

Rol: Firewall

Configuración de firewall con UFW y fail2ban para proteger el servidor.

¿Qué hace?

- Instala UFW (Uncomplicated Firewall)
- Instala fail2ban (protección contra ataques)
- Configura reglas de firewall
- Habilita rate limiting en SSH
- Abre puertos necesarios para servicios

Política de firewall

- **Entrada:** DENY (denegar todo por defecto)
- **Salida:** ALLOW (permitir todo)

Puertos abiertos

Puerto	Protocolo	Servicio	Protección
22	TCP	SSH	Rate limiting
53	TCP/UDP	DNS	Abierto
546	UDP	DHCPv6 Client	Abierto
547	UDP	DHCPv6 Server	Abierto
21000-21010	TCP	FTP Pasivo	Abierto

Fail2ban

Protege contra:

- Ataques de fuerza bruta SSH
- Escaneo de puertos
- Intentos de login fallidos

Configuración:

- **Bantime:** 1 hora
- **Maxretry:** 5 intentos
- **Findtime:** 10 minutos

Ejecutar solo este rol

```
./run.sh firewall
```

Verificar funcionamiento

```
# Ver estado del firewall
sudo ufw status verbose

# Ver reglas numeradas
sudo ufw status numbered

# Ver estado de fail2ban
sudo systemctl status fail2ban

# Ver IPs baneadas
sudo fail2ban-client status sshd

# Monitoreo en tiempo real
sudo /usr/local/bin/fw-monitor
```

Comandos útiles

```
# Permitir IP específica
sudo ufw allow from 2025:db8:10::10

# Denegar IP específica
sudo ufw deny from 2025:db8:10::10

# Eliminar regla
sudo ufw delete [número]

# Desbanear IP
sudo fail2ban-client set sshd unbanip 2025:db8:10::10
```

Archivos creados

- `/etc/ufw/` - Configuración de UFW
- `/etc/fail2ban/jail.local` - Configuración de fail2ban
- `/usr/local/bin/firewall-monitor.sh` - Script de monitoreo
- `/usr/local/bin/fw-monitor` - Alias del script

Reglas avanzadas (opcionales)

Filtrado por rol de VM

Si tienes VMs configuradas en el inventario, el firewall puede:

- Permitir SSH solo desde VMs con rol `admin`
- Bloquear SSH desde VMs con rol `auditor` o `cliente`

Esta funcionalidad se activa automáticamente cuando agregas VMs al grupo `[ubuntu_desktops]` en `inventory/hosts.ini`.

Seguridad avanzada (opcional)

Para habilitar seguridad paranóica:

```
# En group_vars/all.yml
enable_advanced_security: true
```

Esto incluye:

- Auditoría del sistema (auditd)
- Hardening adicional
- Monitoreo de integridad de archivos