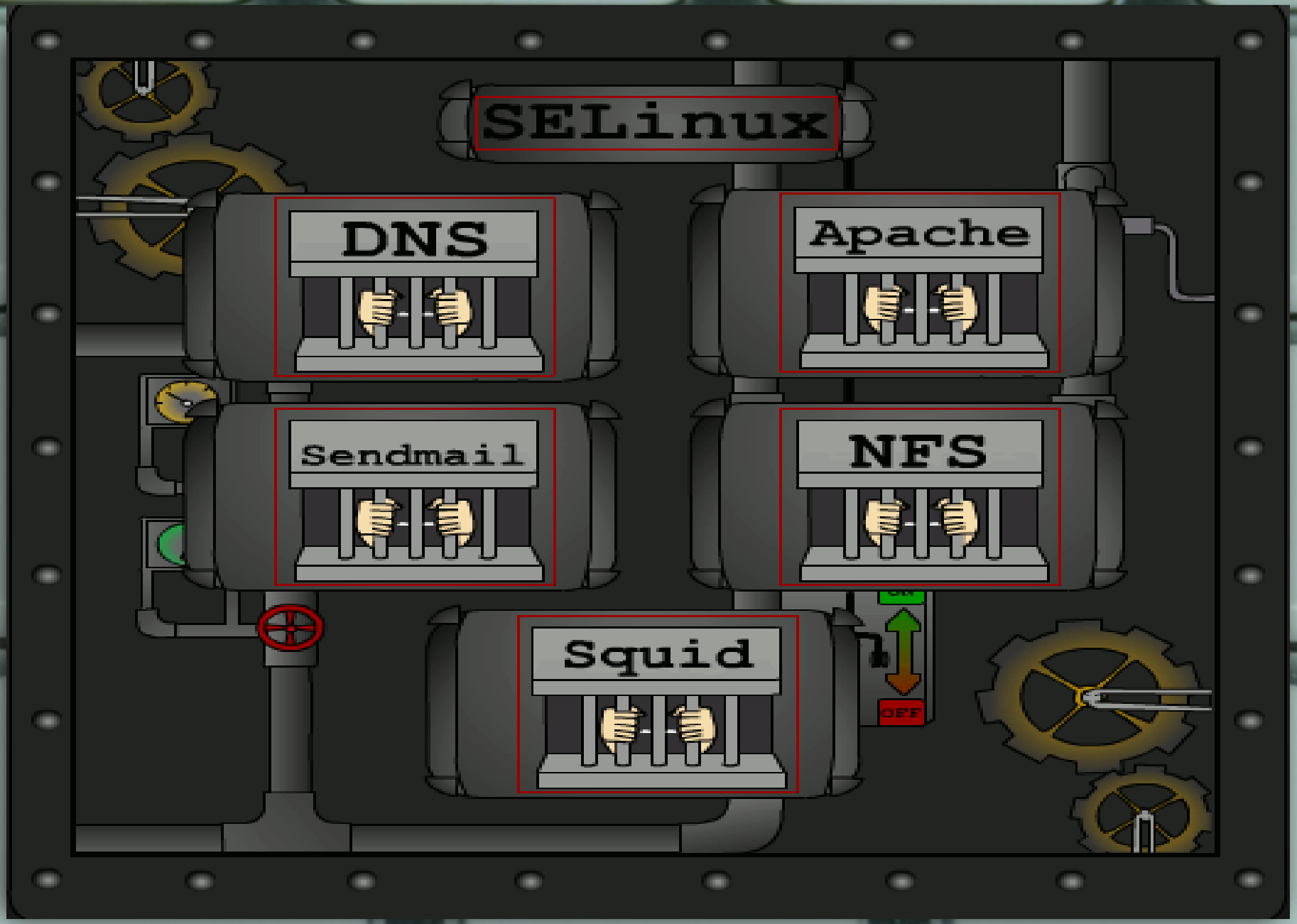
SELinux
DNS
Apache
Sendmail
NFS
Squid
OFF

¿Que es SELinux?

- SELinux del inglés Security-Enhanced Linux, que se traduce como Seguridad Mejorada de Linux
- es una implementación de seguridad para GNU/Linux que provee una variedad de políticas de seguridad, incluyendo el estilo de acceso a los controles del Departamento de Defensa de EE.UU., a través del uso de módulos de Seguridad en el núcleo de Linux.

SECURITY CONTEXT

- The key to SElinux is the security context. All processes have a security context and all objects, like files, devices etc., also have a security context.

user_u:role_r:type_t:s0:c0

(actually, s0-s0:c0.c1023 for the last two fields)

A context is made up from a number of parts, but the key one is called a type.

Basically, when a process is compared with an object, *it is their types that are compared* and used to lookup what that process is allowed to do with that object. SElinux is based on the Type Enforcement™ security model.

Acceso a un file hay que tener:

- acceso regular (permisos ya vistos)
- el acceso SELinux!

Incluso a root se le puede denegar el acceso a un file si los contextos de seguridad no coinciden.

SELinux Decision Process