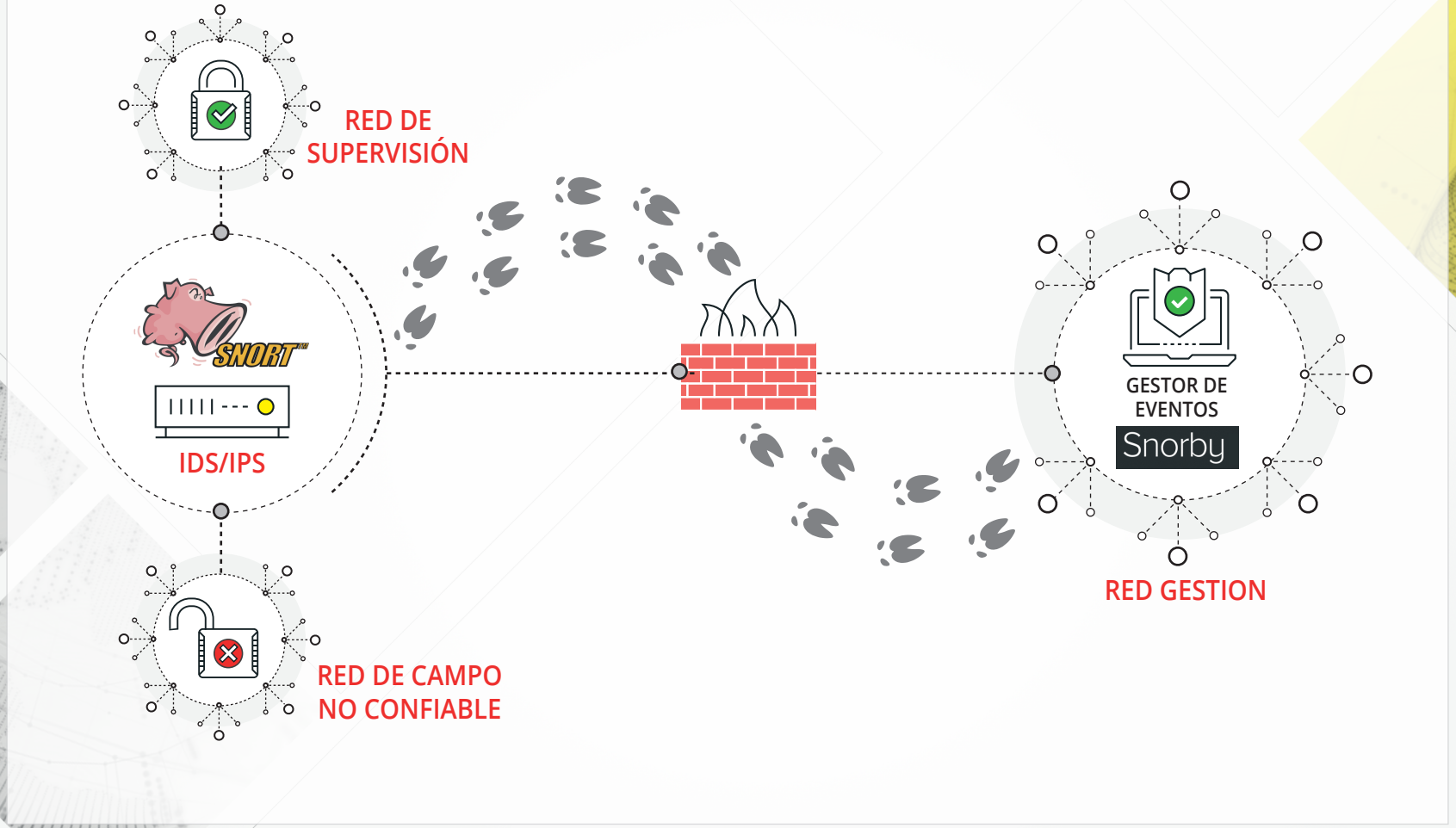
Despliegue de un IDS/IPS y gestión centralizada de alertas



certsi_

Reglas Snort

```
[Acción][Protocolo][IP_Origen][Puerto_Origen] -> [IP_Destino][Puerto_Destino] ( [Opciones de regla] )
```

Reglas para sistemas de control

Quickdraw

- Modbus
- Ethernet/IP
- DNP3

Cisco Talos

- IEC60870-5-104

INSTALACIÓN DE SNORT EN SENSOR IDS

```
apt install libdnet libdnet-dev libpcap-dev make \
automake gc flex bison libdumbnet-dev
ln -s /usr/include/dumbnet.h /usr/include/dnet.h
ldconfig
apt install snort
```

Configuración de DAQ

```
wget \
https://www.snort.org/downloads/snort/daq-[X.X.X].tar.gz
tar zxf daq-[X.X.X].tar.gz
cd daq-[X.X.X]
./configure
make && make install
ldconfig
```

[X.X.X] debe ser cambiado por la versión actual

Cambios en snort.conf

```
ipvar HOME_NET [rango_red]
ipvar EXTERNAL_NET !HOME_NET
config daq: afpacket
config daq_mode: inline
output unified2: filename [fichero] limit 128
```

Cambios en snort.debian.conf

```
DEBIAN_SNORT_INTERFACES = "eth0:eth1"
```

INSTALACIÓN DE BARNYARD2 EN SENSOR IDS

```
apt install libtool
git clone https://github.com/firnsy/barnyard2.git
./autogen.sh
./configure
make && make install
touch /var/log/snort/barnyard2.waldo
```

Cambios en Barnyard.conf

```
output database alert,mysql user=[usuario] \
password=[contraseña] dbname=[nombre_bbdd] \
host=[host_remoto]
```

INSTALACIÓN DE SNORBY EN EQUIPO GESTIÓN

```
apt install apache2 apach2-dev mysql-server \
libmysqlclient-dev ruby-full \
postgreesql-server-dev-9.5 libcurl4-apoenssl-dev
```

Creación de base de datos

```
mysql -u root -p
> create database [snorby];
> create user '[usuario]@'%' identified by \
'[contraseña]'
> grant all privileges on [snorby].* to [usuario]@'%' \
with grant option;
> flush privileges;
> quit
```

Descarga de Snorby

```
git clone https://github.com/Snorby/snorby.git
cp -r snorby /var/www/html
```

Cambios en fichero Gemfile

```
gem 'rake', '0.9.2' -> gem 'rake', '> 0.9.2'
despues de gem 'json','X.X' añadir -> gem 'thin'
en el apartado group (:development) to comentar -> gem \
'thin'
```

Cambios en fichero Gemfile.lock

```
rake (0.9.2) -> rake (0.9.2.2)
```

Instalación de gemas

```
gem install rails bundler passenger wkhtmltopdf \
do_postgres -v '0.10.16'
bundle install
cp config/snorby_config.yml.example \
config/snorby_config.yml
cp config/database.yml.example config/database.yml
passenger-install-apache2-module
touch/etc/apache2/sites-available/snorby.conf
ln -s /etc/apache2/sites-available/ \
snorby.conf/etc/apache2/sites-enabled/snorby.conf
rm/etc/apache2/sites-enabled/000-default.conf
```

Cambios en snorby.conf

```
LoadModule passenger_module \
/var/lib/gems/2.3.0/gems/passenger-5.0.30/buildout/ \
apache2/mod_passenger.so
PassengerRoot /var/lib/gems/2.3.0/gems/passenger-5.0.30
PassengerDefaultRuby /usr/bin/ruby2.3
Servername [IP_Base_datos]
DocumentRoot /var/www/html/snorby/public
<Directory /var/www/html/>
 AllowOverride all
 Order allow,deny
 Allow from all
 Options -MultiViews
</Directory>
```

EJECUCIÓN

Snort y Barnyard2

```
snort -Q -i eth0:eth1 -c snort.conf
barnyard2 -c /etc/snort/barnyard2.conf -d \
/var/log/snort -f snort.conf -w \
/var/log/snort/barnyard2.waldo
```

Snorby

```
RAILS_ENV=production bundle exec rake snorby:setup
```

CREACIÓN CONEXIÓN PUENTE EN SENSOR IDS

```
apt install brige-utils
```

Cambiar /etc/network/interfaces

```
auto br0
iface br0 inet manual
        bridge-ports eth0 eth1
        bridge_stp off
        bridge_fd 0
```

FUNCIONAMIENTO IDS/IPS

```
ifconfig br0 down
"Ejecución del IPS"
ifconfig br0 up -arp
```

certsi_