

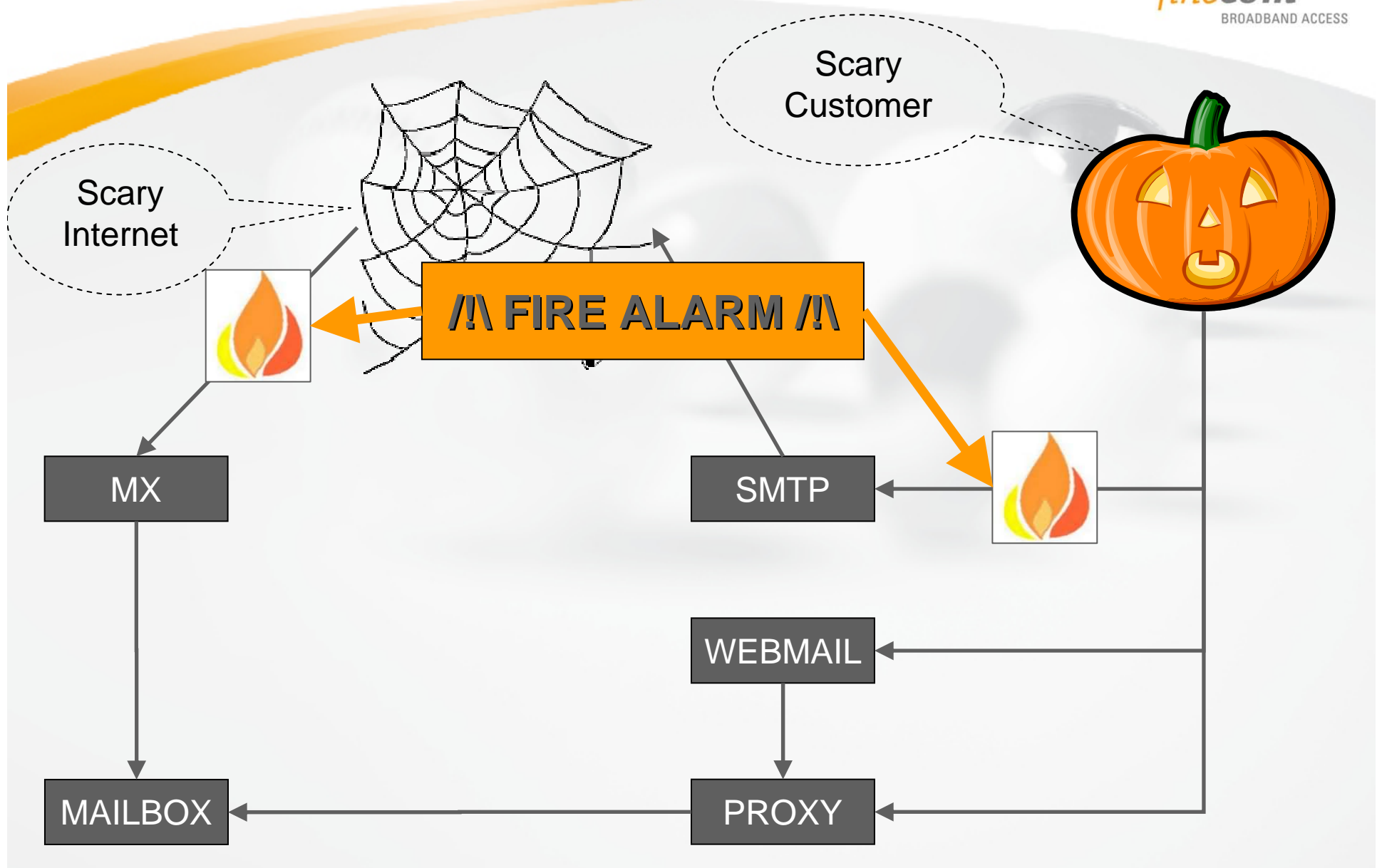
# Large scale SMTP protection

*Pascal Gloor*  
<[pascal.gloor@finecom.ch](mailto:pascal.gloor@finecom.ch)>

# Agenda

- *Protecting your infrastructure from mass mailing, Trojans, viruses, spam, ...*
  - Outgoing SMTP
  - Incoming SMTP
- **AWGL**

# Mail platform overview



# Outgoing SMTP

## Key points

- *Most important is to deliver your service*
- *Some mass mails may be legitimate*
- *You don't want to be a bad "sender"*

# Outgoing SMTP

## Mail traffic classification

- *Follow the white rabbit ...*
- *Who is sending email ?*
  - SASL - SMTP Authentication (username)
  - Cable DHCP (CM MAC address)
  - ADSL radius (username)
  - RIPE inetnum (netname)
  - IP Address (IP) ← SHALL NOT HAPPEN
- *Does it contain a virus ? (bad point)*
- *Is it spam ? (bad point)*
- *Does the mail go out ?*
  - 250 OK (good point)
  - 4xx error (bad point)
  - 5xx error (bad point)

# Outgoing SMTP

## Mail traffic accounting

- *Update your database*
  - Timestamp
  - Sender identification
  - Good or bad points

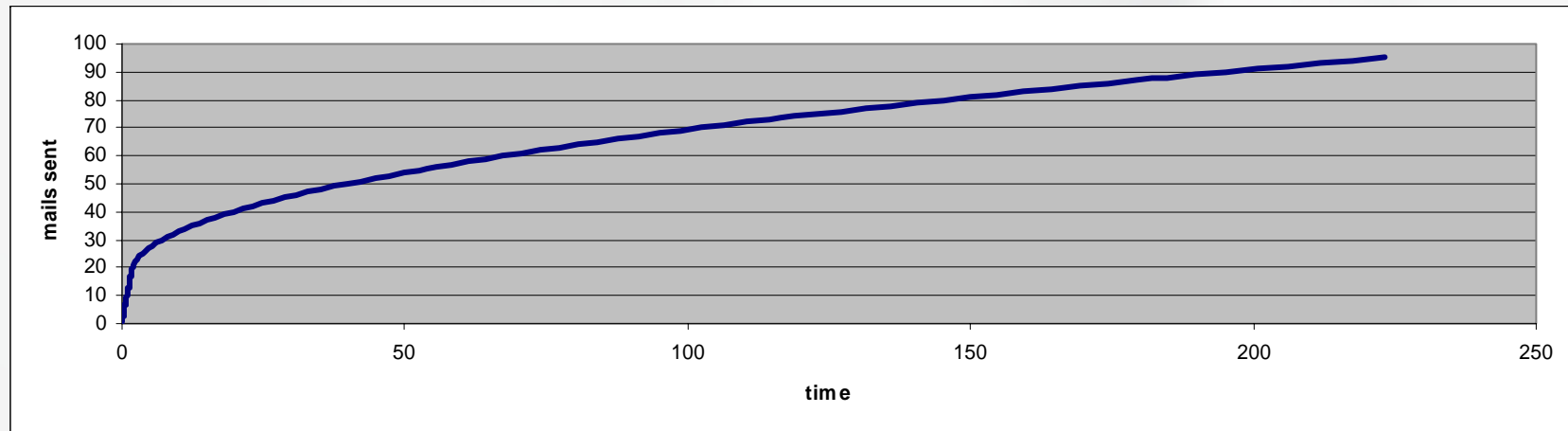
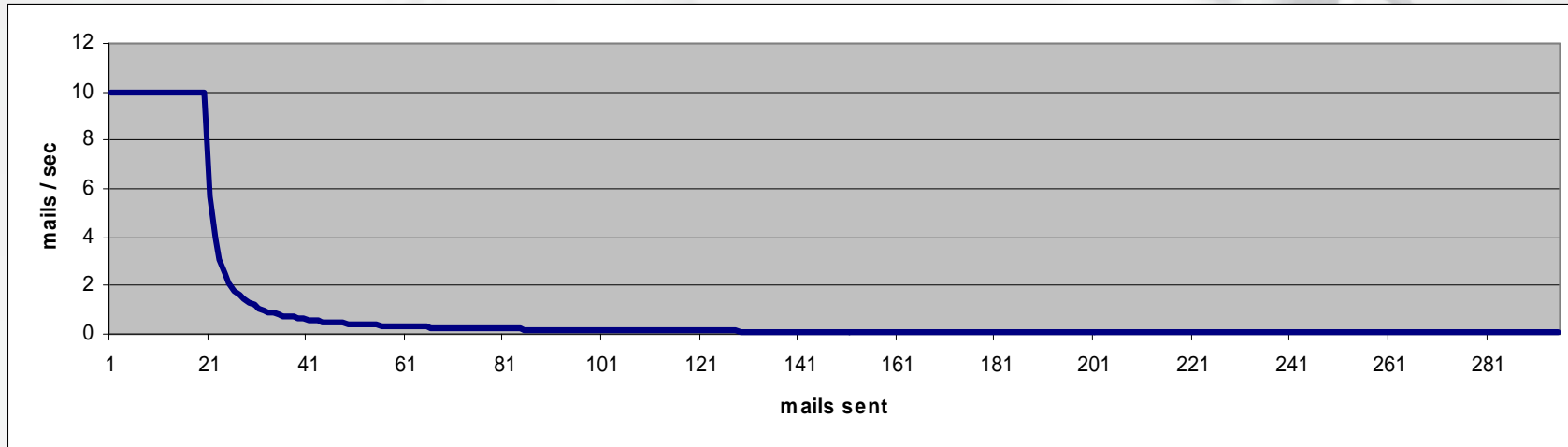
# Outgoing SMTP

## Mail traffic policing

- *Identify the user*
- *Query the database*
  - How many mails sent in the last n minutes ?
  - Percentage of good/bad points ?
- *WAIT*
  - up to 15 seconds based on the mail count
  - up to 15 seconds based on good/bad percentage
  - absolute max, 30 seconds
- *Allow the customer to send his mail*

# Outgoing SMTP

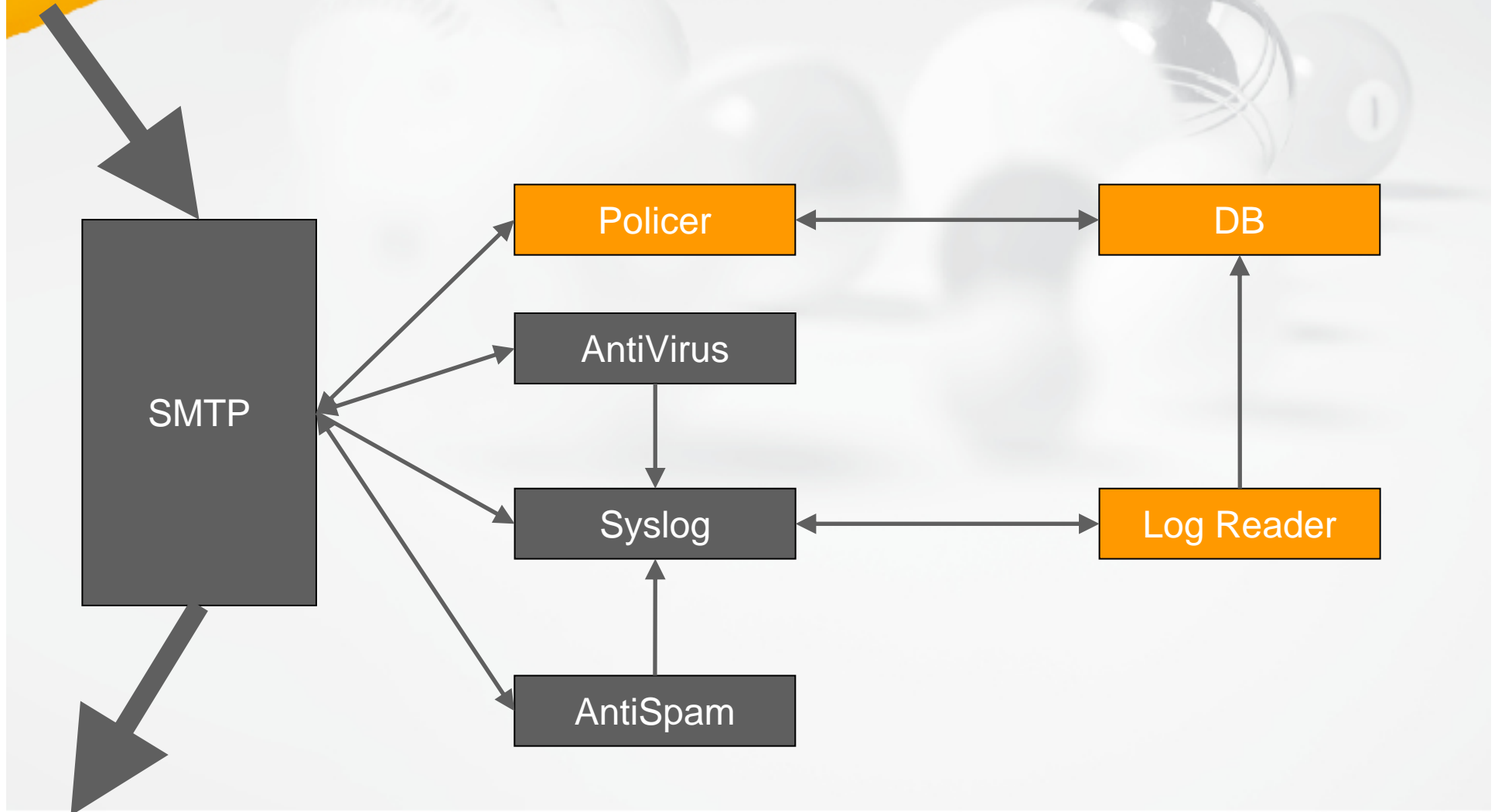
## Mail traffic maximum output



min mail 20 – max mail 200 – mail time 100ms – max sleep 15

# Outgoing SMTP

## Mail traffic flow



# Incoming SMTP

## Key points

- *Greylisting is efficient*
- *Greylisting can be a problem with customers who believe email is a real time service*
- *How to greylist only specific hosts without any manual operation ?*

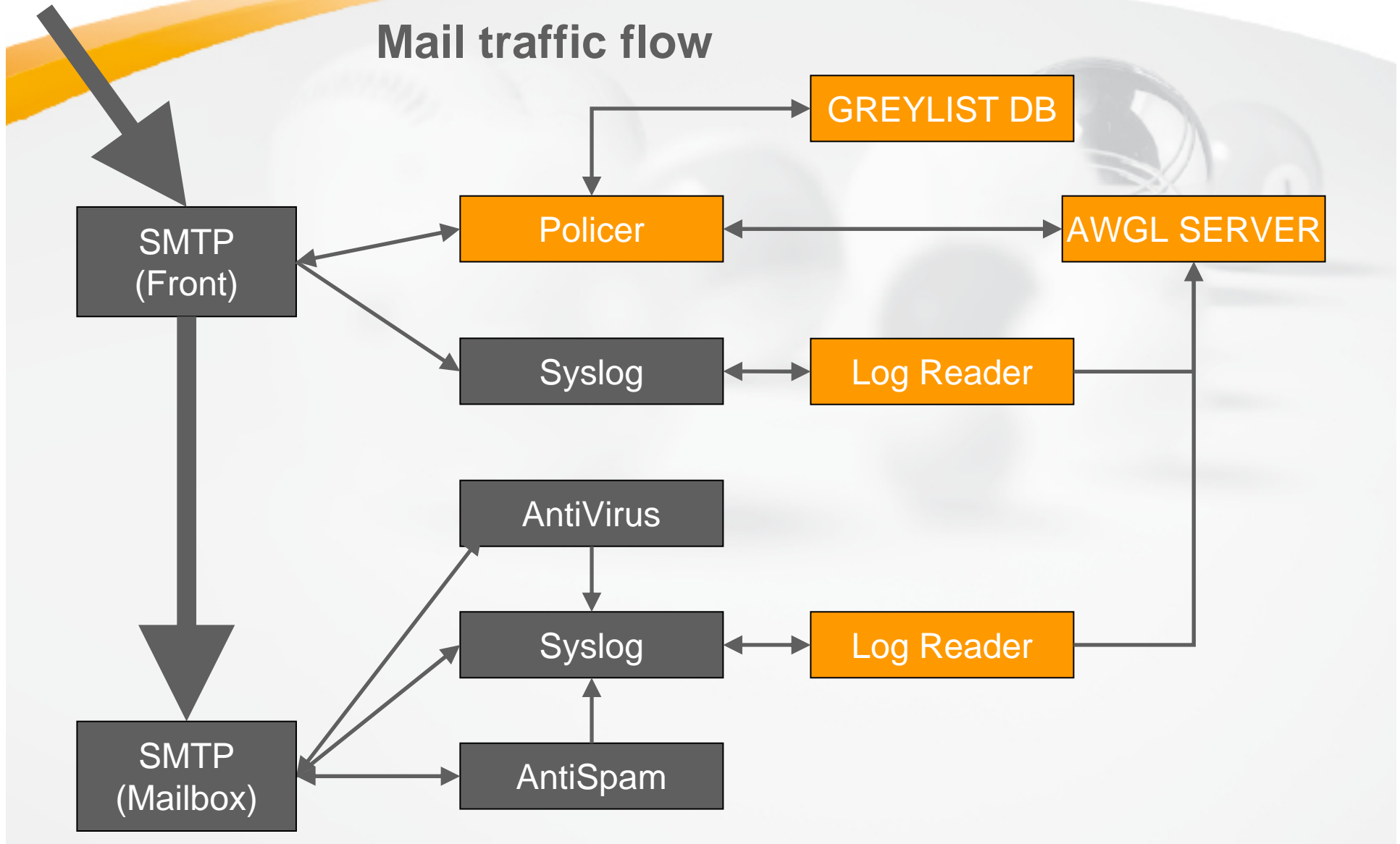
# Incoming SMTP

## What is greylisting ?

- *Many Spammers use a desktop program to directly send spam*
- *Those programs do NOT queue, they are not mail servers*
- *Rejecting the first connection will avoid the retry in most cases*

# Incoming SMTP

## Mail traffic flow



# Incoming SMTP

## AWGL ?

- *Advanced **W**eighted **G**rey**L**isting*
- *Original idea, Perry Lorier, Network Research Group, University of Waikato, New Zealand*
- *Flag IP Addresses (of senders) as ham, spam, virus, unknown (unknown recipient)*
- *Hierarchical flagging (flag all networks from /32 to /0)*

# Incoming SMTP

## AWGL Client (query)

QUERY:

```
./awgl_client \  
  -k username:password \  
  -h awgl.fcom.ch \  
  -i 62.220.132.1 \  
  -q 100
```

ANSWER:

```
ip=62.220.132.1 prefix=62.220.132.1/32  
total=1459 ham=1458 spam=1 virus=0 unknown=0
```

# Incoming SMTP

## AWGL Client (update)

```
QUERY:  
./awgl_client \  
    -k username:password \  
    -h awgl.fcom.ch \  
    -i 62.220.132.1 \  
    -u spam
```

# Incoming SMTP

## AWGL host table

195.49.64.0/18	698	460	234	0	4	34%
195.49.64.0/19	16	15	0	0	1	6%
195.49.96.0/19	682	445	234	0	3	34%
195.49.96.0/20	9	9	0	0	0	n/a
195.49.112.0/20	673	436	234	0	3	35%
195.49.112.0/21	672	435	234	0	3	35%
195.49.112.0/22	18	18	0	0	0	0%
195.49.116.0/22	654	417	234	0	3	36%
195.49.116.0/23	640	411	226	0	3	35%
195.49.116.0/24	640	411	226	0	3	35%
195.49.116.128/25	640	411	226	0	3	35%
195.49.116.128/26	640	411	226	0	3	35%
195.49.116.128/27	640	411	226	0	3	35%
195.49.116.128/28	640	411	226	0	3	35%
195.49.116.136/29	640	411	226	0	3	35%
195.49.116.140/30	640	411	226	0	3	35%
195.49.116.142/31	640	411	226	0	3	35%
195.49.116.142/32	640	411	226	0	3	35%
195.49.116.0/22	14	6	0	0	0	57%

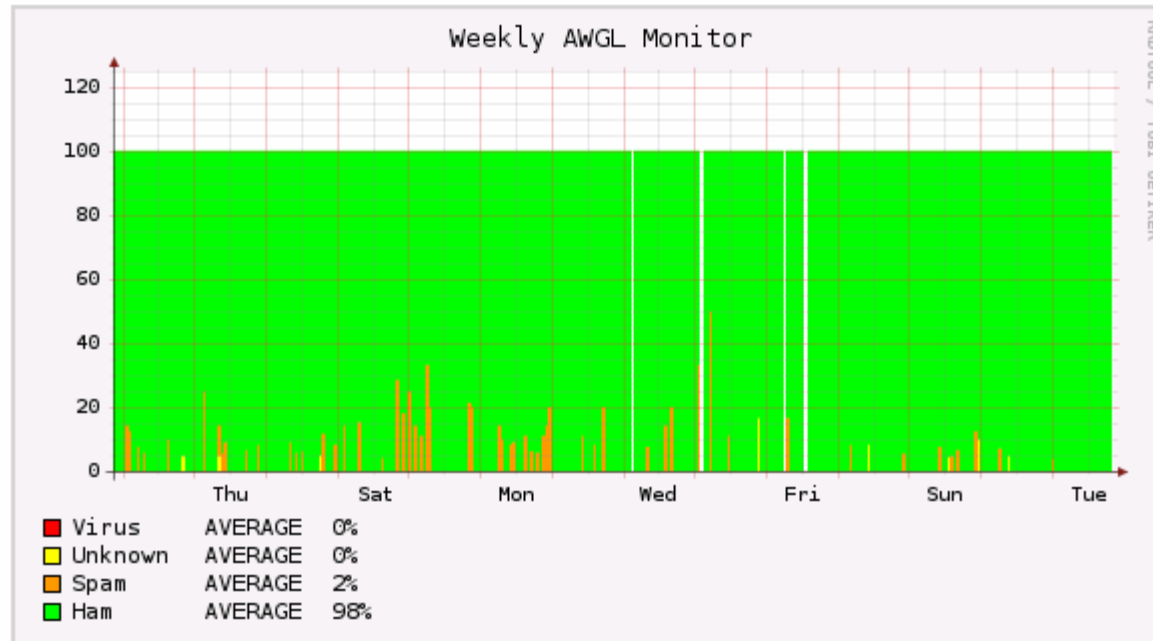
# Incoming SMTP

## AWGL Monitors (1/2)

### Monitor for Bluewin (SMTP Servers)

network: 195.186.18.0/23

{ [Daily](#) | [Weekly](#) | [Monthly](#) | [Yearly](#) }



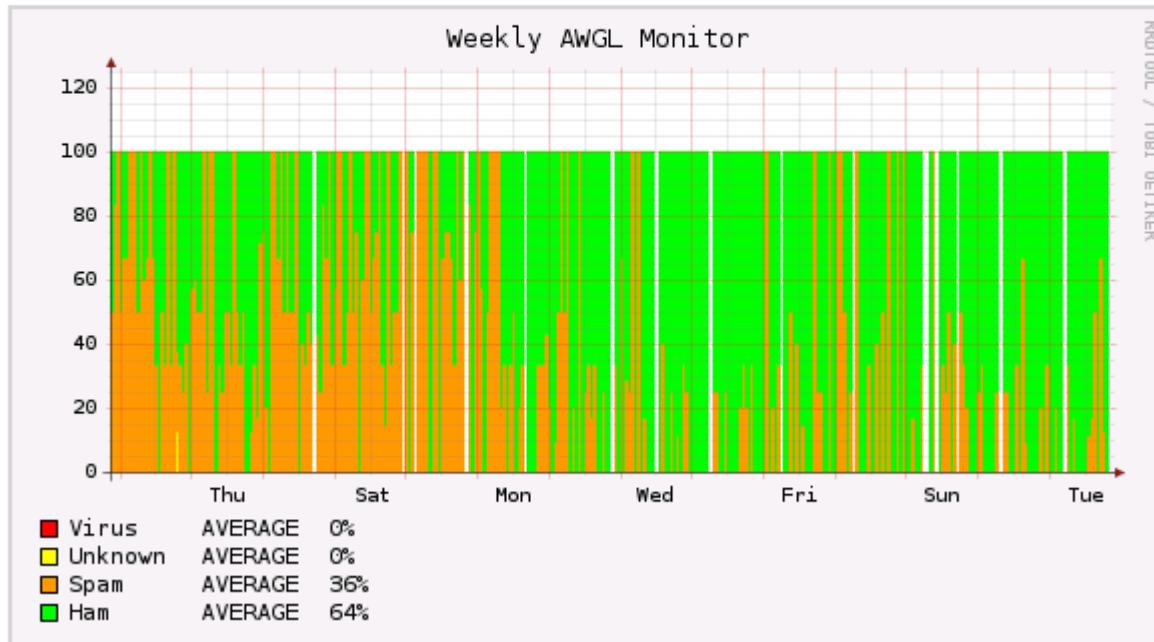
# Incoming SMTP

## AWGL Monitors (2/2)

### Monitor for Sunrise (SMTP Servers)

network: 194.158.229.0/24

{ [Daily](#) | [Weekly](#) | [Monthly](#) | [Yearly](#) }



# Incoming SMTP

## Who can join AWGL?

- *Currently two members (Finecom and Improware)*
- *Beta stage*
- *Need for two or three medium to large ISPs to join us*

# Incoming SMTP

## AWGL in the future

- *Almost certainly free for medium to large “feeders”*
- *Probably non-free (cheap) for read-only access*
- *DNS BL will be free with limited information*

# Questions !?????????



# THANKS!