

DKIM

(DomainKeys Identified Mail, RFC 4871)

Roman Valls Guimerà

Qué es ?



Una sistema para firmar y verificar emails a nivel de MTA usando un par de **llaves publica/privada** y el **RR DNS TXT** para distribuir la llave pública

Autentica el **origen** y sus **contenidos**

NO basado en PKI: No es necesario montar CA (opcional)

No rompe otros sistemas: adopcion asimétrica

Como funciona ?



Envio:

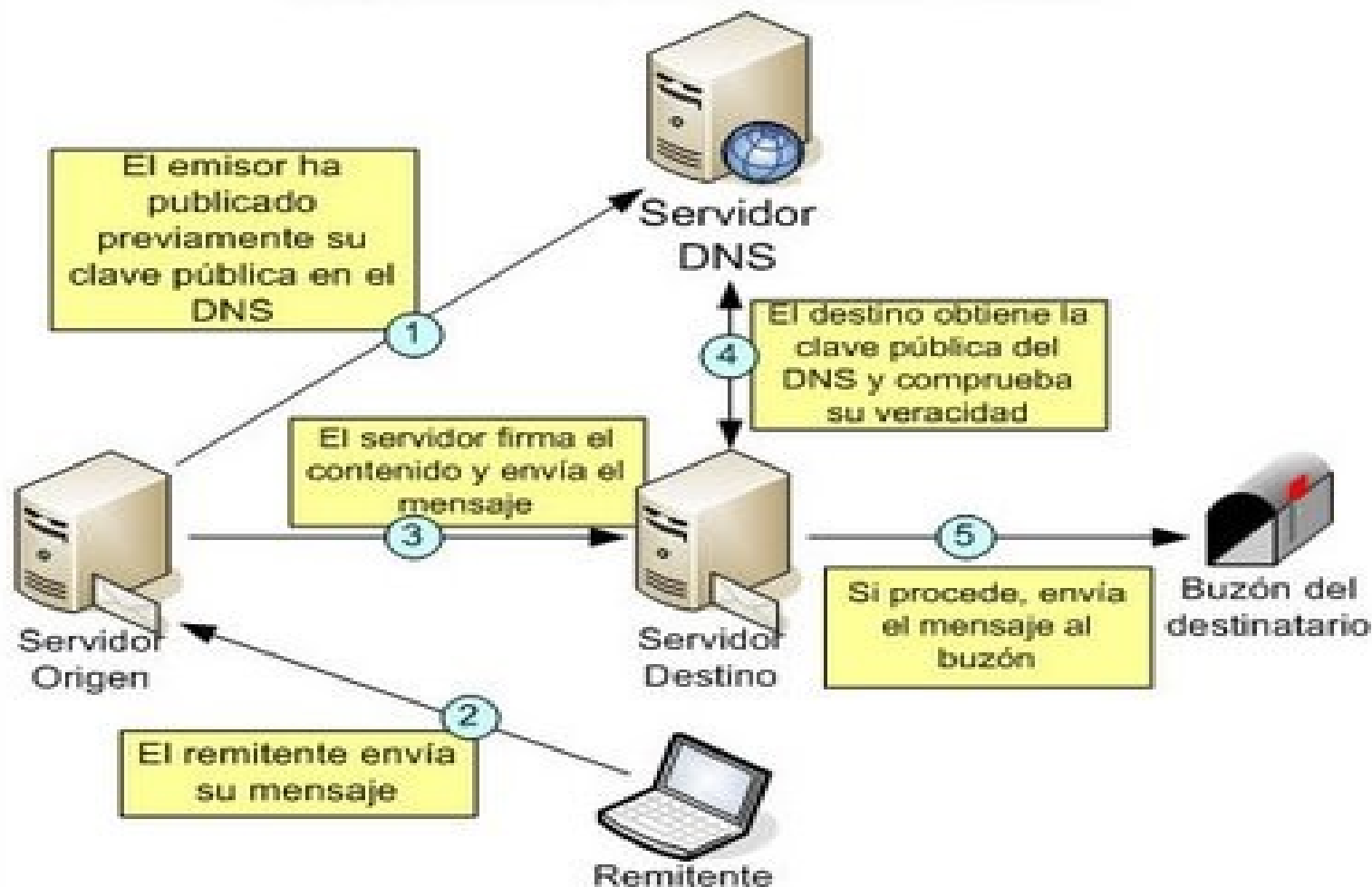
- 1) Firma el mensaje entero (cabeceras & contenidos)
- 2) Llave pública presente en nuestro DNS, privada en MTA
- 3) Los clientes pueden enviar mensajes como siempre, el MTA hará el trabajo

Recepción:

- 1) El MTA extrae la firma y selector de las cabeceras
- 2) Pregunta la llave pública en el DNS remoto y comprueba validez (fase de verificación)
- 3) Se aplica política del sitio (sistema de reputación)

Visión general

Esquema de funcionamiento de DKIM.



Que NO es DKIM por sí mismo ?



Una herramienta antiphishing

Una herramienta antispam

Una herramienta a nivel de cliente o un sustituto a S/MIME o PGP

SIN EMBARGO, puede ser útil para:

Sistemas de reputación, ergo:

Motores antispam

Motores antiphishing

Sistema de reputación básico



```
score DKIM_VERIFIED -0.3
score DKIM_SIGNED 0
score DKIM_POLICY_SIGNALL 0
score DKIM_POLICY_SIGNSOME 0
score DKIM_POLICY_TESTING 0
```

DKIM-based whitelisting of domains with # good reputation:

```
score USER_IN_DKIM_WHITELIST -8.0
whitelist_from_dkim *@intl.paypal.com paypal.com
whitelist_from_dkim *@*.paypal.com
whitelist_from_dkim *@paypal.com
whitelist_from_dkim *@*.paypal.be (...)
```

Sistema de reputación básico (II)



```
# DKIM-based whitelisting of domains with less than perfect
# reputation can be given fewer negative score points:
score USER_IN_DEF_DKIM_WL -1.5
score ENV_AND_HDR_DKIM_MATCH 0
def_whitelist_from_dkim *@google.com
def_whitelist_from_dkim *@gmail.com
def_whitelist_from_dkim *@googlemail.com (...)
```

Vamos a ello !



Mini-howto de configuración en 2 slides



- 1) `openssl genrsa -out rsa.private 1024`
`openssl rsa -in rsa.private -out rsa.public -pubout -outform PEM`
- 2) Pastear llave PEM en la zona DNS con el formato de la siguiente transpa
- 3) `apt-get install dkim-filter && vi /etc/dkim-filter.conf`

```
Domain      escert.upc.edu
KeyFile     /etc/ssl/private/dkim/private.key
Selector    2007
InternalHosts /etc/mail/dkim-milter.internalhosts
```

4) `/etc/postfix/main.cf`:

```
# DKIM
smtpd_milters = inet:localhost:8891
milter_macro_daemon_name = SIGNING
milter_default_action = tempfail
milter_protocol = 3
```

Entrada DKIM en RR TXT



```
2007._domainkey      IN TXT "dkim=all; t=y; k=rsa;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD  
Wnq+ESaf8dAWoXKN6V8XiiSfhgztMKzsTNJE4fvZSUJGu  
oN6vXzD8m04k4kgrJvJJ87PBTBKf7jtbQU1bi0+kVcD4Gy  
JK+HxrKUKWFY1z2JPTH8EbGW2nsBy1kNzjqfmO8czfKo  
cgiltnV4FO/fvIX6/eLaL5EAzmH90wdPzlrQIDAQAB"
```

Alternativa:

<http://www.sendmail.org/dkim/wizard>

Chequeo: Funciona todo ?



WEB: <http://www.sendmail.org/dkim/testChecker>
Mail (dkim-reflector): dkim-test@testing.dkim.org

☐ Subject: DKIM reflector results
From: mail@testing.dkim.org
Date: 10/23/2008 10:26 AM
To: Roman Valls

DKIM Message Reflector Results

Authentication Results

```
testing.dkim.org; v=0.1; dkim=pass, header.i=rvals@escert.upc.edu (
  sig from escert.upc.edu/2007 verified; );
dkim=pass, header.i=rvals@escert.upc.edu (
  sig from escert.upc.edu/2007 verified; );
ssp=pass, header.From=rvals@escert.upc.edu
```

DKIM Processing Output

Cabeceras DKIM a DKIM



esCERT to GMail

Authentication-Results: mx.google.com; spf=pass (google.com: domain of rvalls at escert upc edu designates 147.83.152.5 as permitted sender) smtp.mail=rvalls at escert upc edu; **dkim=pass (test mode)** header.i=@escert.upc.edu

GMail to esCERT

Authentication-Results: mail.escert.upc.edu; **dkim=pass (1024-bit key)**
header.i=@gmail.com

Oops, different "Authentication-Results" headers

Ok, pero va a matar mi servidor de correo ?



"No deberiamos estresar tanto un servicio crítico com es el correo electrónico"

"El tiempo que se tarda en firmar y verificar, podria acabar en un DoS en nuestros servidores. Una ráfaga certera de SPAM y estamos fritos"

**De verdad ?
Lo has medido ?**

Testbed para pruebas de rendimiento



Directamente en nuestro servidor en producción:
mail.escert.upc.edu

Máquina virtual XEN (sin **VT-x** !)
kernel = '/boot/vmlinuz-2.6.24-18-xen'
memory = '512'

Postfix+vmail+amavis+SA+clamav+dovecot+...

DKIM

RSA Private-Key: (1024 bit)
(rsa-sha256)

ZABBIX monitoring

smtp-source & smtp-sink



Dos utilidades (olvidadas?) muy útiles en la suite postfix:

Cliente:

```
smtp-source -s 20 -l 180000 -m 400 -c -f  
rvalls+stress@escert.upc.edu -t rvalls@escert.upc.edu  
mailserver:2525
```

-s 20: sesiones SMTP concurrentes
-l 180000: Tamaño del email en bytes
-m 400: Número de mails a enviar
-f & -t: from & to

Servidor:

```
smtp-sink localhost:2525
```

A estresar el servidor: mail corpus



DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=escert.upc.edu;
s=2007; t=1224777619; bh=ok//XpTG8XwmcouhDJpdS7OWGKsYIOoF4wbpt5WKmX
w=; h=From:To:Date:Message-Id; b=Z5zqxQ/uD9uvTBdyvoQ6PuXCt3zbuMCRlo
XiWS2gb5HKfbpqTPIhG41LPxpKLHrgdk6kmiYwO7I9sRwjTmNqLeRDfzLmRoTIAax9a
ZBGYtveonQ1EWf3rJiWh7e6eEEvLTpgA0t70Kf8FZyWs8+HbKmRlj1VnZ4fHLNh1ExJ
FcE=

From: rvalls+stress escert upc edu
To: rvalls escert upc edu
Date: Thu, 23 Oct 2008 18:00:19 +0200 (CEST)
Message-Id: <225a.0006.0000@mail.escert.upc.edu>

1XX
XX
2XX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX(...) hasta **180KB**

Primer intento: Kill 'em all



150 sesiones SMTP concurrentes
1000 emails **en 1 minuto**

inicio: Tue Oct 28 17:54:08 CET 2008
final: Tue Oct 28 17:55:03 CET 2008

... 18:03: R.I.P

root@escert-dom0:~# xm console mail

```
[106646.515512] Code: c1 f8 05 81 c2 80 d0 3f c0 2b 82 10 07 00 00 8b b2 68 06 00 00 c1 e8 0a 39 cb 8d  
04 40 7f 21 8d 14 18 b9 01 00 00 00 eb 02 01 c9 <0f> a3 16 19 c0 85 c0 74 02 09 cd 83 c3 01 83 c2 01 39  
df 7d e9
```

```
[106646.515592] EIP: [<c01613e6>] get_pageblock_flags_group+0x46/0x70 SS:ESP 0069:e0789dc4
```

```
[106646.515604] ---[ end trace 44a286cd78cf3dae ]---
```

root@escert-dom0:~# xm destroy mail

Round 2



150 sesiones SMTP concurrentes
400 mensajes **en 20 segundos**

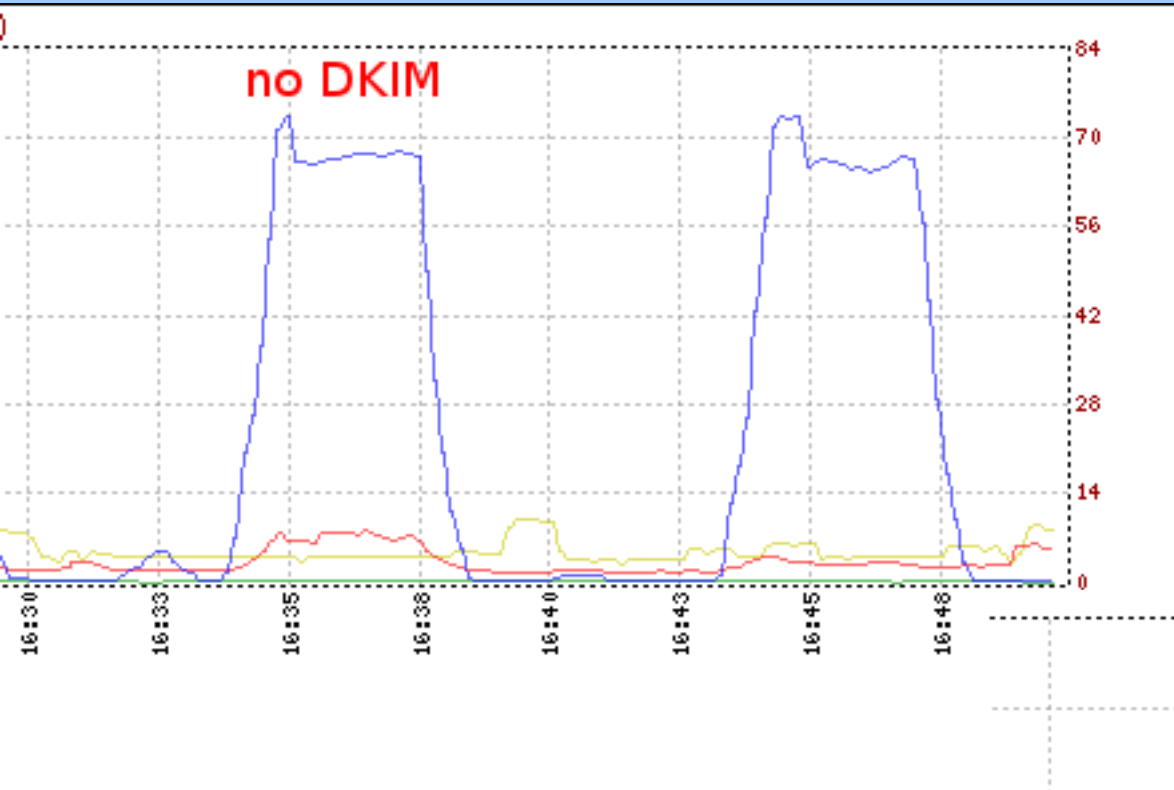
Wed Oct 29 16:34:21 CET 2008

Wed Oct 29 16:34:42 CET 2008

real 0m20.951s

... vivo !

Resultados: CPU/RAM sin DKIM

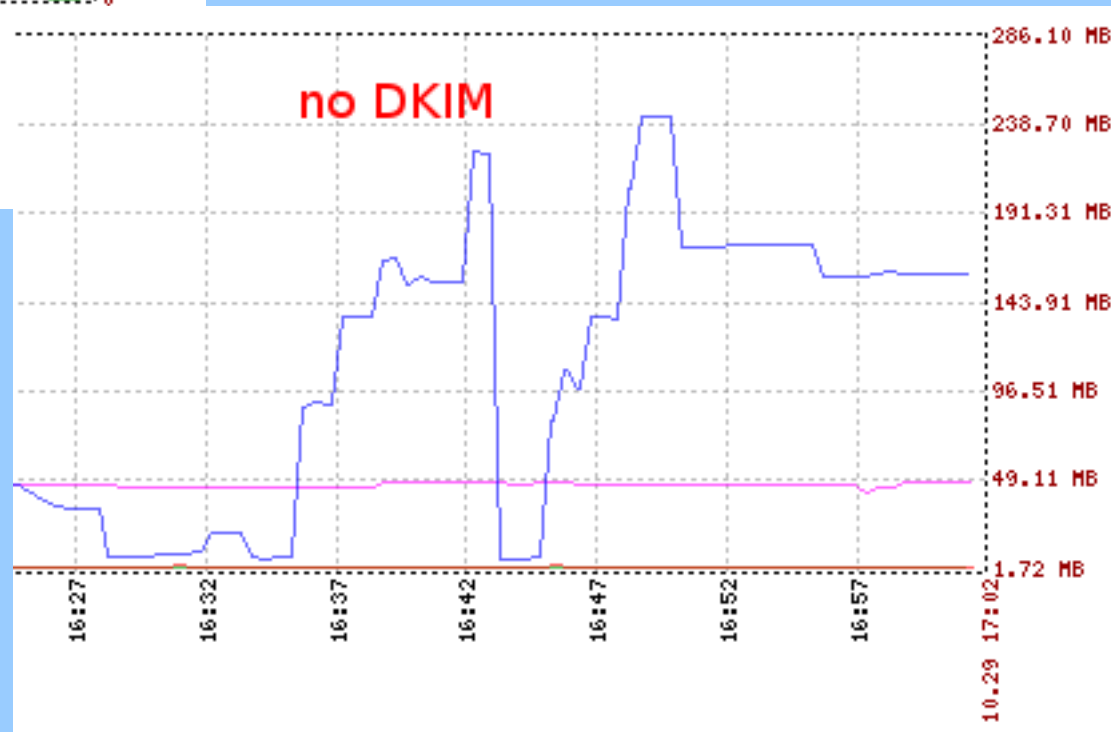


~76% CPU usage

~5 minutes to flush mail queue

~220MB RAM usage

~ 8 min to settle down

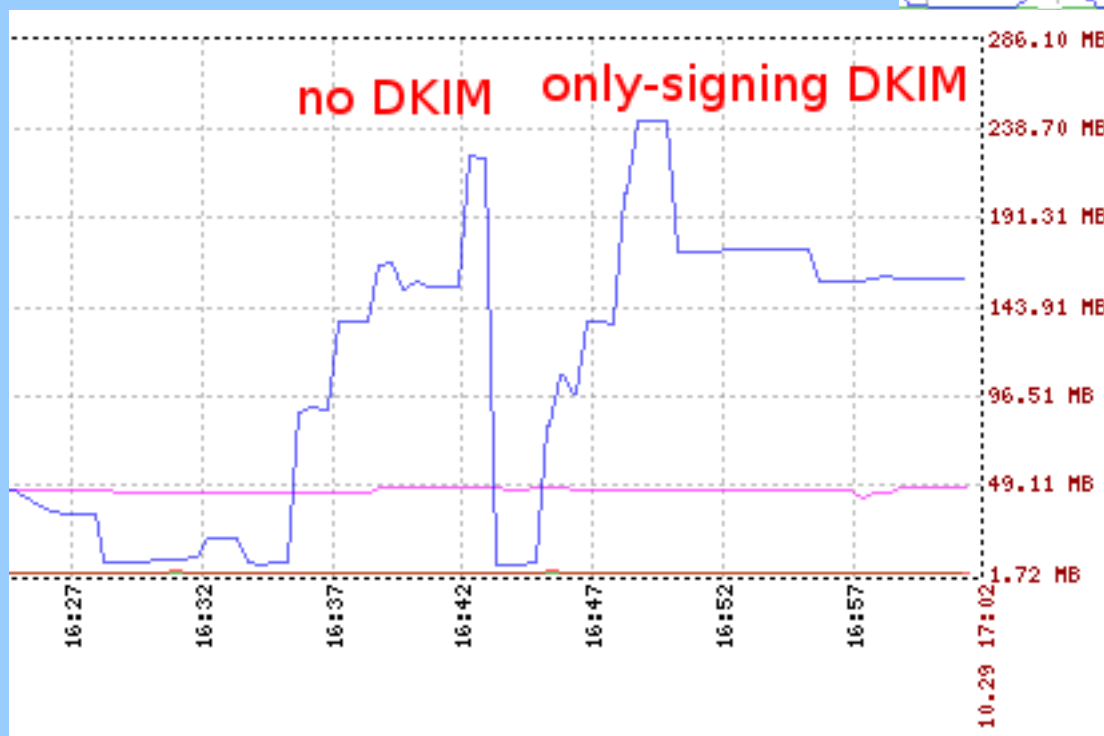
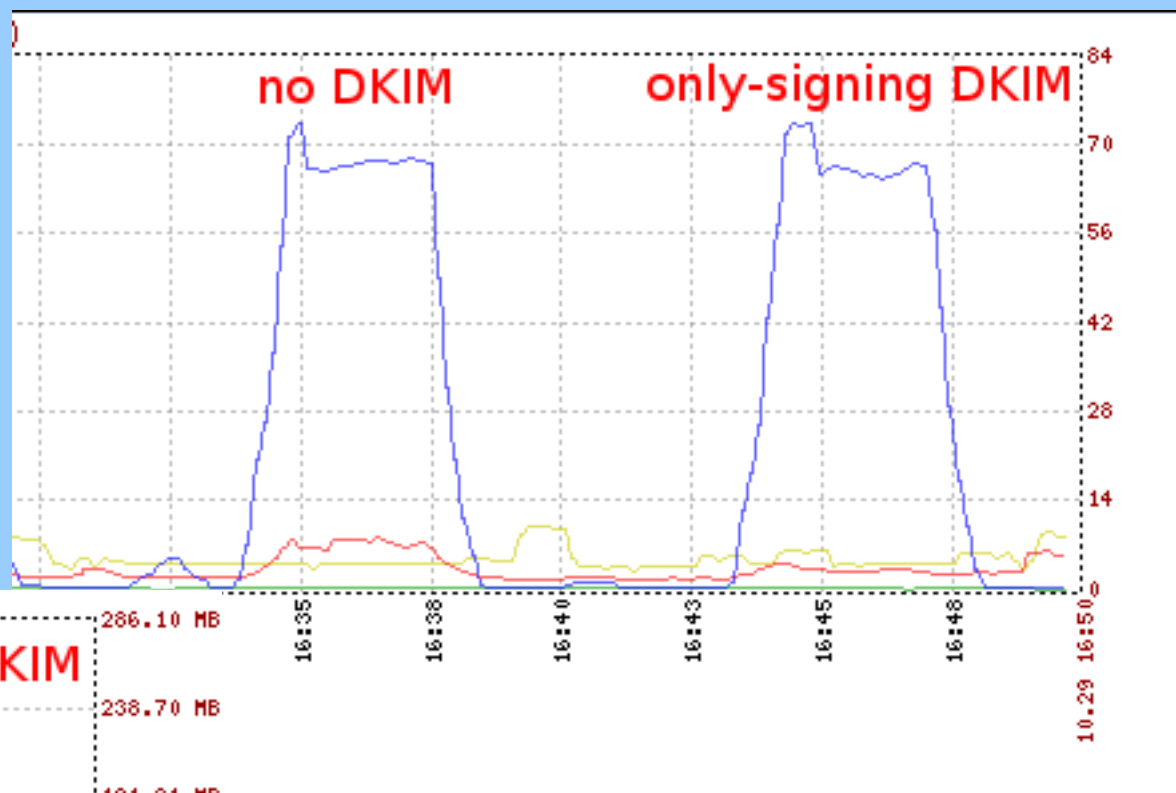


Resultados: CPU/RAM con DKIM

Sólo
firmar



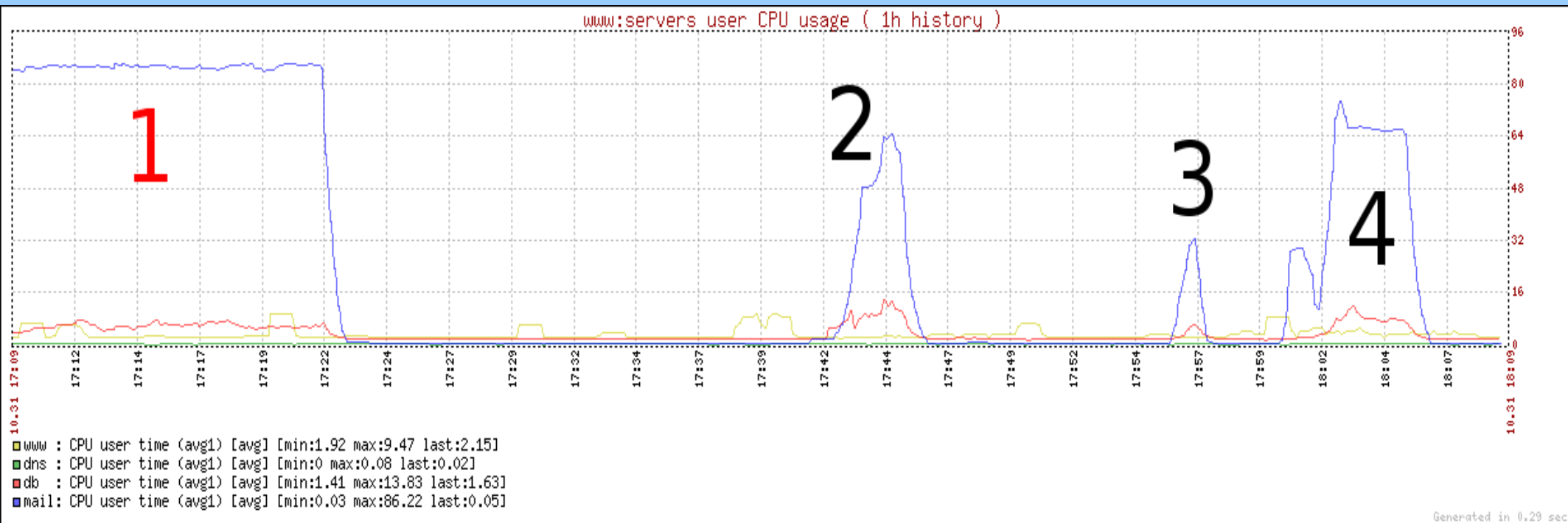
SAME !



nearly the SAME

Resultados: CPU con DKIM

firmar
&
verificar



- 1) Amavis+ClamAV+SA+DKIM(firmar+verificar), 5MB mails
- 2) DKIM(sign+verify) únicamente, 5MB mails
- 3) DKIM(sign+verify) únicamente, 180KB mails
- 4) Amavis+ClamAV+SA, 180KB mails

Conclusiones



Google: "DKIM CPU overhead"

"Compared to the CPU overhead of running SpamAssassin and ClamAV, DKIM is lost in the noise"

Concepción probada con datos reales en esta presentación

Quien usa esto ? Gmail, Yahoo, PayPal, Ebay... estado del despliegue ?:

<http://utility.nokia.net/~lars/meter/dkim.html>

DKIM resulta ser un sistema simple para añadir puntos en un sistema de reputación (no es una bala de plata, pero puede ser útil si se usa bien)

Referencias



Oficiales:

<http://www.dkim.org/>

<http://www.ietf.org/rfc/rfc4871.txt>

<http://www.ietf.org/rfc/rfc5016.txt>

Otras:

<http://hackandalus.nodo50.org/ftp/spf-dk-hackmeeting-2004.pdf>

<http://www.ijs.si/software/amavisd/amavisd-new-docs.html#dkim>

<http://utility.nokia.net/~lars/meter/dkim.html>