CSF + ModSecurity en nginx: MODSEC_LOG y regex custom

El problema

En servidores DirectAdmin con **nginx + ModSecurity 3** (no Apache), CSF/LFD no detecta los bloqueos de ModSecurity. Un usuario puede ser bloqueado repetidamente por ModSecurity (HTTP 406) sin que LFD lo registre ni tome acción (ban temporal, notificación, etc.).

Consecuencia: ModSecurity bloquea requests pero LFD es **ciego** a esos eventos. Si una IP llega a `csf.deny`, es por otro mecanismo (DA BFM, manual), nunca por `LF_MODSEC`.

Causa raíz (triple)

1. `MODSEC_LOG` apunta al fichero equivocado

El default de CSF es:

```
MODSEC_LOG = "/var/log/httpd/error_log"
```

Pero en DirectAdmin con nginx + ModSecurity 3, **ModSecurity corre en nginx, no en Apache**. Los eventos de "Access denied" se escriben en los **error.log per-domain de nginx**, no en httpd:

```
/var/log/nginx/domains/dominio.com.error.log
```

2. CSF no tiene regex para nginx-modsec3

El fichero built-in `RegexMain.pm` solo tiene regex para el formato ModSecurity v2 (Apache). El formato nginx-modsecurity3 tiene campos extra (`PID#TID: *CONN`) que la regex no matchea.

Formato Apache-modsec2:

```
[date] [error] [client IP] ModSecurity: Access denied ...
```

Formato nginx-modsec3:

```
YYYY/MM/DD HH:MM:SS [error] PID#TID: *CONN [client IP] ModSecurity: Access denied ...
```

3. Logs distribuidos por dominio

Los "Access denied" de nginx-modsec3 se escriben en los error.log per-domain de nginx, no en un fichero centralizado. CSF necesita leer TODOS los error.log de dominio.

Solución

Paso 1: Corregir `MODSEC_LOG` en `csf.conf`

```
# En /etc/csf/csf.conf, cambiar:
MODSEC_LOG = "/var/log/nginx/domains/*.error.log"
```

CSF soporta globs — se evalúan al iniciar LFD. Cada `*.error.log` de cada dominio será monitoreado.

Consecuencia: tras crear un nuevo dominio, hay que reiniciar LFD (`csf -ra`) para que monitorice su error.log nuevo.

Paso 2: Crear regex custom para nginx-modsec3

En `/usr/local/csf/bin/regex.custom.pm`, añadir **dentro de la sección de reglas** (antes del `return ()` final):

```
# nginx-modsecurity3 format
# YYYY/MM/DD HH:MM:SS [error] PID#TID: *CONN [client IP] ModSecurity: Access denied ...
```

```
if (($globlogs{MODSEC_LOG}{$lgfile}) and ($line =~ /^\S+ \S+ \[\S+\] \S+ \*\d+ \[client
(\S+)\] ModSecurity:(( \[[^\]]+\])*)? Access denied/)) {
    my $ip = $1;
    my $domain = "";
    if ($line =~ /\[hostname "([^"]+)"\]/) {$domain = $1}
    my $ruleid = "unknown";
    if ($line =~ /\[id "(\d+)"\]/) {$ruleid = $1}
    $ip =~ s/^::ffff://;
    return ("mod_security v3 (id:$ruleid domain:$domain) triggered by", $ip, "modsecnginx",
"5", "80,443", "7200", "0");
}
```

Qué hace:

- Matchea el formato nginx-modsec3
- Extrae IP, dominio (hostname), y rule ID
- Retorna al LFD con trigger type "modsecnginx", 5 hits para ban, puertos 80/443, ban temporal de 2 horas

Paso 3: Verificar sintaxis y reiniciar

```
# Verificar que el Perl compila
perl -c /usr/local/csf/bin/regex.custom.pm

# Reiniciar CSF + LFD
csf -ra
```

Paso 4: Verificar que LFD monitoriza los ficheros

```
# Debe mostrar líneas de "watching" para *.error.log
grep "watching" /var/log/lfd.log | grep nginx | tail -10
```

Persistencia

- `regex.custom.pm` **sobrevive upgrades de CSF** — es el lugar oficial para customizaciones

- `csf.conf` también sobrevive upgrades, pero verificar tras actualizaciones mayores de CSF
- **Los globs en `MODSEC_LOG` solo se evalúan al iniciar LFD** — tras crear un nuevo dominio, reiniciar LFD con `csf -ra`

Diagnóstico

Si sospechas que LFD no está detectando bloqueos ModSecurity:

```
# 1. Verificar que hay eventos ModSecurity en los logs nginx
grep "ModSecurity: Access denied" /var/log/nginx/domains/*.error.log | tail -5

# 2. Verificar que MODSEC_LOG apunta a nginx
grep "MODSEC_LOG" /etc/csf/csf.conf

# 3. Verificar que LFD registra triggers modsec
grep "modsec" /var/log/lfd.log | tail -10

# 4. Si no hay nada en lfd.log pero sí hay eventos en nginx:
# → MODSEC_LOG incorrecto o regex no matchea
```

Servidores aplicados

Servidor	Fecha	Estado
srv120	2026-03-05	Activo
srv121	2026-03-05	Activo
kvm456	2026-03-05	Activo
amazzal	2026-03-05	Activo
dar	2026-03-05	Activo
titrit	N/A	No tiene modsec en nginx

Checklist para nuevos servidores DA

- [ ] `MODSEC_LOG` en csf.conf apunta a `/var/log/nginx/domains/*.error.log`
- [ ] `regex.custom.pm` tiene la regex para nginx-modsec3
- [ ] `perl -c regex.custom.pm` compila sin errores
- [ ] `csf -ra` ejecutado
- [ ] Verificar con `grep "watching" /var/log/lfd.log | grep nginx`

Revision #1
Created 2026-03-24 17:34:48 UTC by Abkrim
Updated 2026-03-24 17:34:48 UTC by Abkrim