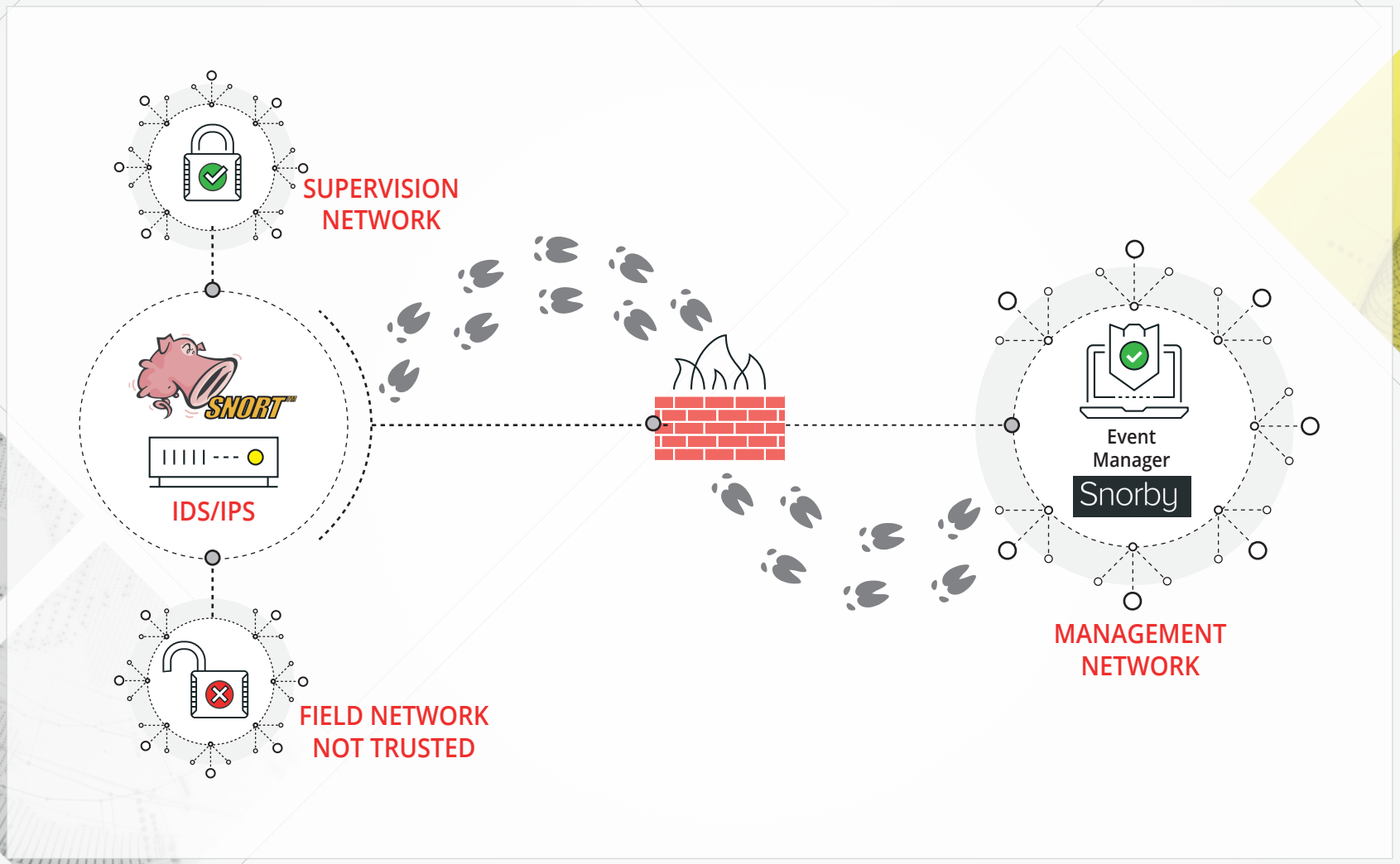
IDS/IPS and Centralized Alert Management System Deployment



certsi_

Snort Rules

```
[Action][Protocol][Source_IP][Source_Port] -> [Dst_IP][DST_Port] ( [Rule Options] )
```

Control System Rules

Quickdraw

- Modbus
- Ethernet/IP
- DNP3

Cisco Talos

- IEC60870-5-104

SNORT INSTALLATION ON IDS SENSOR

```
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
```

DAQ Configuration

```
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] msut be changed by actual version

snort.conf parametrization

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

snort.debian.conf parametrization

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

BARNYARD2 INSTALLATION ON IDS SENSOR

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

Barnyard.conf parametrization

```
output database alert,mysql user=[user] \
password=[password] dbname=[bbdd_name] \
host=[remote_host]
```

SNORBY INSTALLATION ON MANAGEMENT DEVICE

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

Database creation

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

Snorby download

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

Gemfile file changes

```
gem 'rake', '0.9.2' -> gem 'rake', '> 0.9.2'
before gem 'json','X.X' add -> gem 'thin'
in part group (:development) to comment-> gem 'thin'
```

Gemfile.lock file changes

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

Gem installation

```
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
```

snorby.conf parametrization

```
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 [Database_IP]
DocumentRoot /var/www/html/snorby/public
<Directory /var/www/html/>
 AllowOverride all
 Order allow,deny
 Allow from all
 Options -MultiViews
</Directory>
```

EXECUTION

Snort & 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
```

BRIDGE CONNECTION CREATION IN IDS SENSOR

```
apt install brige-utils
```

/etc/network/interfaces changes

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

RUNNING IDS/IPS

```
ifconfig br0 down
"IPS Execution"
ifconfig br0 up -arp
```

certsi_