="checkbox"/> ALLOW	-
Otros	Todos	-	<input checked="" type="checkbox"/> DENY	Bloqueado por defecto

🔍 Comandos de Verificación

Ver estado del firewall

```
sudo ufw status verbose
```

Ver reglas numeradas

```
sudo ufw status numbered
```

Ver logs del firewall

```
sudo tail -f /var/log/ufw.log
```

Ver estado de fail2ban

```
sudo fail2ban-client status
sudo fail2ban-client status sshd
```

Ver IPs bloqueadas

```
sudo fail2ban-client status sshd | grep "Banned IP"
```

Desbloquear una IP manualmente

```
sudo fail2ban-client set sshd unbanip 192.168.1.100
```

🛠️ Modificar Políticas

Agregar nueva regla

```
# Permitir un puerto específico  
sudo ufw allow 8080/tcp comment 'Aplicación personalizada'  
  
# Permitir desde una IP específica  
sudo ufw allow from 2025:db8:10::100 to any port 22  
  
# Permitir un rango de puertos  
sudo ufw allow 3000:3010/tcp
```

Eliminar regla

```
# Ver reglas numeradas  
sudo ufw status numbered  
  
# Eliminar por número  
sudo ufw delete 5  
  
# Eliminar por especificación  
sudo ufw delete allow 8080/tcp
```

Denegar un puerto

```
sudo ufw deny 23/tcp comment 'Telnet bloqueado'
```

🔗 Gestión del Firewall

Habilitar/Deshabilitar

```
# Habilitar  
sudo ufw enable  
  
# Deshabilitar  
sudo ufw disable  
  
# Recargar reglas  
sudo ufw reload
```

Resetear configuración

```
# CUIDADO: Esto borra todas las reglas  
sudo ufw reset
```

Ver logs en tiempo real

```
# Logs de UFW  
sudo tail -f /var/log/ufw.log  
  
# Logs de fail2ban  
sudo tail -f /var/log/fail2ban.log
```

📝 Monitoreo

Script de monitoreo automático

```
# Ejecutar script de monitoreo  
sudo /usr/local/bin/firewall-monitor.sh  
  
# O usar el alias  
sudo fw-monitor
```

Estadísticas de conexiones

```
# Ver conexiones activas  
sudo ss -tulpn  
  
# Ver conexiones por servicio  
sudo ss -tulpn | grep :53    # DNS  
sudo ss -tulpn | grep :22    # SSH  
sudo ss -tulpn | grep :80    # HTTP
```

⚠️ Respuesta a Incidentes

Si detectas un ataque

```
# 1. Ver IPs sospechosas  
sudo tail -100 /var/log/auth.log | grep "Failed password"  
  
# 2. Bloquear IP manualmente  
sudo ufw deny from 192.168.1.100  
  
# 3. Ver intentos de conexión  
sudo journalctl -u ssh -n 100 | grep "Failed"  
  
# 4. Revisar fail2ban  
sudo fail2ban-client status sshd
```

Desbloquear IP legítima

```
# Si bloqueaste una IP por error  
sudo ufw delete deny from 192.168.1.100  
sudo fail2ban-client set sshd unbanip 192.168.1.100
```

📝 Configuración de fail2ban

Archivo de configuración

```
# Editar configuración  
sudo nano /etc/fail2ban/jail.local
```

Parámetros importantes

```
[DEFAULT]  
bantime = 10m      # Tiempo de bloqueo  
findtime = 10m      # Ventana de tiempo para contar fallos  
maxretry = 5        # Intentos antes de bloquear  
  
[sshd]  
enabled = true  
port = 22  
logpath = /var/log/auth.log
```

Reiniciar fail2ban

```
sudo systemctl restart fail2ban
```

☑ Checklist de Seguridad

- Firewall UFW habilitado
- Política por defecto: DENY incoming
- SSH con rate limiting
- fail2ban activo y monitoreando
- Solo puertos necesarios abiertos
- Logs de firewall habilitados
- Monitoreo automático configurado
- Revisar logs semanalmente

- Actualizar reglas según necesidad
 - Auditoría de seguridad mensual
-

Referencias

- **UFW Documentation:** <https://help.ubuntu.com/community/UFW>
 - **fail2ban Documentation:** <https://www.fail2ban.org/>
 - **Ansible UFW Module:**
https://docs.ansible.com/ansible/latest/collections/community/general/ufw_module.html
-

Contacto y Soporte

Para modificar las políticas de firewall:

1. Editar `roles/firewall/tasks/main.yml`
2. Ejecutar: `bash scripts/run/run-firewall.sh`
3. Verificar: `sudo ufw status verbose`

Nota: Cualquier cambio en las políticas debe ser documentado y probado en un entorno de desarrollo primero.