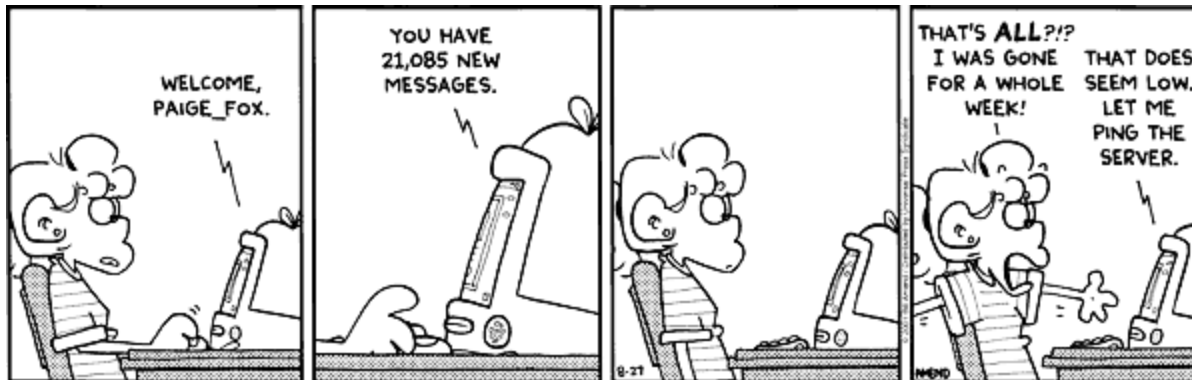


Eposta sistemleri

Linux Yaz Kampı 2011

Eray Aslan <eras@gentoo.org>



Eposta sistemleri

- Genel Kurallar
- Postfix
- Amavisd-new
- Dovecot
- Diğer konular
- Soru cevap



Genel Kurallar

- Gizlilik Hakkı



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik
- Basitlik



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik
- Basitlik
- Otomasyon



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik
- Basitlik
- Otomasyon
- İzleme



Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik
- Basitlik
- Otomasyon
- İzleme
- Güvenlik



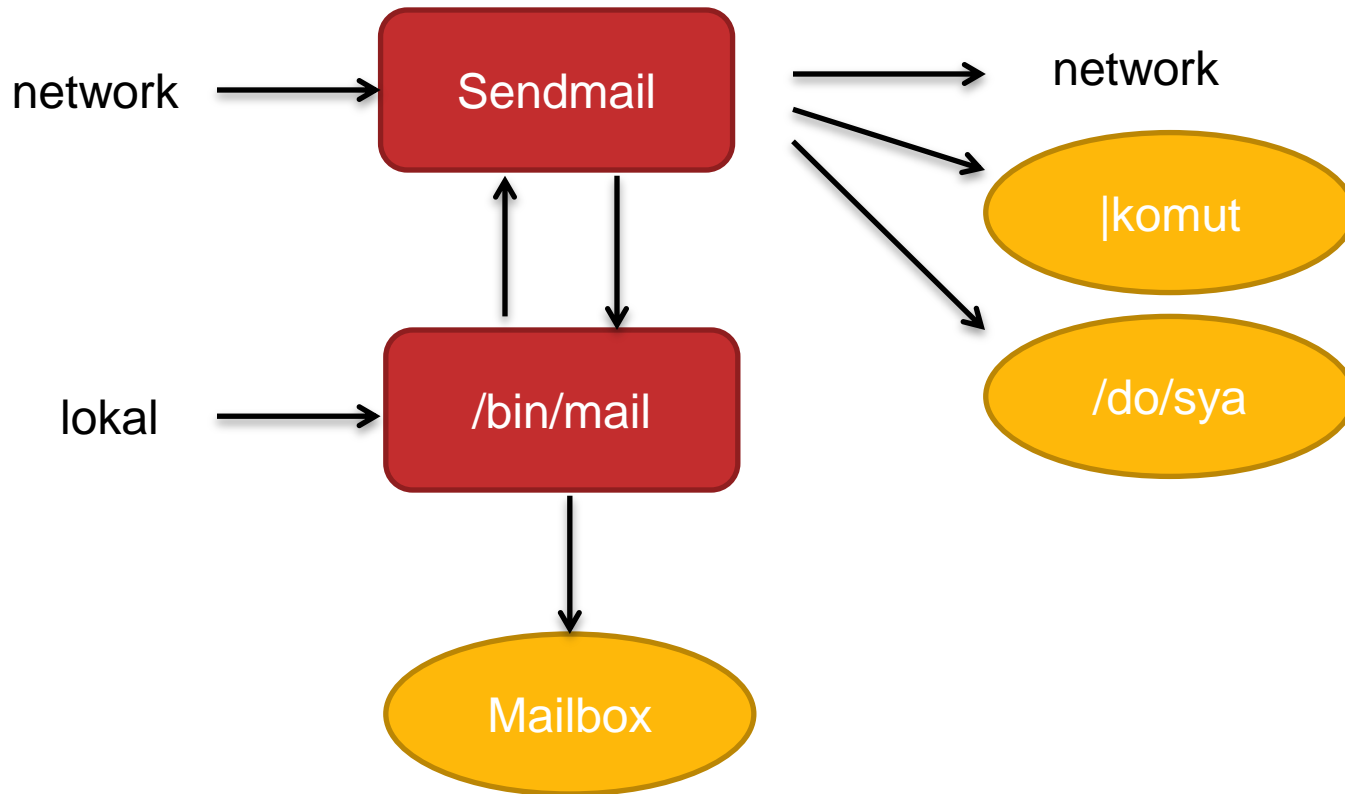
Genel Kurallar

- Gizlilik Hakkı
- Adlandırma
- Güvenilirlik
- Basitlik
- Otomasyon
- İzleme
- Güvenlik
- Şifreleme



Postfix

Geleneksel (BSD) UNIX mail yapısı

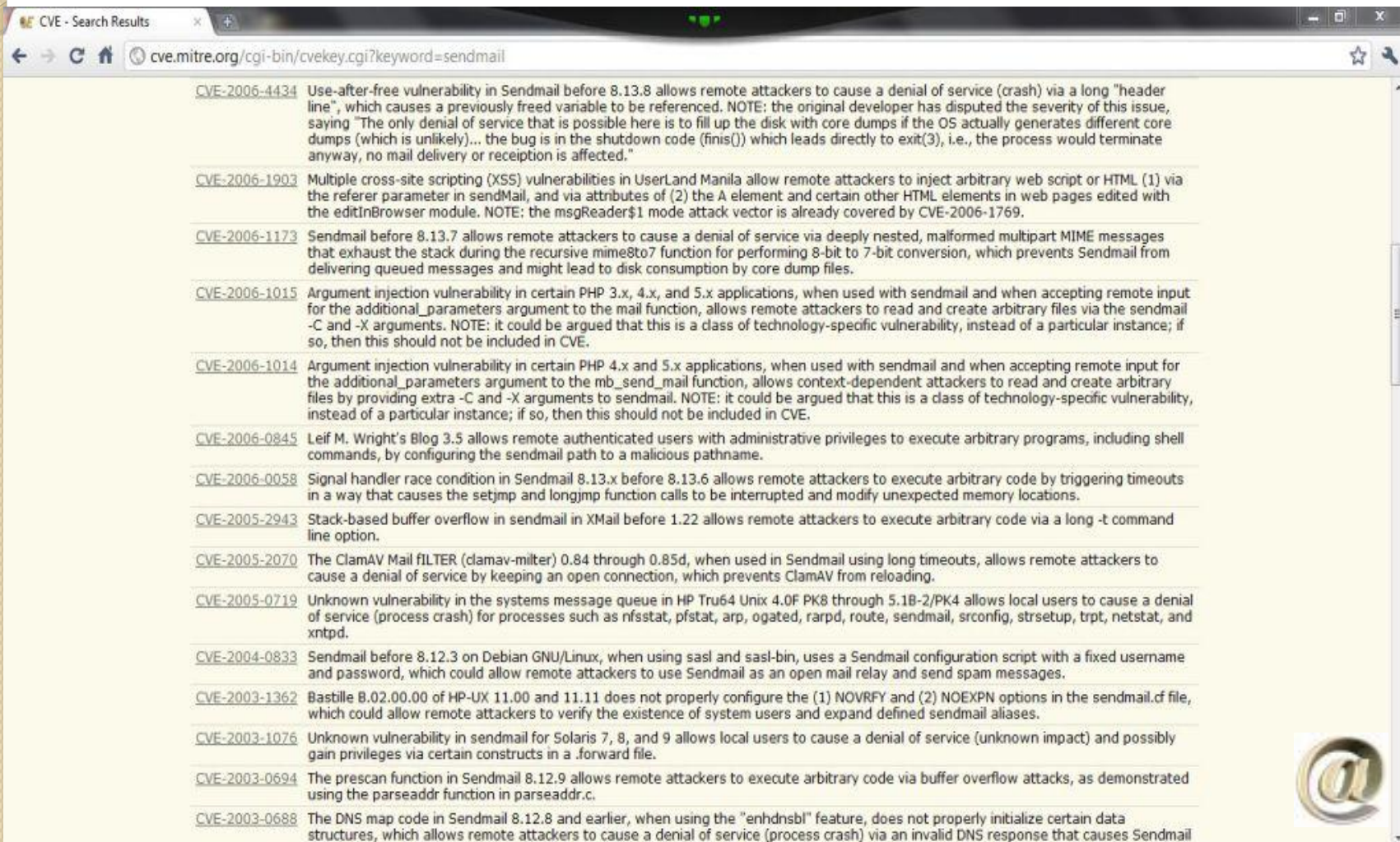


Sendmail CVE'ler: sayfa 1 / 4



Postfix

Sendmail CVE'ler: sayfa 2 / 4



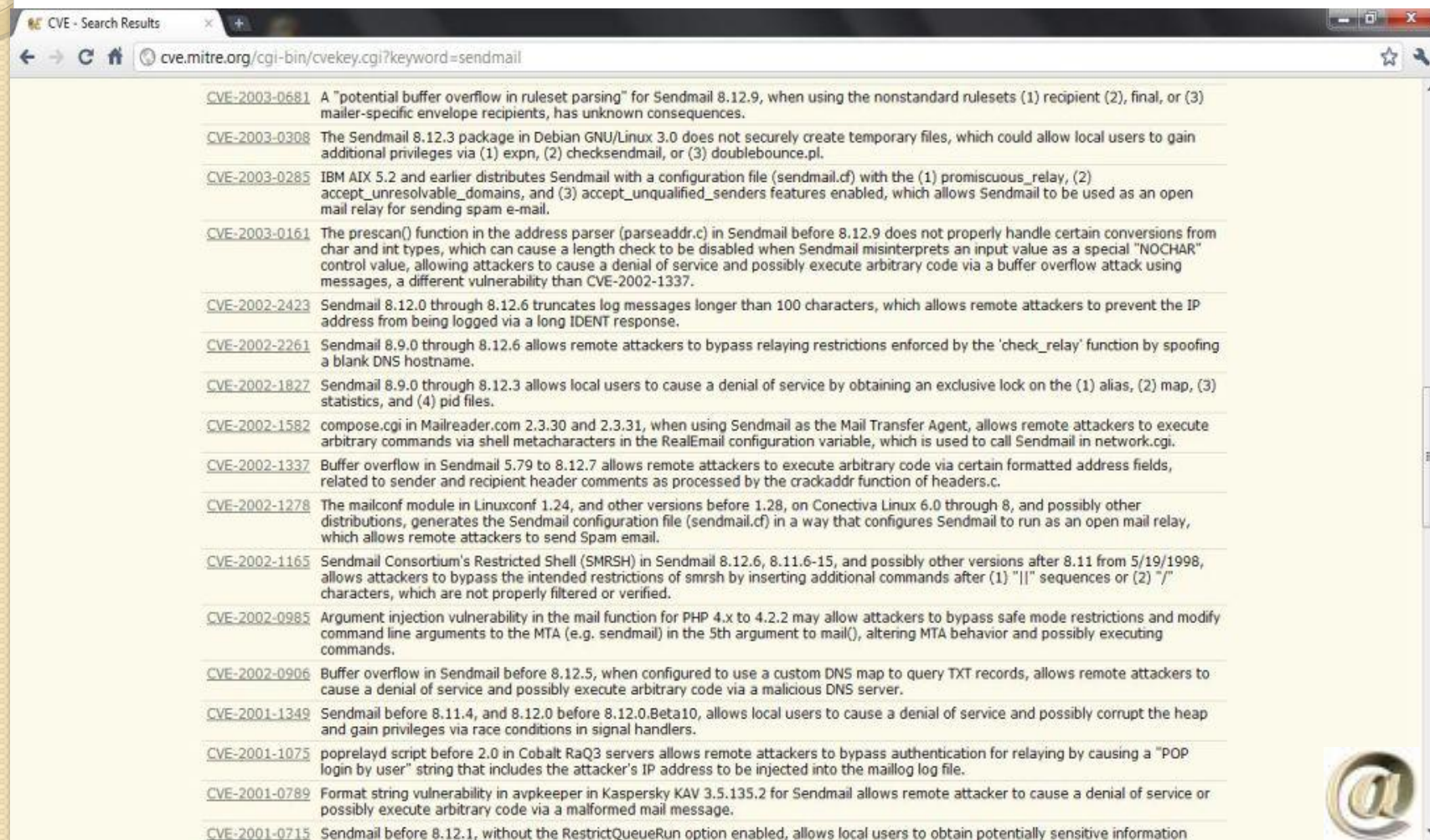
The screenshot shows a web browser window with the address bar displaying `cve.mitre.org/cgi-bin/cvekey.cgi?keyword=sendmail`. The page content lists various CVEs related to Sendmail, each with a link to the full entry and a brief description of the vulnerability.

CVE ID	Description
CVE-2006-4434	Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is unlikely)... the bug is in the shutdown code (finis()) which leads directly to exit(3), i.e., the process would terminate anyway, no mail delivery or reception is affected."
CVE-2006-1903	Multiple cross-site scripting (XSS) vulnerabilities in UserLand Manila allow remote attackers to inject arbitrary web script or HTML (1) via the referer parameter in sendMail, and via attributes of (2) the A element and certain other HTML elements in web pages edited with the editInBrowser module. NOTE: the msgReader\$1 mode attack vector is already covered by CVE-2006-1769.
CVE-2006-1173	Sendmail before 8.13.7 allows remote attackers to cause a denial of service via deeply nested, malformed multipart MIME messages that exhaust the stack during the recursive mime8to7 function for performing 8-bit to 7-bit conversion, which prevents Sendmail from delivering queued messages and might lead to disk consumption by core dump files.
CVE-2006-1015	Argument injection vulnerability in certain PHP 3.x, 4.x, and 5.x applications, when used with sendmail and when accepting remote input for the additional_parameters argument to the mail function, allows remote attackers to read and create arbitrary files via the sendmail -C and -X arguments. NOTE: it could be argued that this is a class of technology-specific vulnerability, instead of a particular instance; if so, then this should not be included in CVE.
CVE-2006-1014	Argument injection vulnerability in certain PHP 4.x and 5.x applications, when used with sendmail and when accepting remote input for the additional_parameters argument to the mb_send_mail function, allows context-dependent attackers to read and create arbitrary files by providing extra -C and -X arguments to sendmail. NOTE: it could be argued that this is a class of technology-specific vulnerability, instead of a particular instance; if so, then this should not be included in CVE.
CVE-2006-0845	Leif M. Wright's Blog 3.5 allows remote authenticated users with administrative privileges to execute arbitrary programs, including shell commands, by configuring the sendmail path to a malicious pathname.
CVE-2006-0058	Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.
CVE-2005-2943	Stack-based buffer overflow in sendmail in XMail before 1.22 allows remote attackers to execute arbitrary code via a long -t command line option.
CVE-2005-2070	The ClamAV Mail FILTER (clamav-milter) 0.84 through 0.85d, when used in Sendmail using long timeouts, allows remote attackers to cause a denial of service by keeping an open connection, which prevents ClamAV from reloading.
CVE-2005-0719	Unknown vulnerability in the systems message queue in HP Tru64 Unix 4.0F PK8 through 5.1B-2/PK4 allows local users to cause a denial of service (process crash) for processes such as nfsstat, pfstat, arp, ogated, rapd, route, sendmail, srconfig, strsetup, trpt, netstat, and xntpd.
CVE-2004-0833	Sendmail before 8.12.3 on Debian GNU/Linux, when using sasl and sasl-bin, uses a Sendmail configuration script with a fixed username and password, which could allow remote attackers to use Sendmail as an open mail relay and send spam messages.
CVE-2003-1362	Bastille 8.02.00.00 of HP-UX 11.00 and 11.11 does not properly configure the (1) NOVRFY and (2) NOEXPX options in the sendmail.cf file, which could allow remote attackers to verify the existence of system users and expand defined sendmail aliases.
CVE-2003-1076	Unknown vulnerability in sendmail for Solaris 7, 8, and 9 allows local users to cause a denial of service (unknown impact) and possibly gain privileges via certain constructs in a .forward file.
CVE-2003-0694	The prescan function in Sendmail 8.12.9 allows remote attackers to execute arbitrary code via buffer overflow attacks, as demonstrated using the parseaddr function in parseaddr.c.
CVE-2003-0688	The DNS map code in Sendmail 8.12.8 and earlier, when using the "enhdnsbl" feature, does not properly initialize certain data structures, which allows remote attackers to cause a denial of service (process crash) via an invalid DNS response that causes Sendmail



Postfix

Sendmail CVE'ler: sayfa 3 / 4



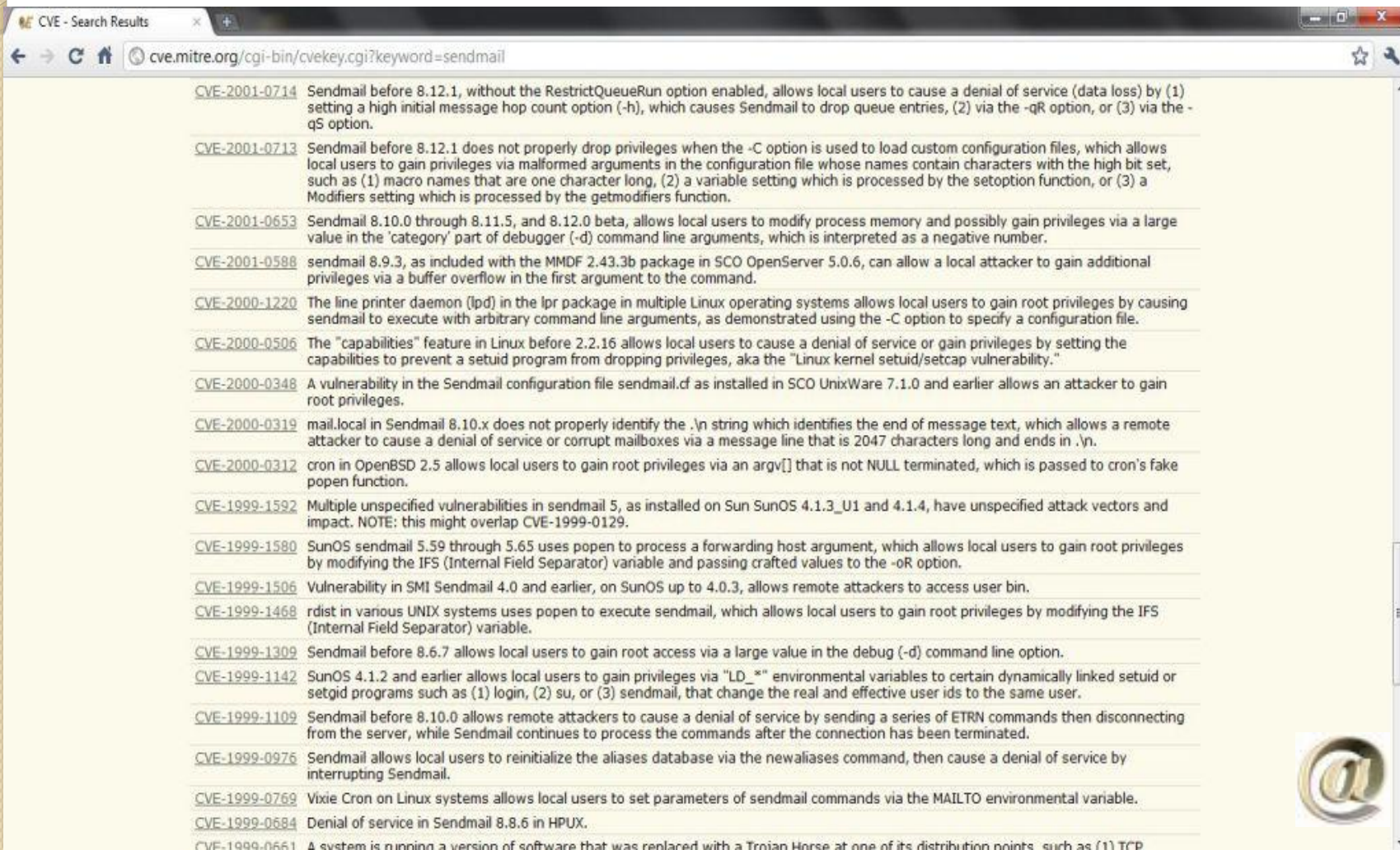
The screenshot shows a web browser window with the address bar displaying `cve.mitre.org/cgi-bin/cvekey.cgi?keyword=sendmail`. The page title is "CVE - Search Results". The main content area lists 20 CVE entries, each with a link to the full entry and a brief description of the vulnerability. The vulnerabilities are sorted by date, with the most recent at the top. The list includes CVE-2003-0681, CVE-2003-0308, CVE-2003-0285, CVE-2003-0161, CVE-2002-2423, CVE-2002-2261, CVE-2002-1827, CVE-2002-1582, CVE-2002-1337, CVE-2002-1278, CVE-2002-1165, CVE-2002-0985, CVE-2002-0906, CVE-2001-1349, CVE-2001-1075, CVE-2001-0789, and CVE-2001-0715. The descriptions detail various issues such as buffer overflows, privilege escalation, and denial of service.

CVE ID	Description
CVE-2003-0681	A "potential buffer overflow in ruleset parsing" for Sendmail 8.12.9, when using the nonstandard rulesets (1) recipient (2), final, or (3) mailer-specific envelope recipients, has unknown consequences.
CVE-2003-0308	The Sendmail 8.12.3 package in Debian GNU/Linux 3.0 does not securely create temporary files, which could allow local users to gain additional privileges via (1) expn, (2) checksendmail, or (3) doublebounce.pl.
CVE-2003-0285	IBM AIX 5.2 and earlier distributes Sendmail with a configuration file (sendmail.cf) with the (1) promiscuous_relay, (2) accept_unresolvable_domains, and (3) accept_unqualified_senders features enabled, which allows Sendmail to be used as an open mail relay for sending spam e-mail.
CVE-2003-0161	The prescan() function in the address parser (parseaddr.c) in Sendmail before 8.12.9 does not properly handle certain conversions from char and int types, which can cause a length check to be disabled when Sendmail misinterprets an input value as a special "NOCHAR" control value, allowing attackers to cause a denial of service and possibly execute arbitrary code via a buffer overflow attack using messages, a different vulnerability than CVE-2002-1337.
CVE-2002-2423	Sendmail 8.12.0 through 8.12.6 truncates log messages longer than 100 characters, which allows remote attackers to prevent the IP address from being logged via a long IDENT response.
CVE-2002-2261	Sendmail 8.9.0 through 8.12.6 allows remote attackers to bypass relaying restrictions enforced by the 'check_relay' function by spoofing a blank DNS hostname.
CVE-2002-1827	Sendmail 8.9.0 through 8.12.3 allows local users to cause a denial of service by obtaining an exclusive lock on the (1) alias, (2) map, (3) statistics, and (4) pid files.
CVE-2002-1582	compose.cgi in Mailreader.com 2.3.30 and 2.3.31, when using Sendmail as the Mail Transfer Agent, allows remote attackers to execute arbitrary commands via shell metacharacters in the RealEmail configuration variable, which is used to call Sendmail in network.cgi.
CVE-2002-1337	Buffer overflow in Sendmail 5.79 to 8.12.7 allows remote attackers to execute arbitrary code via certain formatted address fields, related to sender and recipient header comments as processed by the crackaddr function of headers.c.
CVE-2002-1278	The mailconf module in Linuxconf 1.24, and other versions before 1.28, on Conectiva Linux 6.0 through 8, and possibly other distributions, generates the Sendmail configuration file (sendmail.cf) in a way that configures Sendmail to run as an open mail relay, which allows remote attackers to send Spam email.
CVE-2002-1165	Sendmail Consortium's Restricted Shell (SMRSH) in Sendmail 8.12.6, 8.11.6-15, and possibly other versions after 8.11 from 5/19/1998, allows attackers to bypass the intended restrictions of smrsh by inserting additional commands after (1) " " sequences or (2) "/" characters, which are not properly filtered or verified.
CVE-2002-0985	Argument injection vulnerability in the mail function for PHP 4.x to 4.2.2 may allow attackers to bypass safe mode restrictions and modify command line arguments to the MTA (e.g. sendmail) in the 5th argument to mail(), altering MTA behavior and possibly executing commands.
CVE-2002-0906	Buffer overflow in Sendmail before 8.12.5, when configured to use a custom DNS map to query TXT records, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a malicious DNS server.
CVE-2001-1349	Sendmail before 8.11.4, and 8.12.0 before 8.12.0.Beta10, allows local users to cause a denial of service and possibly corrupt the heap and gain privileges via race conditions in signal handlers.
CVE-2001-1075	poprelayd script before 2.0 in Cobalt RaQ3 servers allows remote attackers to bypass authentication for relaying by causing a "POP login by user" string that includes the attacker's IP address to be injected into the maillog log file.
CVE-2001-0789	Format string vulnerability in avpkeeper in Kaspersky KAV 3.5.135.2 for Sendmail allows remote attacker to cause a denial of service or possibly execute arbitrary code via a malformed mail message.
CVE-2001-0715	Sendmail before 8.12.1, without the RestrictQueueRun option enabled, allows local users to obtain potentially sensitive information



Postfix


Sendmail CVE'ler: sayfa 4 / 4



CVE - Search Results

cve.mitre.org/cgi-bin/cvekey.cgi?keyword=sendmail

- [CVE-2001-0714](#) Sendmail before 8.12.1, without the RestrictQueueRun option enabled, allows local users to cause a denial of service (data loss) by (1) setting a high initial message hop count option (-h), which causes Sendmail to drop queue entries, (2) via the -qR option, or (3) via the -qS option.
- [CVE-2001-0713](#) Sendmail before 8.12.1 does not properly drop privileges when the -C option is used to load custom configuration files, which allows local users to gain privileges via malformed arguments in the configuration file whose names contain characters with the high bit set, such as (1) macro names that are one character long, (2) a variable setting which is processed by the setoption function, or (3) a Modifiers setting which is processed by the getmodifiers function.
- [CVE-2001-0653](#) Sendmail 8.10.0 through 8.11.5, and 8.12.0 beta, allows local users to modify process memory and possibly gain privileges via a large value in the 'category' part of debugger (-d) command line arguments, which is interpreted as a negative number.
- [CVE-2001-0588](#) sendmail 8.9.3, as included with the MMDF 2.43.3b package in SCO OpenServer 5.0.6, can allow a local attacker to gain additional privileges via a buffer overflow in the first argument to the command.
- [CVE-2000-1220](#) The line printer daemon (lpd) in the lpr package in multiple Linux operating systems allows local users to gain root privileges by causing sendmail to execute with arbitrary command line arguments, as demonstrated using the -C option to specify a configuration file.
- [CVE-2000-0506](#) The "capabilities" feature in Linux before 2.2.16 allows local users to cause a denial of service or gain privileges by setting the capabilities to prevent a setuid program from dropping privileges, aka the "Linux kernel setuid/setcap vulnerability."
- [CVE-2000-0348](#) A vulnerability in the Sendmail configuration file sendmail.cf as installed in SCO UnixWare 7.1.0 and earlier allows an attacker to gain root privileges.
- [CVE-2000-0319](#) mail.local in Sendmail 8.10.x does not properly identify the .\n string which identifies the end of message text, which allows a remote attacker to cause a denial of service or corrupt mailboxes via a message line that is 2047 characters long and ends in .\n.
- [CVE-2000-0312](#) cron in OpenBSD 2.5 allows local users to gain root privileges via an argv[] that is not NULL terminated, which is passed to cron's fake popen function.
- [CVE-1999-1592](#) Multiple unspecified vulnerabilities in sendmail 5, as installed on Sun SunOS 4.1.3_U1 and 4.1.4, have unspecified attack vectors and impact. NOTE: this might overlap CVE-1999-0129.
- [CVE-1999-1580](#) SunOS sendmail 5.59 through 5.65 uses popen to process a forwarding host argument, which allows local users to gain root privileges by modifying the IFS (Internal Field Separator) variable and passing crafted values to the -oR option.
- [CVE-1999-1506](#) Vulnerability in SMI Sendmail 4.0 and earlier, on SunOS up to 4.0.3, allows remote attackers to access user bin.
- [CVE-1999-1468](#) rdist in various UNIX systems uses popen to execute sendmail, which allows local users to gain root privileges by modifying the IFS (Internal Field Separator) variable.
- [CVE-1999-1309](#) Sendmail before 8.6.7 allows local users to gain root access via a large value in the debug (-d) command line option.
- [CVE-1999-1142](#) SunOS 4.1.2 and earlier allows local users to gain privileges via "LD_*" environmental variables to certain dynamically linked setuid or setgid programs such as (1) login, (2) su, or (3) sendmail, that change the real and effective user ids to the same user.
- [CVE-1999-1109](#) Sendmail before 8.10.0 allows remote attackers to cause a denial of service by sending a series of ETRN commands then disconnecting from the server, while Sendmail continues to process the commands after the connection has been terminated.
- [CVE-1999-0976](#) Sendmail allows local users to reinitialize the aliases database via the newaliases command, then cause a denial of service by interrupting Sendmail.
- [CVE-1999-0769](#) Vixie Cron on Linux systems allows local users to set parameters of sendmail commands via the MAILTO environmental variable.
- [CVE-1999-0684](#) Denial of service in Sendmail 8.8.6 in HP-UX.
- [CVE-1999-0661](#) A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP



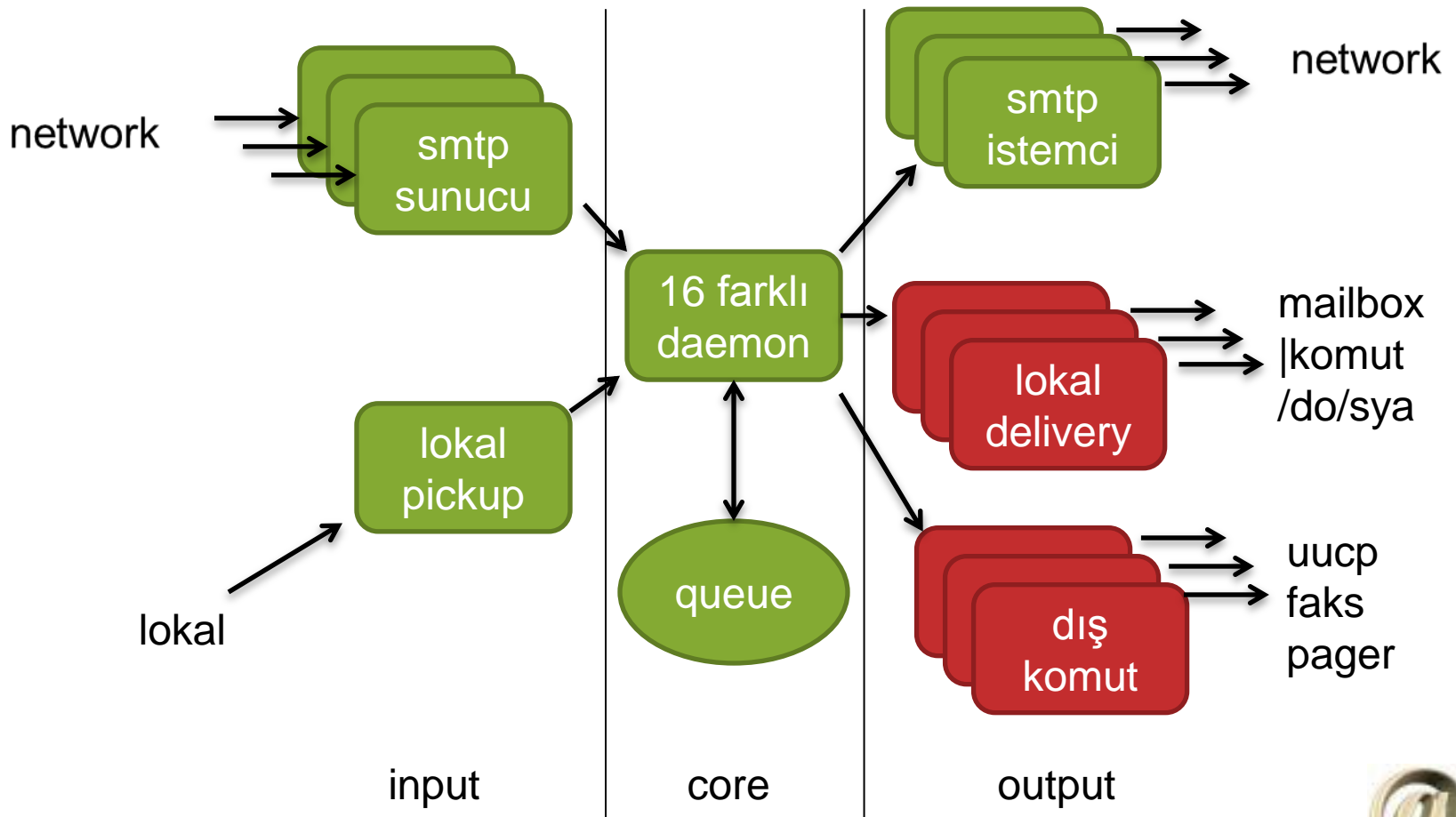
Postfix

- Sendmail: Monolithic ve root
 - Bir hata yeterli:
 - İstemci root hakkı elde eder
 - İç güvenlik duvarı yok:
 - İçeri sızmak kolay



Postfix

Postfix genel yapı



Postfix

- Ön şartlar:

- Doğru hostname

- `$ hostname --fqdn`
 - `green.caf.com.tr`

- Bağlantı

- `$ telnet mail.gentoo.org 25`
 - `Trying 140.211.166.183...`
 - `Connected to mail.gentoo.org.`
 - `Escape character is '^]'.`
 - `220 smtp.gentoo.org Gentoo ESMTP Mail Server`
 - `quit`
 - `221 2.0.0 Bye`
 - `Connection closed by foreign host.`



Postfix

- Ön şartlar: (devam)

- Doğru zaman

- `$ date`
 - `Sat Jan 22 16:05:15 UTC 2011`
 - `$ ntpq -pn`
 - | remote | refid | st | t | when | poll | reach | delay | offset | jitter |
|------------|----------------|----|---|------|------|-------|-------|--------|--------|
| ===== | | | | | | | | | |
| *10.0.2.23 | 131.211.84.189 | 2 | u | 602 | 1024 | 377 | 0.173 | 1.531 | 0.062 |
| +10.0.2.25 | 89.188.26.129 | 3 | u | 724 | 1024 | 377 | 4.566 | -1.966 | 1.485 |

- Syslog

- `# ps auxwww| grep [s]yslog`
 - `root 1563 0.0 0.2 28492 1408 ? S1 01:53 0:03 /usr/sbin/rsyslogd -c4`
 - **Syslogd kullanıyorsanız:**
 - `mail.* -/var/log/maillog`



Postfix

- Ön şartlar: (devam)

- DNS - istemci

- `$ dig gentoo.org MX`
 - `; <<>> DiG 9.7.2-P2 <<>> gentoo.org MX`
 - `;; global options: +cmd`
 - `;; Got answer:`
 - `;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21501`
 - `;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1`
 - `;; QUESTION SECTION:`
 - `;gentoo.org. IN MX`
 - `;; ANSWER SECTION:`
 - `gentoo.org. 15391 IN MX 10 mail.gentoo.org.`
 - `;; AUTHORITY SECTION:`
 - `gentoo.org. 58590 IN NS ns1.gentoo.org.`
 - `gentoo.org. 58590 IN NS ns2.gentoo.org.`
 - `;; ADDITIONAL SECTION:`
 - `mail.gentoo.org. 15392 IN A 140.211.166.183`
 - `;; Query time: 1 msec`
 - `;; SERVER: 10.0.2.23#53(10.0.2.23)`
 - `;; WHEN: Sat Jan 22 16:19:09 2011`
 - `;; MSG SIZE rcvd: 101`



Postfix

- Ön şartlar: (devam)
 - DNS – sunucu
 - A record
 - `$ dig +short mail.gentoo.org A`
 - 140.211.166.183
 - PTR record
 - `$ dig +short -x 140.211.166.183`
 - smtp.gentoo.org.
 - MX record
 - `$ dig +short gentoo.org MX`
 - 10 mail.gentoo.org.



Postfix

Email

header

body

attachment header

attachment body

Postfix

Return-Path: <lkd-duyuru-bounces@liste.linux.org.tr>

Delivered-To: eray.aslan@zeplin.net

Received: from localhost (sunny.caf.com.tr [127.0.0.1])

by mail.caf.com.tr (Postfix) with ESMTP id 76F9839E374

for <eray.aslan@caf.com.tr>; Fri, 21 Jan 2011 16:32:01 +0000 (UTC)

X-Quarantine-ID: <TnPr3OSlwJrX>

X-Spam-Flag: NO

X-Spam-Score: 1.604

X-Spam-Status: No, score=1.604 required=6.2 tests=[BAYES_80=2,

CRM114_CHECK=-0.286, L_POF_Linux=-0.1, T_RP_MATCHES_RCVD=-0.01]

autolearn=disabled

X-CRM114-Status: UNSURE (7.15)

X-Amavis-OS-Fingerprint: Linux 2.6 (newer, 3) (NAT!) (up: 3199 hrs), (distance

9, link: pppoe (DSL)), [139.179.139.185:56009]

Received: from mail.caf.com.tr ([127.0.0.1])

by localhost (sunny.caf.com.tr [127.0.0.1]) (amavisd-new, port 10024)

with ESMTP id TnPr3OSlwJrX for <eray.aslan@caf.com.tr>;

Fri, 21 Jan 2011 16:31:59 +0000 (UTC)

Date: Fri, 21 Jan 2011 18:26:42 +0200

From: Recep =?UTF-8?B?S8Sxcm3EsXrEsQ==?= <recep.kirmizi@linux.org.tr>

To: lkd-duyuru@liste.linux.org.tr

Message-Id: <20110121182642.0b96a426.recep.kirmizi@linux.org.tr>

...

Akademik Bili=FEim Konferans=FD 2011'de Linux Seminerleri ve Kurslar=FD

Konferans =D6ncesinde Kurslar

Postfix

Received: from postaci.linux.org.tr (postaci.linux.org.tr
[139.179.139.185]) by mail.caf.com.tr (Postfix) with ESMTP
id 3F6EC39E366 for eray.aslan@caf.com.tr
; Fri, 21 Jan 2011 16:31:59 +0000 (UTC)

Received:

[from <heloname>]

[by <host>]

[with <protocol>]

[id <value>]

[for <forward-path>]

; date

[...] optional

Postfix

- Ayarlar: Email firewall
- http://www.postfix.org/MULTI_INSTANCE_README.html
 - Multi-instance postfix
 - Queue, data, configuration dosyalari farkli
 - Program ve dokumantasyon dosyalari ayni
 - null client
 - postfix-in
 - postfix-out
 - [msa-in]
 - [msa-out]
 - [test]



Postfix

- Loglar (Birinci bölüm):
 - Jul 15 09:02:12 debian postfix/pickup[17341]: DE0357807: uid=0 from=<root>
 - Jul 15 09:02:12 debian postfix/cleanup[17631]: DE0357807: message-id=<20110715130212.DE0357807@london0.caf.com.tr>
 - Jul 15 09:02:12 debian postfix/qmgr[17343]: DE0357807: from=<root@caf.com.tr>, size=289, nrcpt=1 (queue active)
 - Jul 15 09:02:13 debian postfix/smtp[17634]: DE0357807: to=<eray.aslan@caf.com.tr>, orig_to=<root>, relay=mail.caf.com.tr[88.250.130.162]:25, delay=0.83, delays=0.02/0.01/0.37/0.44, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 8CEEE60084)
 - Jul 15 09:02:13 debian postfix/qmgr[17343]: DE0357807: removed



Amavisd-new

- MTA ile anti-virus / anti-spam arası iletişim
- Yasaklı içerik kontrolü
- Karantina / Arşiv
- DKIM: imza ve imza kontrolü
- İzleme: SNMP, SQL log, nanny



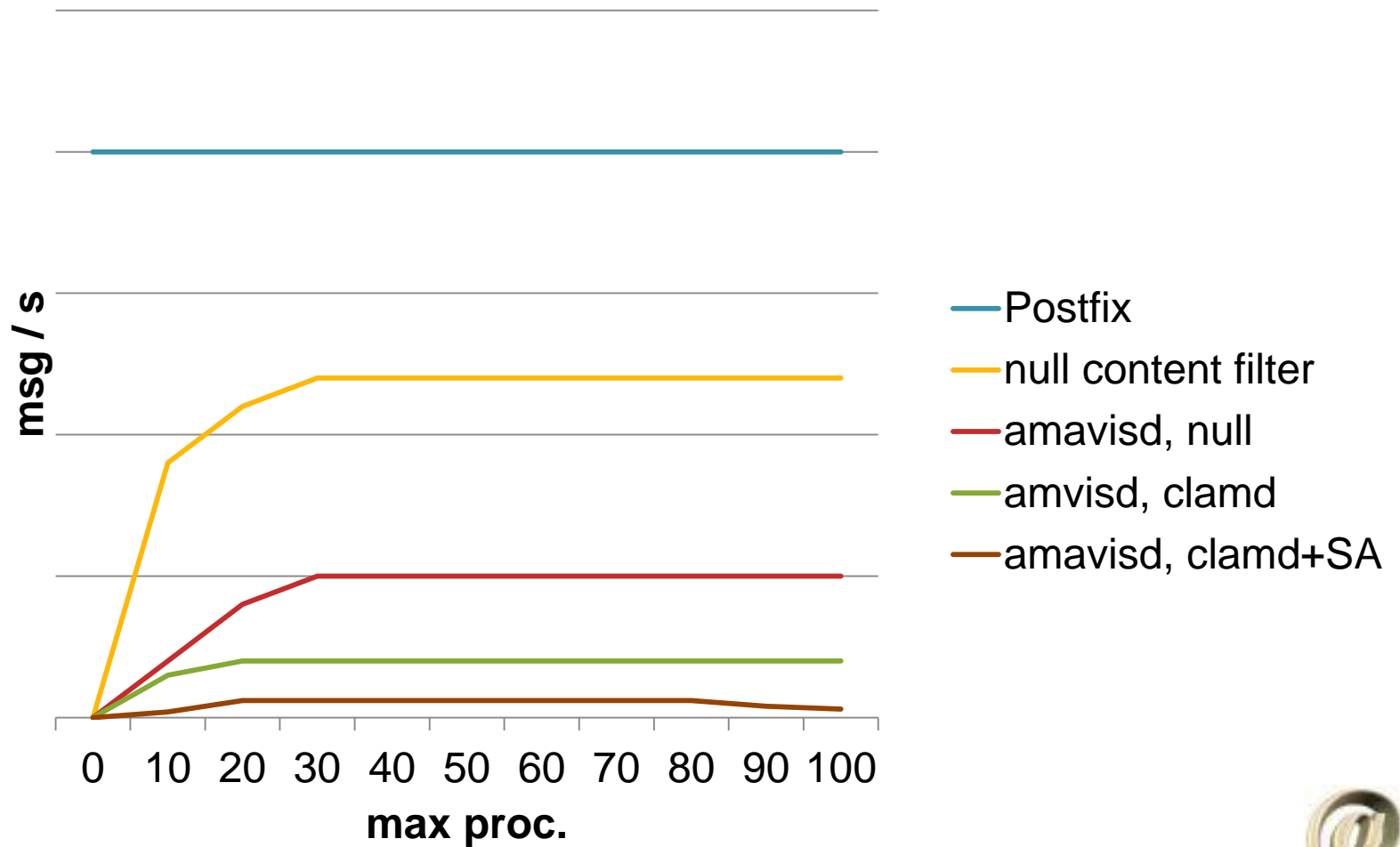
Amavisd-new

Niye popüler?

- Güvenli:
 - Her işlemi kontrol eder
 - Hata olursa, email MTA'da kalır
- Standartlara uygun (SMTP, MIME, DSN ...)
- Nispeten hızlı ve “feature-rich”
- Güvenli: perl, taint kontrolü, chroot mümkün
- Olgun: 7+ yıl düzenli geliştirme
- OSS: GPL lisansı (+ BSD lisanslı araçlar)



Amavisd-new



Amavisd-new

Performans ayarları

- Max. proc seçimi
 - Komut satırından virüs tarama yapma
 - MTA ve amavisd tmp için farklı diskler
 - Linux syslogd: async mail log
 - Bazı kurallar vakit alıyor. Test.
-
- Ayrı MTA ve amavisd sunucuları
 - Birkaç MX sunucu



Amavisd-new

Ayarlar:

- Bütün ayarlar amavisd.conf-default dosyasında
- Klasörler, hostname ...
- User (uid)
- Gönderen, alan
- \$max_servers
- \$nanny_details_level=2;



Amavisd-new

Ayarlar – kaynak:

- @mynetworks, \$originating

Etkileri:

- DKIM imzalama
- Disclaimer ekleme
- Bounce killer
- Pen pals
- MYUSER policy bank



Amavisd-new

Ayarlar – input:

- SMTP veya LMTP veya AM.PDP veya AM.CL
- # TCP portlar
 - \$inet_socket_port = [10024, 10026, 10027];
- # erişim kısıtlaması
 - @inet_acl = qw(127.0.0.0/8 [::1] 192.168.1.1);
- # sadece loopback
 - \$inet_socket_bind = '127.0.0.1';
- # karantina veya milter için
 - \$unix_socketname = '/var/amavis/amavis.sock';



Amavisd-new

Ayarlar – output:

- SMTP veya LMTP veya pipe
 - `$forward_method = 'smtp:[127.0.0.1]:10025';`
 - `$notify_method = 'smtp:[127.0.0.1]:10025';`
 - `$forward_method = 'smtp:*:*';`
 - `$notify_method = 'smtp*:10587';`
 - ilk yildiz : SMTP istemci adresi
 - ikinci yildiz : SMTP/LMTP gelen port+1
 - `$virus_quarantine_method,`
`$spam_quarantine_method ...`



Amavisd-new

Policy banks

- Programı etkileyen bütün değişkenler
- Birkaç tane kullanıma hazır kolayca yüklenebilen alternatif değişkenler
- Bütün mesajı etkiler (alıcı bazında değil)



Amavisd-new

- Policy banks

kırmızı

```
$a = "kırmızı";  
$b = "4",  
$c = "ABC";
```

yeşil

```
$a = "yeşil";
```

mavi

```
$a = "mavi";  
$b = 99;  
@d = (88);
```

geçerli

```
$a = "siyah";  
$b = 2;  
$c = undef;  
@d = (1,2,3);
```



Amavisd-new

- Policy banks

kırmızı

```
$a = "kırmızı";  
$b = "4",  
$c = "ABC";
```

yeşil

```
$a = "yeşil";
```

mavi

```
$a = "mavi";  
$b = 99;  
@d = (88);
```

geçerli

```
$a = "mavi";  
$b = 99;  
$c = undef;  
@d = (88);
```



Amavisd-new

- Policy banks

kırmızı

```
$a = "kırmızı";  
$b = "4",  
$c = "ABC";
```

yeşil

```
$a = "yeşil";
```

mavi

```
$a = "mavi";  
$b = 99;  
@d = (88);
```

geçerli

```
$a = "yeşil";  
$b = 99;  
$c = undef;  
@d = (88);
```



Amavisd-new

- Policy banks

kırmızı

```
$a = "kırmızı";  
$b = "4",  
$c = "ABC";
```

yeşil

```
$a = "yeşil";
```

mavi

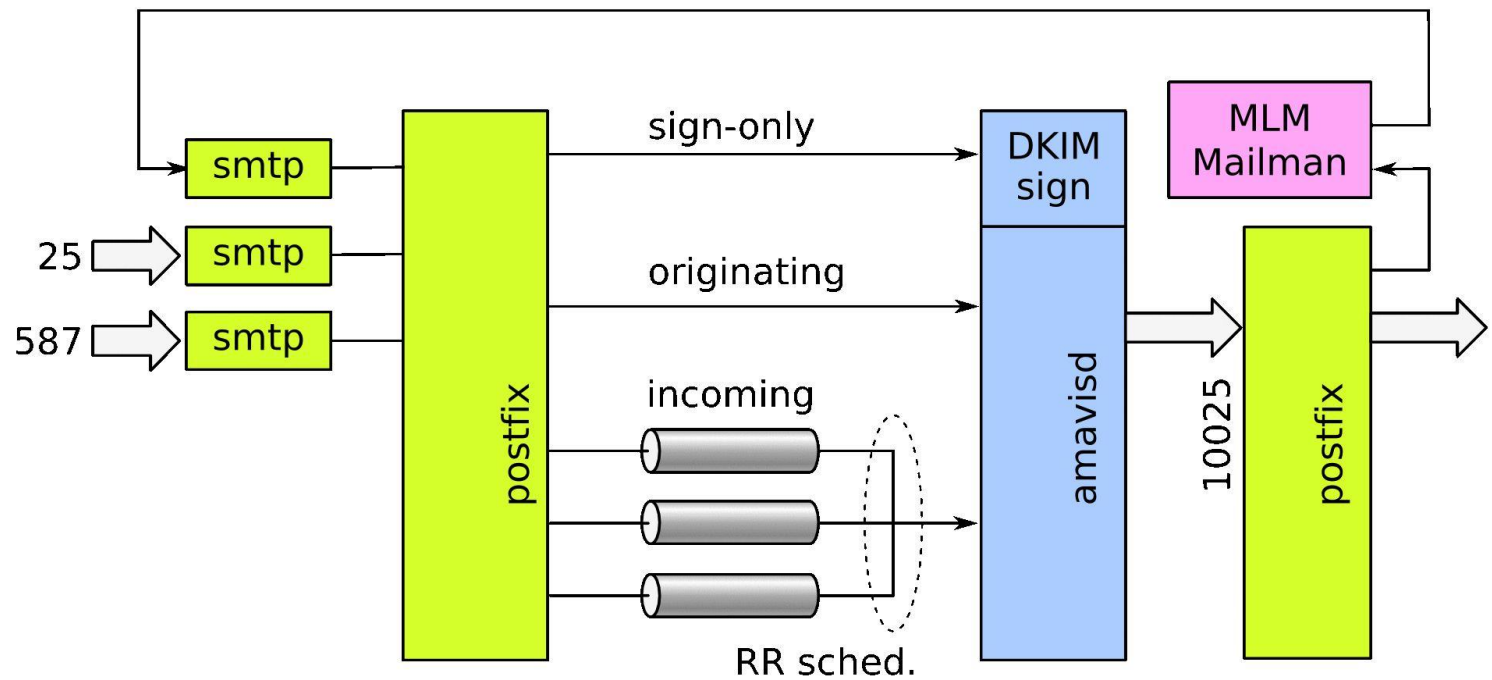
```
$a = "mavi";  
$b = 99;  
@d = (88);
```

geçerli

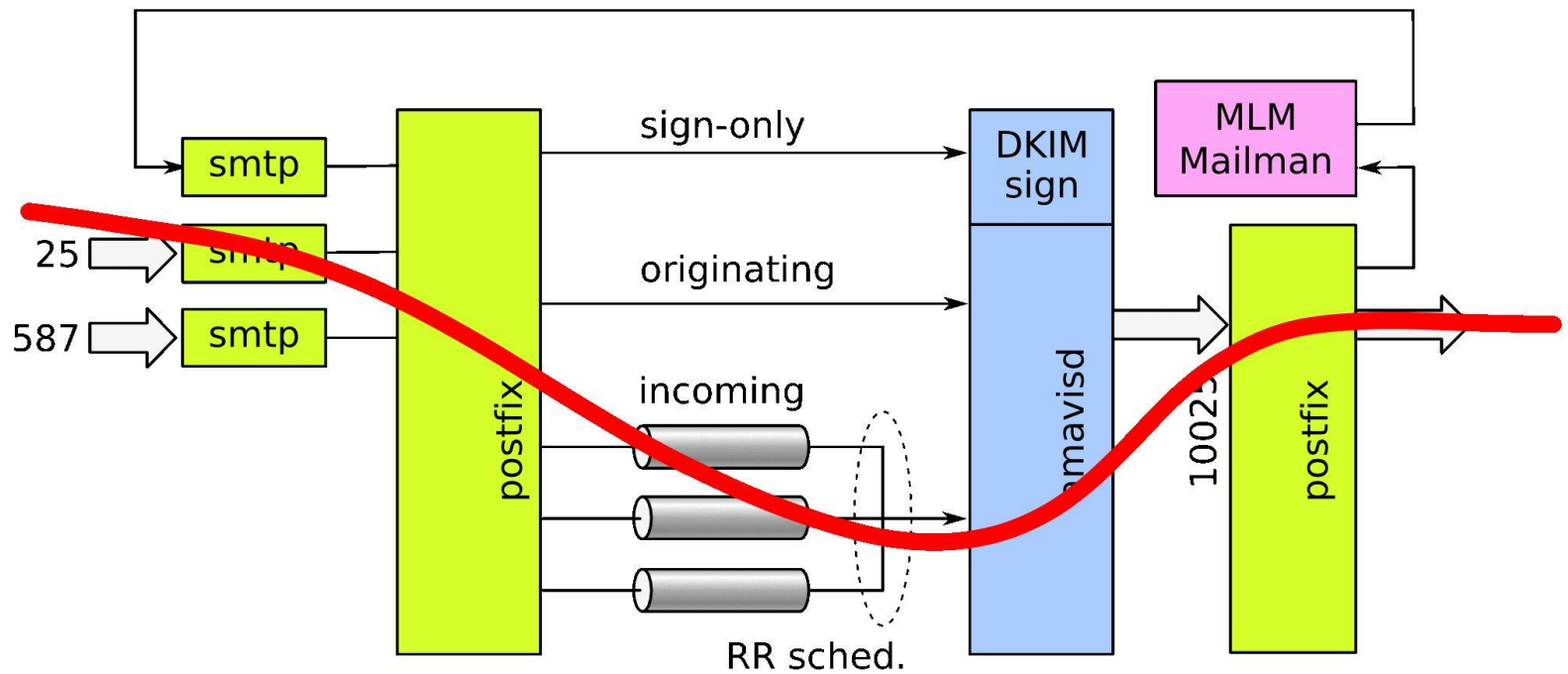
```
$a = "kırmızı";  
$b = 4;  
$c = ABC;  
@d = (88);
```



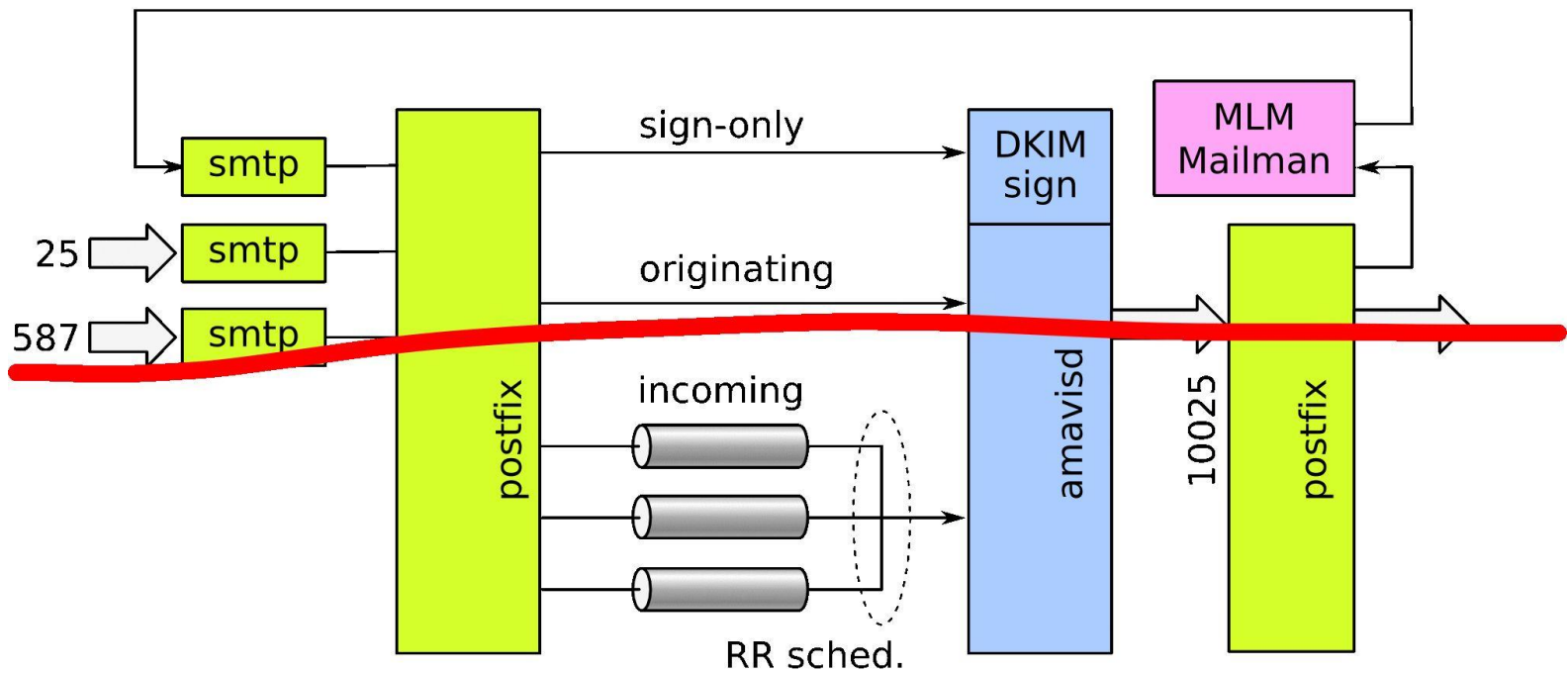
Amavisd-new



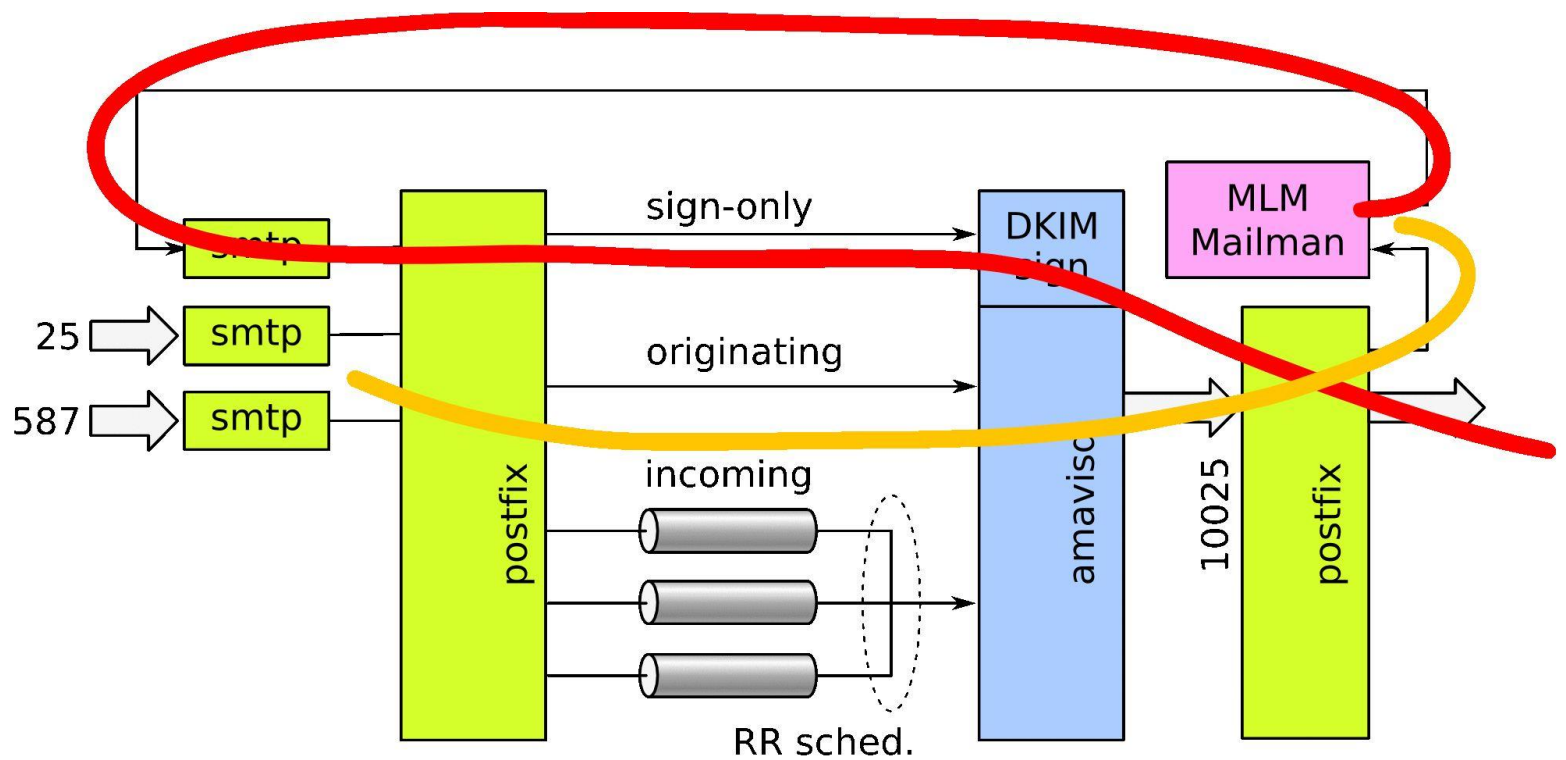
Amavisd-new



Amavisd-new



Amavisd-new



Amavisd-new

Ayarlar /etc/amavis/conf.d/50-user

```
$myhostname = "london0.caf.com.tr";  
$mydomain = "caf.com.tr";  
$inet_socket_port = 10025;  
$forward_method = 'smtp:[127.0.0.1]:10026';  
$notify_method = 'smtp:[127.0.0.1]:10026';  
$log_level = 2;  
$max_servers = 4;  
$enable_db = 1;  
$nanny_details_level = 2;  
$enable_dkim_verification = 1;  
$QUARANTINEDIR = undef;
```



Amavisd-new

Ayarlar (devam):

```
$sa_tag_level_deflt = undef;  
$sa_tag2_level_deflt = 6.2;  
$sa_kill_level_deflt = 6.9;  
$sa_dsn_cutoff_level = undef;  
$sa_crediblefrom_dsn_cutoff_level = undef;  
$final_virus_destiny    = D_DISCARD;  
$final_banned_destiny   = D_DISCARD;  
$final_spam_destiny     = D_PASS;  
$final_bad_header_destiny = D_PASS;
```



Amavisd-new

Jul 15 11:17:00 debian postfix-in/smtpd[27966]: connect from unknown[178.79.138.144]
Jul 15 11:17:22 debian postfix-in/smtpd[27966]: 5E3BAB8B7: client=unknown[178.79.138.144]
Jul 15 11:17:44 debian postfix-in/cleanup[27971]: 5E3BAB8B7: message-id=<>
Jul 15 11:17:44 debian postfix-in/qmgr[26897]: 5E3BAB8B7: from=<>, size=237, nrcpt=1 (queue active)
Jul 15 11:17:44 debian amavis[27960]: (27960-01) ESMTP::10025 /var/lib/amavis/tmp/amavis-20110715T111744-27960: <> -> <eray.aslan@caf.com.tr> SIZE=237 Received: from london0.caf.com.tr ([127.0.0.1]) by localhost (london0.caf.com.tr [127.0.0.1]) (amavisd-new, port 10025) with ESMTP for <eray.aslan@caf.com.tr>; Fri, 15 Jul 2011 11:17:44 -0400 (EDT)
Jul 15 11:17:44 debian amavis[27960]: (27960-01) Checking: 9ZRNpJEOEI18 [178.79.138.144] <> -> <eray.aslan@caf.com.tr>
Jul 15 11:17:44 debian amavis[27960]: (27960-01) p001 1 Content-Type: text/plain, size: 8 B, name:
Jul 15 11:17:44 debian amavis[27960]: (27960-01) check_header: 7, Missing required header field: "Date"
Jul 15 11:17:44 debian amavis[27960]: (27960-01) bounce unverifiable, <> -> <eray.aslan@caf.com.tr>
Jul 15 11:17:44 debian amavis[27960]: (27960-01) skip local delivery(3): <> -> <bad-header-quarantine>
Jul 15 11:17:44 debian amavis[27960]: (27960-01) SPAM-TAG, <> -> <eray.aslan@caf.com.tr>, No, score=4.237 required=6.2 tests=[FH_FROMEML_NOTLD=0.18, MISSING_DATE=1.396, MISSING_MID=0.14, RDNS_NONE=1.274, TO_MALFORMED=1.247] autolearn=no
Jul 15 11:17:44 debian postfix-out/smtpd[27975]: connect from localhost.localdomain[127.0.0.1]
Jul 15 11:17:44 debian postfix-out/smtpd[27975]: 5988078E7: client=unknown[178.79.138.144]
Jul 15 11:17:44 debian postfix-out/cleanup[27977]: 5988078E7: message-id=<>
Jul 15 11:17:44 debian postfix-out/qmgr[26886]: 5988078E7: from=<>, size=998, nrcpt=1 (queue active)
Jul 15 11:17:44 debian amavis[27960]: (27960-01) FWD via SMTP: <> -> <eray.aslan@caf.com.tr>, BODY=7BI 2.0.0 Ok, id=27960-01, from MTA([127.0.0.1]:10026): 250 2.0.0 Ok: queued as 5988078E7

.....



Amavisd-new

....

Jul 15 11:17:44 debian amavis[27960]: (27960-01) Passed BAD-HEADER, [178.79.138.144] [178.79.138.144] <> -> <eray.aslan@caf.com.tr>, mail_id: 9ZRNpJEOEII8, Hits: 4.237, size: 237, queued_as: 5988078E7, 265 ms

Jul 15 11:17:44 debian amavis[27960]: (27960-01) TIMING-SA total 130 ms - parse: 1.29 (1.0%), extract_message_metadata: 3 (2.0%), get_uri_detail_list: 0.19 (0.1%), tests_pri_-1000: 5 (3.8%), tests_pri_-950: 1.12 (0.9%), tests_pri_-900: 1.10 (0.8%), tests_pri_-400: 0.90 (0.7%), tests_pri_0: 32 (24.3%), check_spf: 5 (4.2%), poll_dns_idle: 65 (49.6%), check_pyzor: 0.24 (0.2%), tests_pri_500: 68 (52.0%), get_report: 1.54 (1.2%)

Jul 15 11:17:44 debian postfix-in/smtp[27972]: 5E3BAB8B7: to=<eray.aslan@caf.com.tr>, relay=127.0.0.1[127.0.0.1]:10025, delay=32, delays=31/0.01/0.01/0.26, dsn=2.0.0, status=sent (250 2.0.0 Ok, id=27960-01, from MTA([127.0.0.1]:10026): 250 2.0.0 Ok: queued as 5988078E7)

Jul 15 11:17:44 debian postfix-in/qmgr[26897]: 5E3BAB8B7: removed

Jul 15 11:17:44 debian amavis[27960]: (27960-01) TIMING [total 269 ms] - SMTP greeting: 4 (2%)2, SMTP EHLO: 1 (0%)2, SMTP pre-MAIL: 1 (0%)2, mkdir tempdir: 0 (0%)2, create email.txt: 0 (0%)2, SMTP pre-DATA-flush: 2 (1%)3, SMTP DATA: 37 (14%)17, check_init: 0 (0%)17, digest_hdr: 1 (0%)17, digest_body_dkim: 0 (0%)17, gen_mail_id: 1 (0%)18, mkdir parts: 1 (0%)18, mime_decode: 6 (2%)20, get-file-type1: 20 (8%)28, parts_decode: 0 (0%)28, check_header: 2 (1%)28, AV-scan-1: 4 (1%)30, spam-wb-list: 1 (1%)30, SA parse: 4 (1%)32, SA check: 124 (46%)78, update_cache: 7 (3%)81, decide_mail_destiny: 1 (0%)81, notif-quar: 3 (1%)82, save-to-local-mailbox: 2 (1%)83, fwd-connect: 16 (6%)89, fwd-xforward: 1 (0%)89, fwd-mail-pip: 16 (6%)95, fwd-rcpt-pip: 0 (0%)95, fwd-data-chkpnt: 0 (0%)95, write-header: 1 (0%)95, fwd-data-contents: 0 (0%)95, fwd-end-chkpnt: 3 (1%)96, prepare-dsn: 1 (0%)96, main_log_entry: 6 (2%)99, update_snmp: 2 (1%)99, SMTP pre-response: 1 (0%)99, SMTP response: 0 (0%)100, unlink-1-files: 0 (0%)100,...

Jul 15 11:17:44 debian amavis[27960]: (27960-01) ... rundown: 1 (0%)100

Jul 15 11:17:44 debian postfix-out/smtp[27978]: 5988078E7: to=<eray.aslan@caf.com.tr>, relay=mail.caf.com.tr[88.250.130.162]:25, delay=0.59, delays=0.02/0.01/0.28/0.28, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as C427560074)

Jul 15 11:17:44 debian postfix-out/qmgr[26886]: 5988078E7: removed

Jul 15 11:17:46 debian postfix-in/smtpd[27966]: disconnect from unknown[178.79.138.144]



Amavisd-new

Amavisd-agent

sysUpTime (0 days, 14:03:43.46)

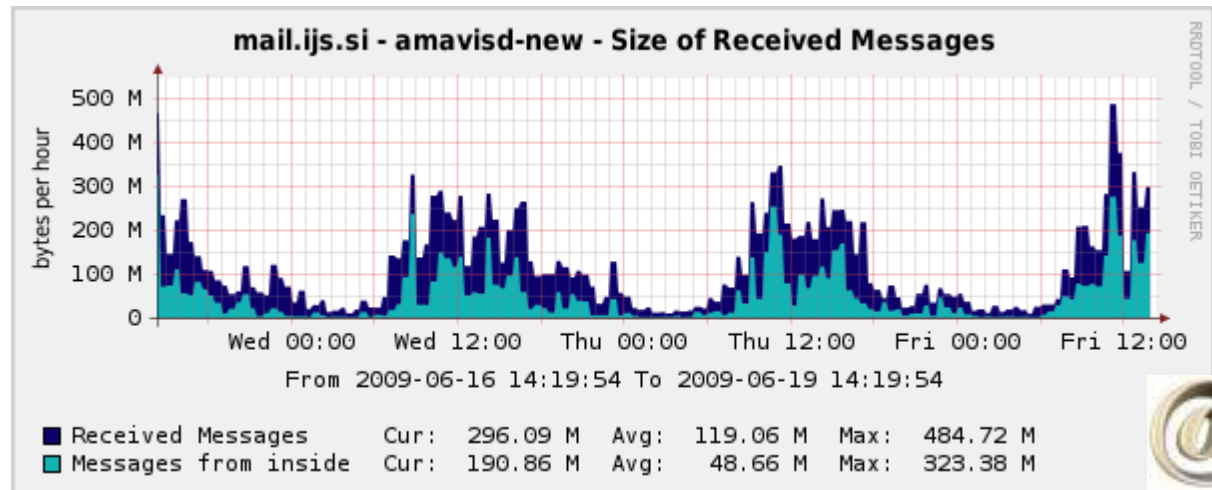
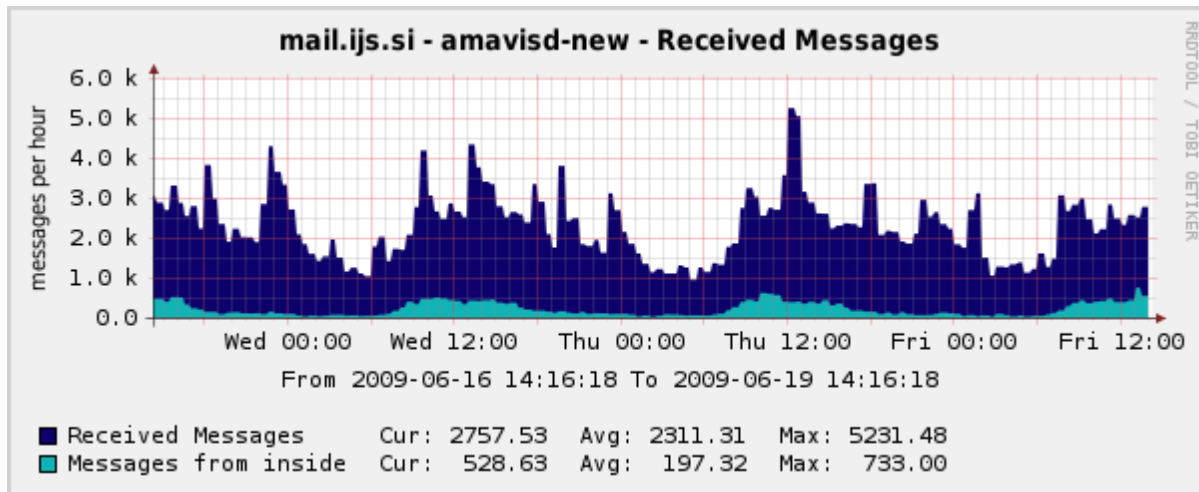
InMsgs	14490	1030/h	100.0% (InMsgs)
InMsgsRecips	27169	1932/h	187.5% (InMsgs)

ContentCleanMsgs	6020	428/h	41.5% (InMsgs)
ContentSpamMsgs	7807	555/h	53.9% (InMsgs)
ContentVirusMsgs	567	40/h	3.9% (InMsgs)
ContentBadHdrMsgs	91	6/h	0.6% (InMsgs)
ContentBannedMsgs	5	0/h	0.0% (InMsgs)

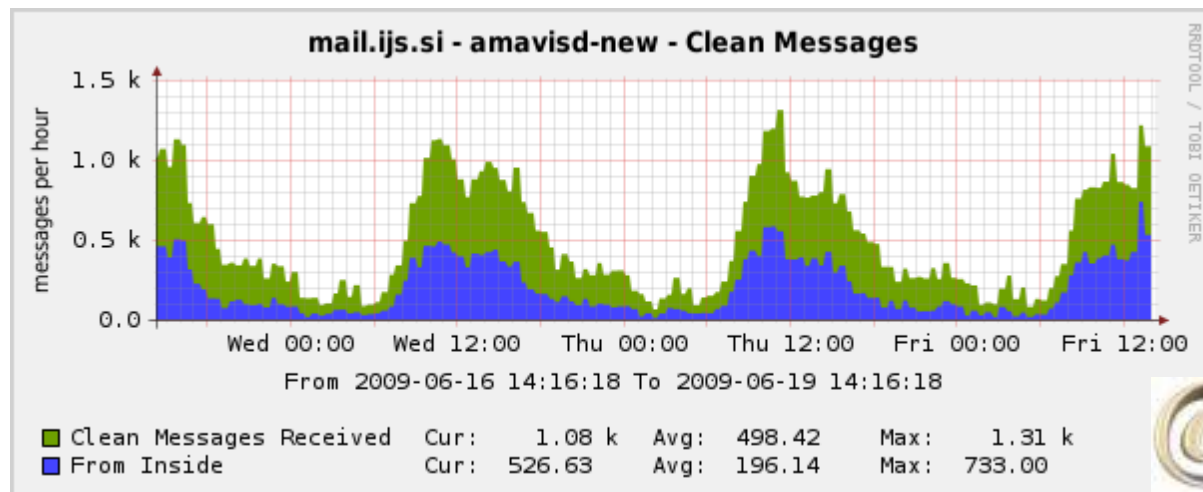
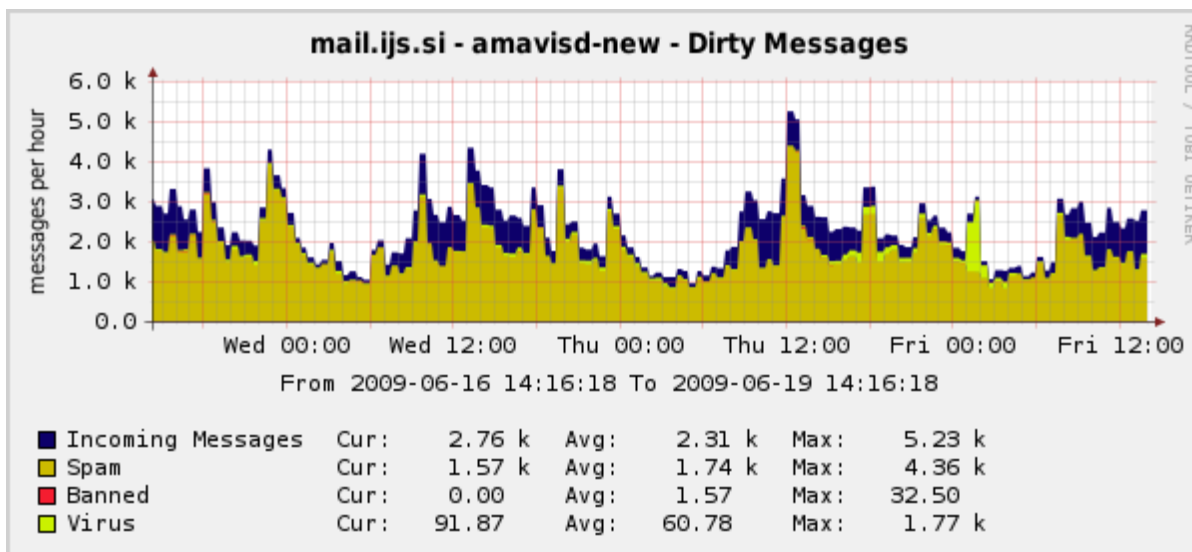
....



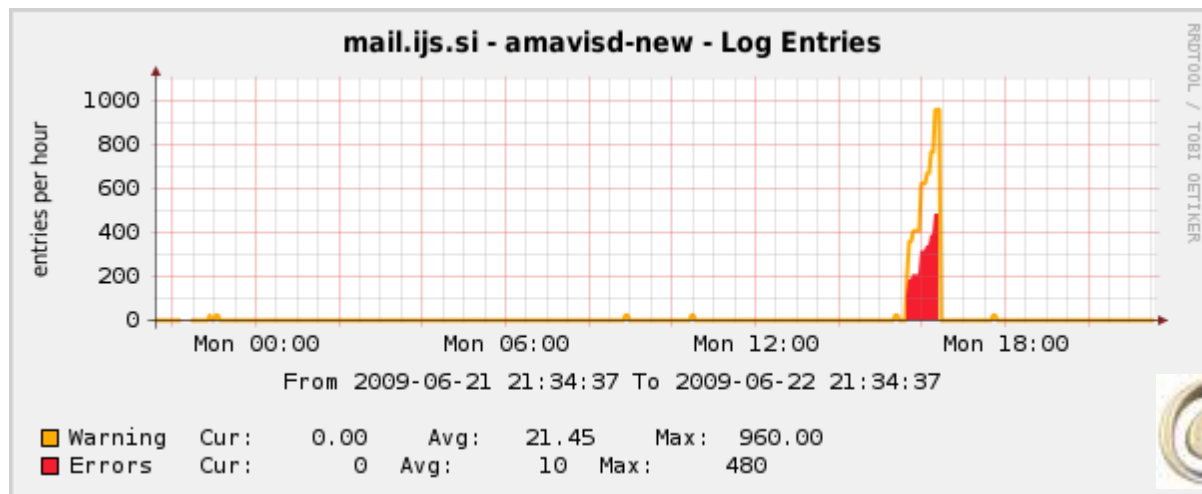
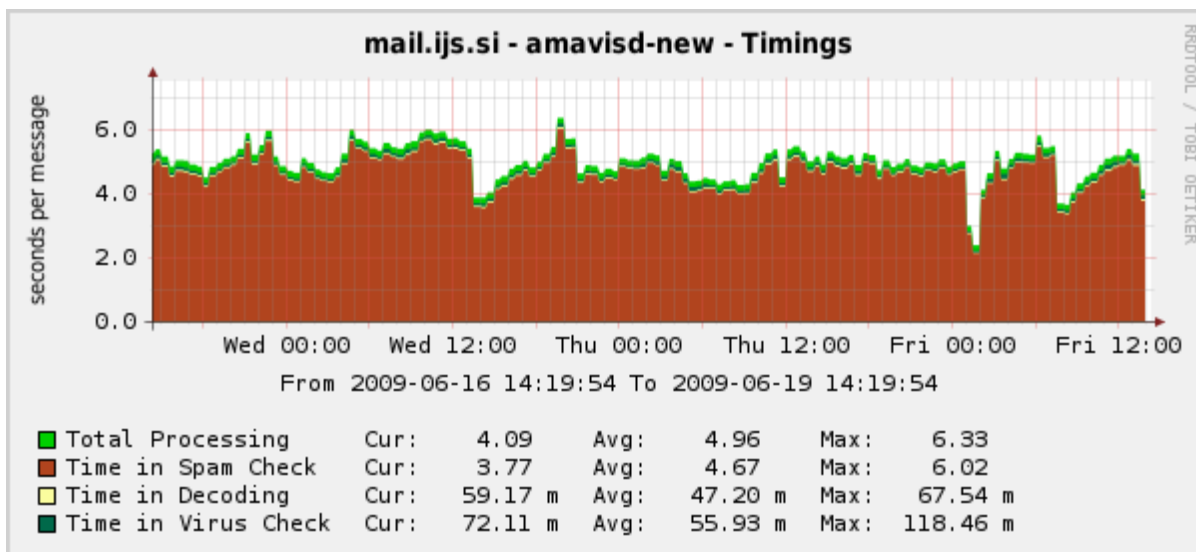
Amavisd-new



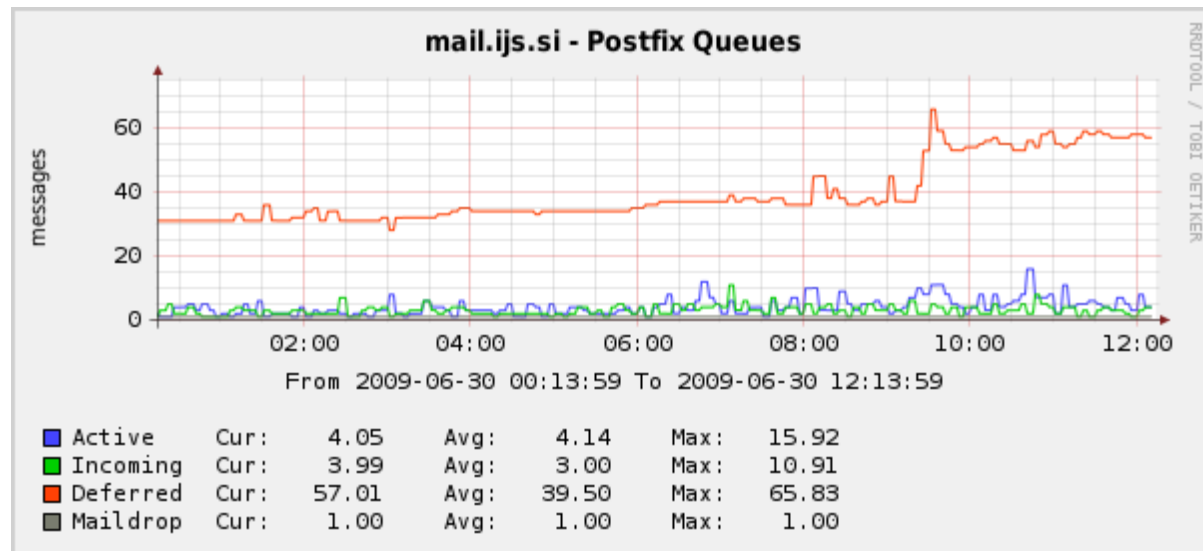
Amavisd-new



Amavisd-new



Amavisd-new



Dovecot

- Açık kaynak IMAP/POP sunucu
 - Sadece istemcilerden mail alımı. Mail gönderimi yok.
- İlk versiyon 2002
- Yüksek performans önemli hedeflerden biri
 - Genelde problem disk i/o → optimize



Dovecot

- Geleneksel mailbox formatları
- Dovecot index'leri
- Dovecot mailbox formatları



Dovecot

mbox

- Header'lardaki metadata filtreden geçer
 - X-UID, Status, X-Status, X-Keywords vs
- Mail silmek için datanın taşınması gerekir
 - Kırılgan: taşınırken crash
 - Eski mesajları silmek yavaş
- Devamlı eklemeler ile parçalı (fragmented)
- Ama az parçalı iken hızlı okuma



Dovecot

maildir

- Her mesaj ayrı dosyada
 - Bütün dosyaları okumak yavaş olabilir
- Mesaj metadata (okundu/cevaplandı vs) dosya isminde (name:2,<flags>)
 - Birçok rename()
- Kilitsiz maildir? Pek değil
 - Aksi halde rename() sırasında geçici dosya kaybı
 - Silindi mi yoksa okundu mu?



Dovecot

Dovecot Index Dosyaları

- Ana index
 - Mesaj listesi
 - Mesaj metadata'sı (okundu/cevaplandı vs)
 - Cache kayıt offsetleri
- Cache dosyası
 - Mesaj büyüklüğü, bazı metadata'lar
 - Sadece istemcilerin istediği bilgiler tutulur
 - Farklı istemciler farklı bilgi isteyebilir



Dovecot

Dovecot Ana Index

- İki dosya
 - dovecot.index: Yakın zamanda güncellenmiş snapshot
 - dovecot.index.log: Son değişiklikler
- Bütün değişiklikler log üzerinden
- Snapshot -> hafıza, sonra log'daki değişiklikleri uygula
 - Bir kere okunduktan sonra, sadece log'daki update'ler
 - Uzak dosya sistemleri için çok iyi (NFS, GFS2 vs)
- Snapshot'lar arada sırada güncellenir
 - Minimum I/O yüküne çalışılır
 - Yazmak okumaktan daha pahalı
- Log IMAP istemcilerinin “ne değişti” sorusu için de kullanılır (IDLE vs)



Dovecot

Dovecot Cache

- İyi performansın sebebi
- Farklı IMAP istemcileri farklı bilgi ister
 - Gereksiz bilgiyi önbelleğe almak I/O ve yer kaybı
- Esnek yapı: İstenilen kayıt eklenebilir
 - Kayıt başına karar: hayır, geçici, devamlı
- Önbellek bilgileri değişmez (IMAP protokolü garantiler)
 - Data kilitsiz eklenir (iki kere eklenebilir)
- Arada sırada yeniden oluşturulur -> sil, istenmeyen bilgiler olmadan yeniden oluştur



Dovecot

Single-dbox aka sdbox

- Her mesaj ayrı dosyada (u.<IMAP UID>)
- Mesajlarda değişmeyen metadata
 - Alış zamanı vs
- Maildir'e göre avantajlar
 - Dosya ismi değişmiyor
 - IMAP UID – dosya ismi eşleşmesi gerekmiyor
- Kalan metadata'lar (okundu/cevaplandı vs) sadece dovecot index dosyalarında
 - Arada sırada dovecot.index.backup oluşturur
 - Metadata'yı korumak için özen gösterir



Dovecot

Multi-dbox aka mbox

- Birkaç mesaj aynı dosyada (m.<id>)
 - dbox ile aynı dosya formatı
- Her mailbox'da birkaç dosya
 - Dosyalar 2MB boyutunda (ayarlanabilir)
 - Büyük dosyalar -> Parçalanma az ama silmek daha yavaş
 - Önceden yer ayırır
 - N günde bir döndürülebilir (backup)
 - Gecikmeli (her akşam?) mesaj silimi
- Güç kaybı bilgi kaybına yol açmaz
- Metadata'yı korumak için özen gösterir
 - Bozuk dosyanın kopyasını alır



Dovecot

[m|s]dbox faydaları

- Alternatif mail deposu
 - Kullanıcılar eski mesajlarını pek okumazlar
 - Düşük performans depo daha ucuz
- MIME bölümleri mesajdan ayrı saklanabilir
 - Base64 decoded (25% daha az yer)
- Single Instance Storage
 - Farklı mesajlar / aynı ek -> Tek ek



Kerberos

Bilgisayar/Network güvenlik ihtiyacı:

- Authentication – Kimlik doğrulama
 - Kim onay istiyor?
- Authorization - Yetkilendirme
 - Yetkisi var mı?
- Auditing - Denetleme
 - Yapılanların kontrolü



Kerberos

Authentication – Kimlik doğrulama

- Ne biliyorsun?
- Neye sahipsin?
- Nesin?



Daha
kuvvetli



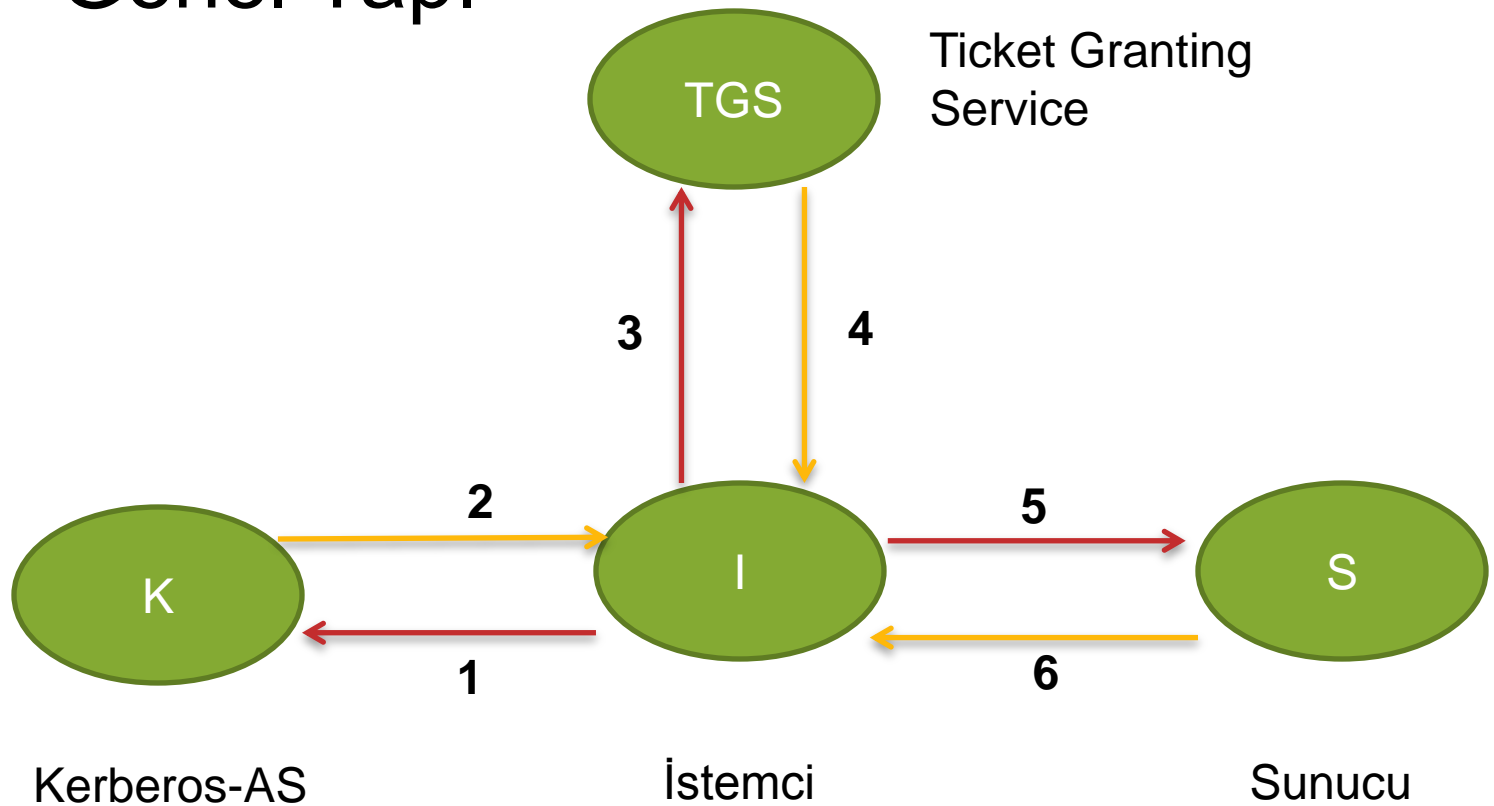
Kerberos

- MIT ve Heimdal (ve Shishi)
- Trusted third party (TTP)
 - KDC
 - *Put all your eggs in one basket and then watch that basket very carefully - Anonymous*
- Single sign-on
- Şifreler network üzerinden gönderilmez



Kerberos

- Genel Yapı



Kerberos

Varsayımlar

- Güvensiz network
 - Bütün paketler dinlenebilir ve yeniden oynatılabilir
- Güvenli zaman servisi
 - Yetkisiz zaman değişikliği yapılamaz



Kerberos

Varsayımlar (devam)

- İstemci kullandığı bilgisayara güvenebilir
 - Şifrelemek ve şifreleri çözmek için güvenli bir yer
- Bilgisayar kullanıcı tarafından kontrol edilir
 - Halka açık bilgisayarlar için doğru değil



Kerberos

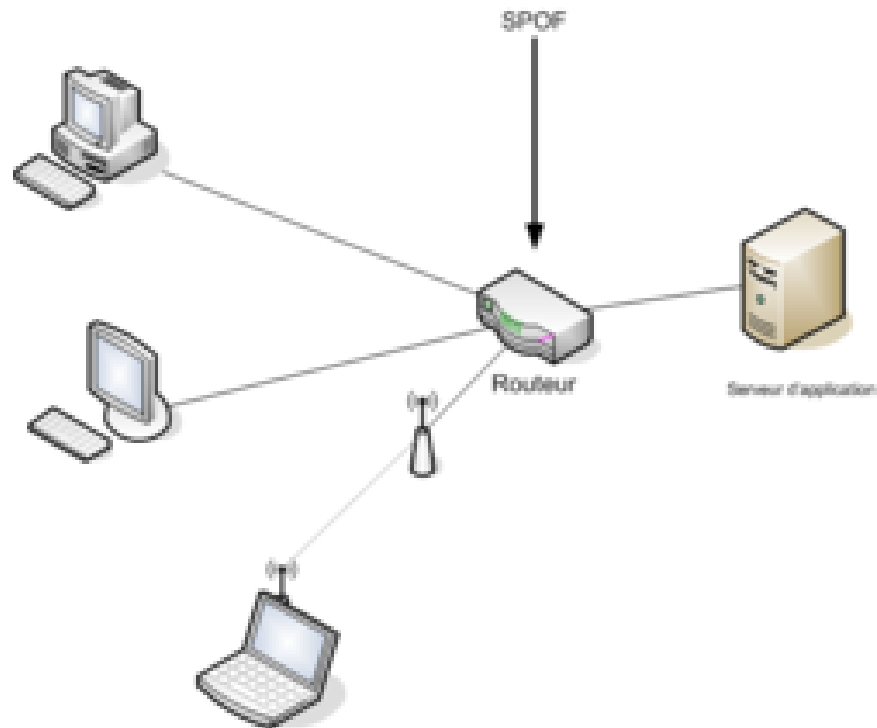
Sonuç

- Karışık sistemlerde
 - Windows, *nix, Solaris vs
- Ölçeklenebilir
- Geniş destek

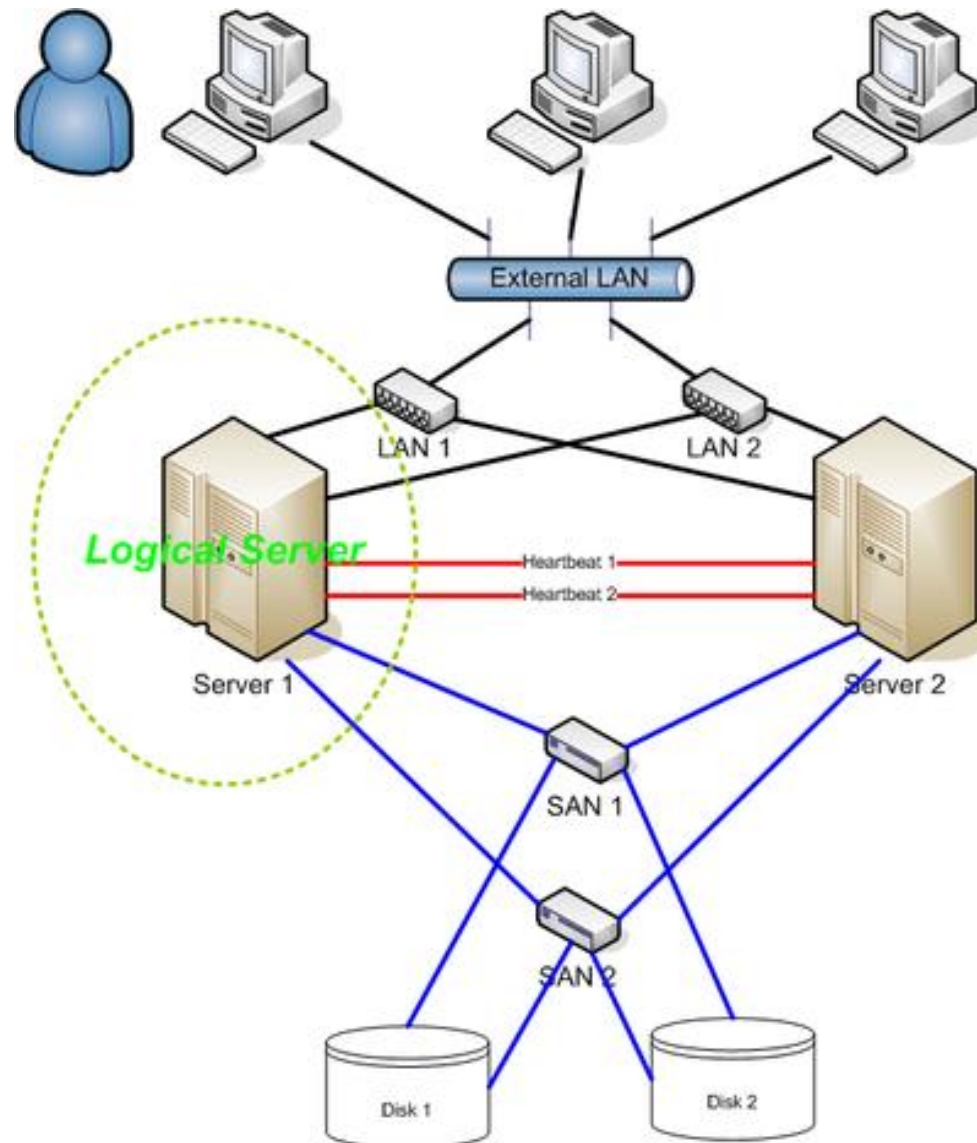


High - Availability

- SPOF (single point of failure)



High - Availability



Ayarlar – Postfix Örnek

```
# postconf -n
alias_database = hash:/etc/mail/aliases
biff = no
broken_sasl_auth_clients = yes
command_directory = /usr/sbin
content_filter = smtp-amavis:[127.0.0.1]:10024
daemon_directory = /usr/lib64/postfix
data_directory = /var/lib/postfix
debug_peer_level = 2
home_mailbox = .maildir/
html_directory = /usr/share/doc/postfix-2.7.2/html
local_recipient_maps = $alias_maps unix:passwd.byname
mydestination = $myhostname, localhost.$mydomain, localhost
myhostname = mail.caf.com.tr
mynetworks = 1.2.3.4/32, 5.6.7.8/32, 127.0.0.0/8
newaliases_path = /usr/bin/newaliases
```



Ayarlar – Postfix Örnek

```
parent_domain_matches_subdomains = debug_peer_list smtpd_access_maps
proxy_interfaces = 88.250.85.68, 188.59.0.34
queue_directory = /var/spool/postfix
readme_directory = /usr/share/doc/postfix-2.7.2/readme
receive_override_options = no_address_mappings
relay_domains = caf.com.tr, caf.local
relay_recipient_maps = hash:/etc/postfix/relay_recipients
remote_header_rewrite_domain = domain.invalid
sample_directory = /etc/postfix
sendmail_path = /usr/sbin/sendmail
show_user_unknown_table_name = no
smtp_skip_5xx_greeting = no
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_security_level = may
smtp_tls_session_cache_database =
    btree:${data_directory}/smtp_tls_session_cache
```



Ayarlar – Postfix Örnek

```
smtpd_banner = $myhostname ESMTP ${stress?(Stress condition)}
smtpd_discard_ehlo_keyword_address_maps =
    cidr:/etc/postfix/esmtp_access
smtpd_error_sleep_time = ${stress?0}${stress:5}
smtpd_etrn_restrictions = reject
smtpd_hard_error_limit = ${stress?1}${stress:20}
smtpd_helo_required = yes
smtpd_recipient_restrictions =
    reject_non_fqdn_sender
    reject_non_fqdn_recipient
    reject_unlisted_recipient
    reject_unlisted_sender
    permit_sasl_authenticated
    permit_mynetworks
    reject_unauth_destination
    check_recipient_access hash:/etc/postfix/recipient_checks
    check_client_access cidr:/etc/postfix/client_wl_bl_byip
```



Ayarlar – Postfix Örnek

```
reject_invalid_helo_hostname
check_sender_access pcre:/etc/postfix/valid_sender.pcre
check_sender_access hash:/etc/postfix/sender_access
reject_unknown_reverse_client_hostname
reject_rbl_client zen.spamhaus.org
warn_if_reject reject_rbl_client bl.mailspike.net

smtpd_sasl_auth_enable = yes
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
smtpd_timeout = ${stress?5}${stress:300}
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /etc/postfix/postfixCert.pem
smtpd_tls_eecdh_grade = strong
smtpd_tls_key_file = /etc/postfix/postfix.key
smtpd_tls_received_header = yes
```



Ayarlar – Postfix Örnek

```
smtpd_tls_session_cache_database =  
    btree:${data_directory}/smtpd_tls_session_cache  
strict_rfc821_envelopes = yes  
tls_random_source = dev:/dev/urandom  
transport_maps = hash:/etc/postfix/transport  
unknown_local_recipient_reject_code = 550  
virtual_alias_maps = proxy:mysql:/etc/postfix/mysql-virtual.cf  
virtual_gid_maps = static:1001  
virtual_mailbox_base = /  
virtual_mailbox_domains = zeplin.cn zeplin.net zeplin.com.tr  
    zeplin.eu  
virtual_mailbox_maps = proxy:mysql:/etc/postfix/mysql-virtual-  
maps.cf  
virtual_minimum_uid = 1000  
virtual_transport = dovecot  
virtual_uid_maps = static:1001
```



Ayarlar – Dovecot Örnek

```
# doveconf -n
# 2.0.9: /etc/dovecot/dovecot.conf
# OS: Linux 2.6.34-gentoo-r12 x86_64 Gentoo Base System release
1.12.14
auth_gssapi_hostname = mail.caf.com.tr
auth_krb5_keytab = /etc/dovecot/dovecot.keytab
auth_mechanisms = plain login gssapi
first_valid_uid = 1000
hostname = mail.caf.com.tr
listen = *
mail_location = maildir:~/.maildir
managesieve_notify_capability = mailto
managesieve_sieve_capability = fileinto reject envelope encoded-
    character vacation subaddress comparator-i;ascii-numeric
    relational regex imap4flags copy include variables body
    enotify environment mailbox date
```



Ayarlar – Dovecot Örnek

```
passdb {  
    args = /etc/dovecot/dovecot-sql.conf.ext  
    driver = sql  
}  
plugin {  
    sieve = ~/.dovecot.sieve  
    sieve_dir = ~/sieve  
}  
postmaster_address = postmaster@caf.com.tr  
protocols = imap pop3 lmtp sieve  
service auth {  
    unix_listener /var/spool/postfix/private/auth {  
        group = postfix  
        mode = 0660  
        user = postfix  
    }  
}
```



Ayarlar – Dovecot Örnek

```
unix_listener auth-userdb {  
    group = vmail  
    mode = 0600  
    user = vmail  
}  
  
service imap-login {  
    inet_listener imaps {  
        port = 993  
        ssl = yes  
    }  
}
```



Ayarlar – Dovecot Örnek

```
service managesieve-login {  
    inet_listener sieve {  
        port = 4190  
    }  
    vsz_limit = 256 M  
}  
ssl_cert = </etc/ssl/dovecot/dovecotCert.pem  
ssl_key = </etc/ssl/dovecot/dovecot.key  
userdb {  
    args = /etc/dovecot/dovecot-sql.conf.ext  
    driver = sql  
}  
protocol lda {  
    mail_plugins = sieve  
}  
protocol imap {  
    mail_max_userip_connections = 50  
}
```



Sorular?

