Электронная почта.
Не попадайтесь на крючок!

Павел Родионов
Cisco CSE Security

18 мая 2016

Cisco Forum

Краткий обзор

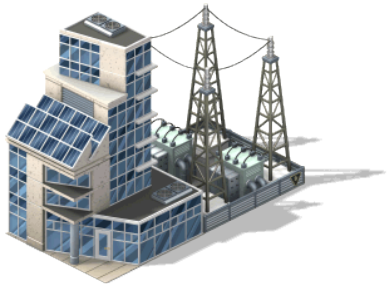
Cisco является лидером на рынке безопасности Email, но традиционно многие подразделения и люди, которые занимаются информационной безопасностью не рассматривают Email как сферу своей деятельности.

Эта сессия предоставит информацию, как работает SMTP и доставка email, а также какие механизмы существуют для защиты от врожденных недостатков SMTP протокола.

Содержание

- Краткая история SMTP
- Маршрутизатция: DNS MX записи
- Bounces: Протокол управления Email
- MIME: Отправка контента с использованием 7-бит ASCII
- Присоединенные функции безопасности SMTP: ESMTP, TLS, Аутентификация, SPF, DKIM, DMARC…
- Q&A

Но почему именно безопасность Email?



Май 2014

Атака на предприятия Укрзалізниці

Август 2014

Blackenergy 0-Day атака на широкий спектр органов госвласти в Украине

Октябрь 2015

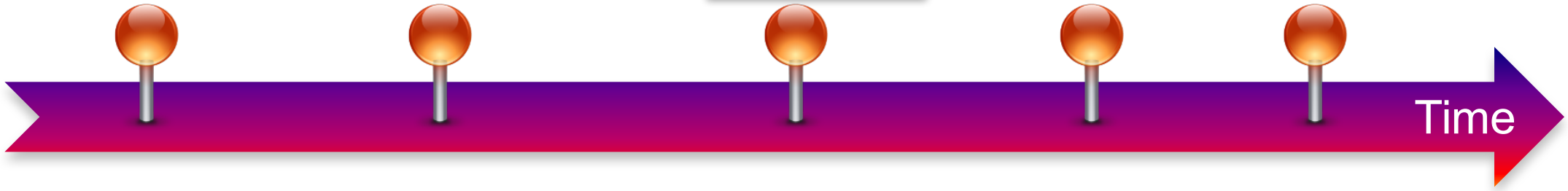
Blackenergy атака на медиакомпании. Уничтожение видеоматериалов, вывод из строя рабочих мест операторов

Декабрь 2015

Blackenergy атака на ряд облэнерго. Вывод из строя АСУТП электроподстанций, обесточена значительная территория на несколько часов

Декабрь 2015

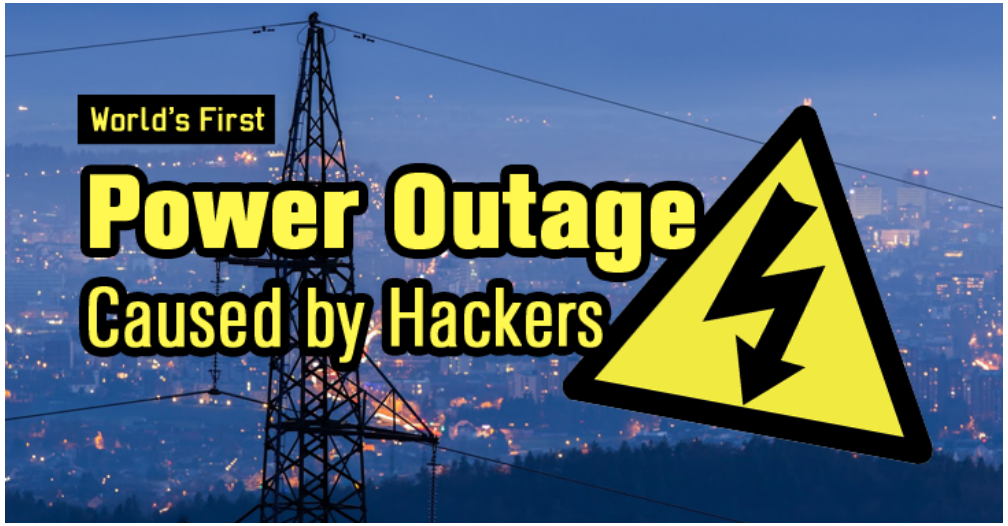
Атака на АП Борисполь при помощи BlackEnergy



Кибератаки в Украине

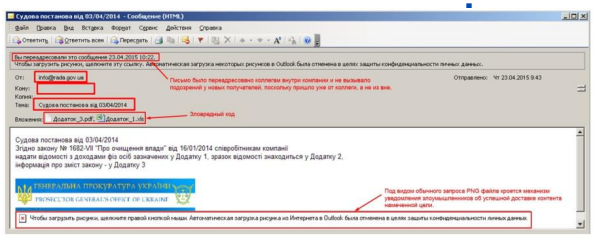
Вектор -- Email

- Перед атакой следует стадия рекогнисцировки
  - производится анализ email адресов компании, формирование соответствующих образом созданных писем, чтобы пользователь их открыл
- Атака включает рассылку электронных писем с вредоносным содержимым, который не обнаруживается традиционными средствами защиты
- Для включения базовых механизмов безопасности часто даже не надо менять оборудование
  - SPF, DKIM, DMARC, NIST 800-177 (общее описание)



Типичная атака. Starlight Media

1 Фишинговое письмо



2 Действия пользователя

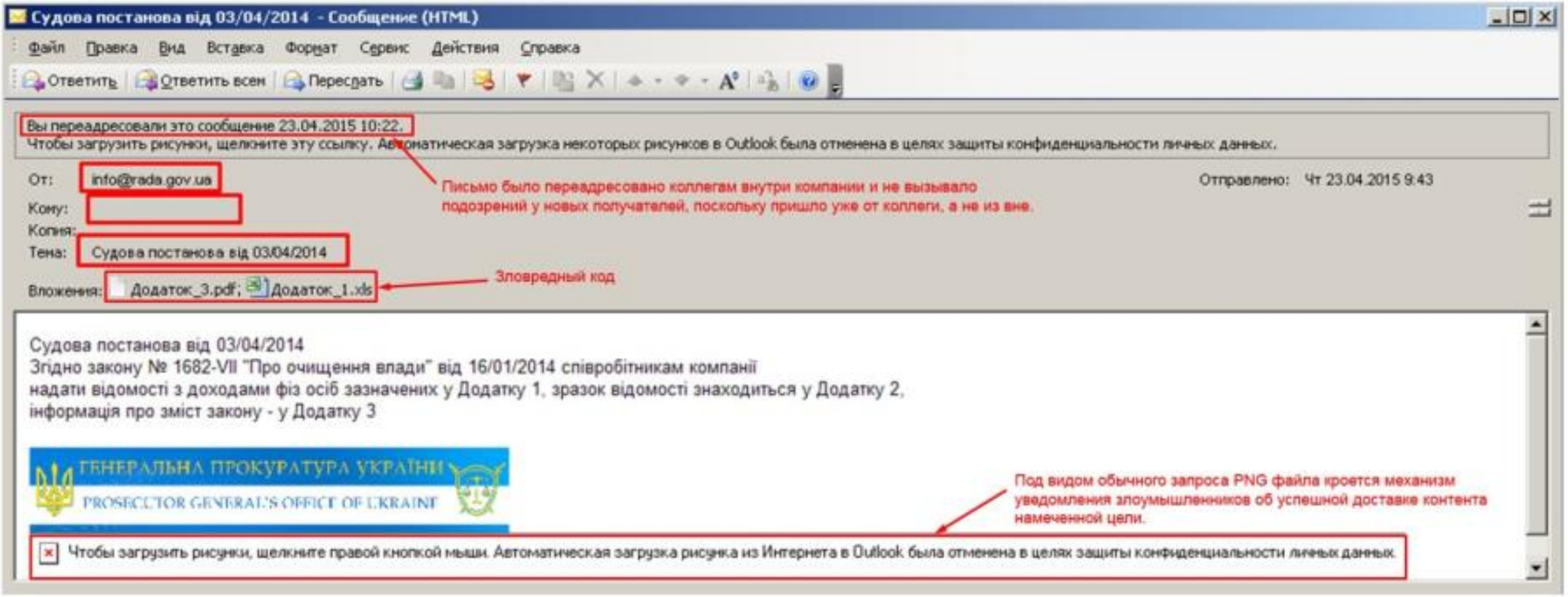
3 Эксплоит, загрузка основного тела, распространение

4 Вызов, CnC, дополнительный инструмент

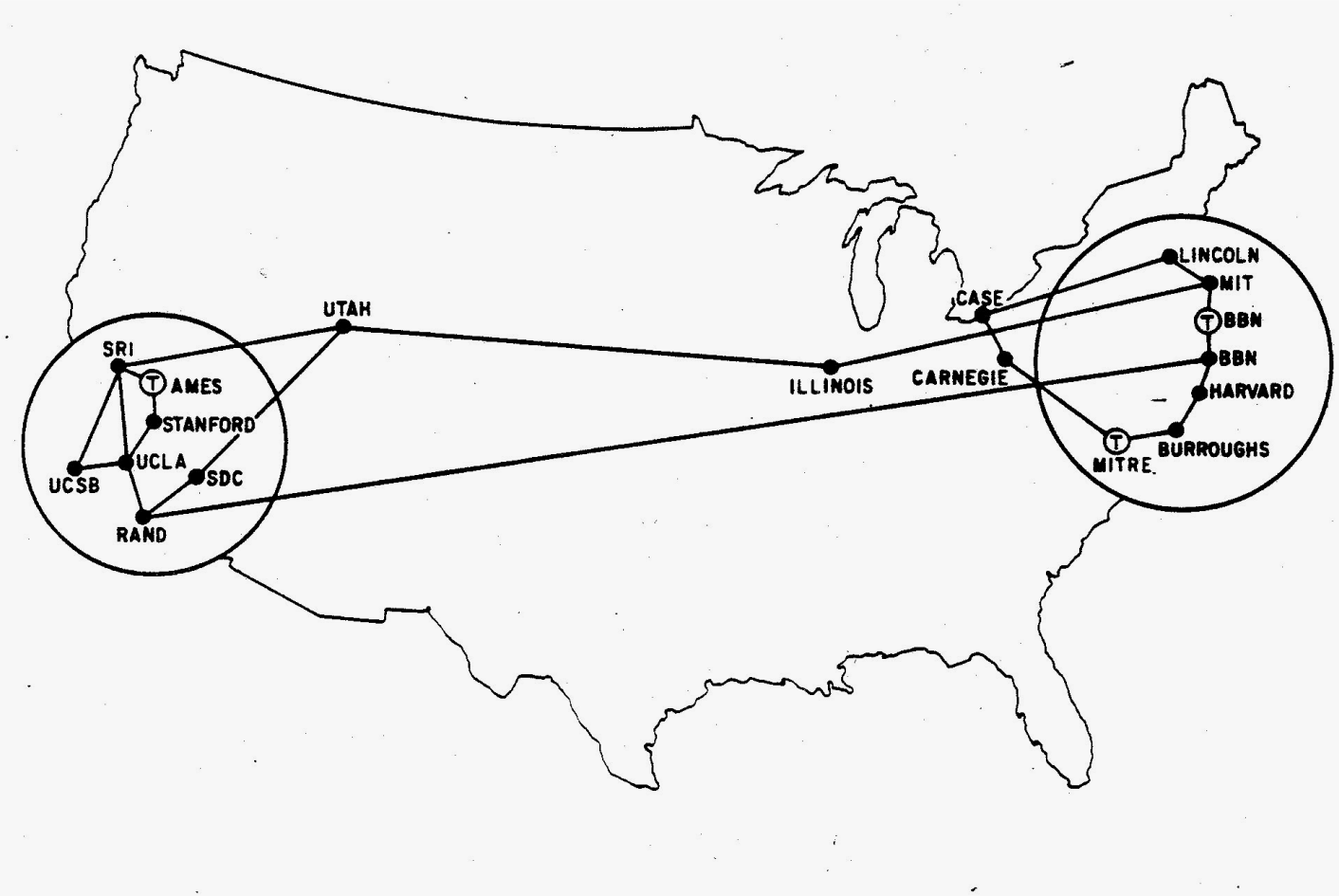
5 Распространение по сети

6 Хищение данных, ботнет, удаление…

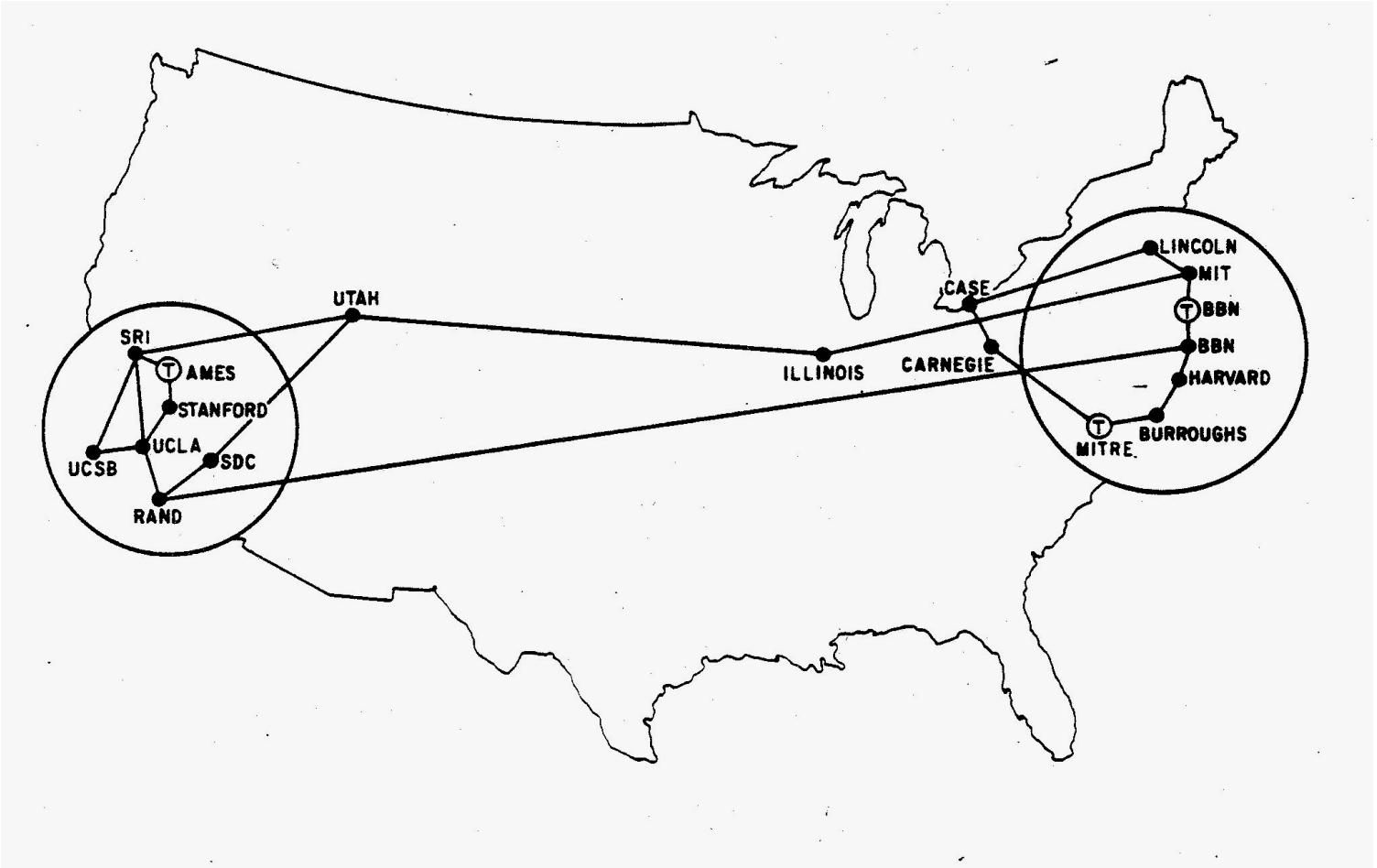
То самое письмо!



Краткая история SMTP



ARPANET в 1971



Source: Heart, F., McKenzie, A., McQuillian, J., and Walden, D., ARPANET Completion Report, Bolt, Beranek and Newman, Burlington, MA, January 4, 1978

Первая система Email: SNDMSG & CPYNET

BBN-TENEXB

DEC PDP-10
216 KB memory

Teletype KSR-33

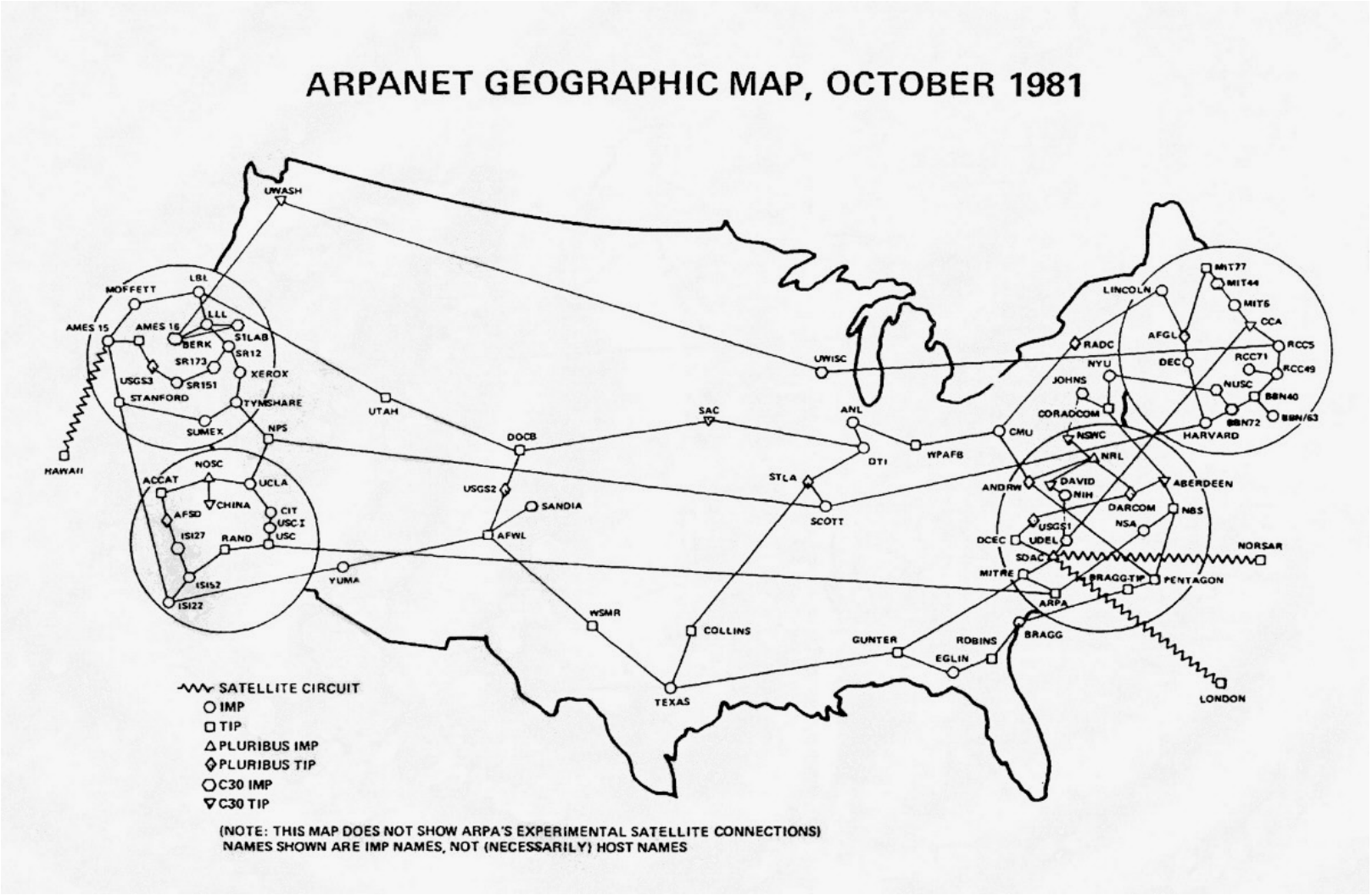
Первая email программа!

BBN-TENEXA

DEC PDP-10
288 KB memory

Source: http://openmap.bbn.com/~tomlinso/ray/ka10.html, retrieved 01 Dec 2014. Photograph courtesy of Dan Murphy,

1981: RFC788, Simple Mail Transfer Protocol



Source: http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html, retrieved 01 December 2014.

14

1978: Первый спамер, Гари Тверк!

Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT
Date: 1 May 1978 1233-EDT
From: THUERK at DEC-MARLBORO
Subject: ADRIAN@SRI-KL
To: DDAY at SRI-KL, DAY at SRI-KL, DEBOER at UCLA-CCN,
To: WASHDC at SRI-KL, LOGICON at USC-ISI, SDAC at USC-ISI,
To: DELDO at USC-ISI, DELEOT at USC-ISI, DELFINO at USC-ISI,
To: DENICOFF at USC-ISI, DESPAIN at USC-ISI, DEUTSCH at SRI-KL,
To: DEUTSCH at PARC-MAXC, EMY at CCA-TENEX, DIETER at USC-ISIB,
To: DINES at AMES-67, MERADCON at SRI-KL, EPG-SPEC at SRI-KA,
To: DIVELY at SRI-KL, DODD at USC-ISI, DONCHIN at USC-ISIC,
To: JED at LLL-COMP, DORIN at CCA-TENEX, NYU at SRI-KA,
To: DOUGHERTY at USC-ISI, PACOMJ6 at USC-ISI,
To: DEBBY at UCLA-SECURITY, BELL at SRI-KL, JHANNON at SRI-KA,
To: DUBOIS at USC-ISI, DUDA at SRI-KL, POH at USC-ISI,
To: LES at SU-AI, EAST at BBN-TENEX, DEASTMAN at USC-ECL,
To: EBISU at I4-TENEX, NAC at USC-ISIE, ECONOMIDIS at I4-TENEX,
To: WALSH at SRI-KL, GEDWARDS at SRI-KL, WEDWARDS at USC-ISI,
To: NUSC at SRI-KL, RM at SU-AI, ELKIND at PARC-MAXC,
To: ELLENBY at PARC-MAXC, ELLIS at PARC-MAXC, ELLIS at USC-ISIB,
To: ENGELBART at SRI-KL, ENGELMORE at SUMEX-AIM,
To: ENGLISH at PARC-MAXC, ERNST at I4-TENEX,
To: ESTRIN at MIT-MULTICS, EYRES at USC-ISIC,
To: FAGAN at SUMEX-AIM, FALCONER at SRI-KL,
To: DUF at UCLA-SECURITY, FARBER at RAND-UNIX, PMF at SU-AI,
To: HALFF at USC-ISI, RJF at MIT-MC, FEIERBACH at I4-TENEX,
To: FEIGENBAUM at USC-ISI, FEINLER at SRI-KL,

1978: Первый спамер, Гари Тверк!

To: FELDMAN at SUMEX-AIM, FELDMAN at SRI-KL, FERNBACH at LLL-COMP,
To: FERRARA at RADC-MULTICS, FERRETTI at SRI-KA,
To: FIALA at PARC-MAXC, FICKAS at USC-ISIC, AFIELD at I4-TENEX,
To: FIKES at PARC-MAXC, REF at SU-AI, FINK at MIT-MULTICS,
To: FINKEL at USC-ISIB, FINN at USC-ISIB, AFGWC at BBN-TENEX,
To: FLINT at SRI-KL, WALSH at SRI-KL, DRXAN at SRI-KA,
To: FOX at SRI-KL, FRANCESCHINI at MIT-MULTICS,
To: SAI at USC-ISIC, FREDRICKSON at RAND-RCC, ETAC at BBN-TENEXB,
To: FREYLING at BBN-TENEXE, FRIEDLAND at SUMEX-AIM,
To: FRIENDSHUH at SUMEX-AIM, FRITSCH at LLL-COMP, ME at SU-AI,
To: FURST at BBN-TENEXB, FUSS at LLL-COMP, OP-FYE at USC-ISIB,
To: SCHILL at USC-ISIC, GAGLIARDI at USC-ISIC,
To: GAINES at RAND-UNIX, GALLENSON at USC-ISIB,
To: GAMBLE at BBN-TENEXE, GAMMILL at RAND-UNIX,
To: GANAN at USC-ISI, GARCIA at SUMEX-AIM,
To: GARDNER at SUMEX-AIM, MCCUTCHEN at SRI-KL,
To: GARDNER at MIT-MULTICS, GARLICK at SRI-KL,
To: GARVEY at SRI-KL, GAUTHIER at USC-ISIB,
To: USGS-LIA at BBN-TENEX, GEMOETS at I4-TENEX,
To: GERHART at USC-ISIB, GERLA at USC-ISIE, GERLACH at I4-TENEX,
To: GERMAN at HARV-10, GERPHEIDE at SRI-KA, DANG at SRI-KL,
To: GESCHKE at PARC-MAXC, GIBBONS at CMU-10A,
To: GIFFORD.COMPSYS at MIT-MULTICS, JGILBERT at BBN-TENEXB,
To: SGILBERT at BBN-TENEXB, SDAC at USC-ISI,
To: GILLOGLY at RAND-UNIX, STEVE at RAND-UNIX,
To: GLEASON at SRI-KL, JAG;BIN(1525) at UCLA-CCN,
To: GOLD at LL-11, GOLDBERG at USC-ISIB, GOLDGERG at SRI-KL,

1978: Первый спамер, Гари Тверк!

To: GROBSTEIN at SRI-KL, GOLDSTEIN at BBN-TENEXB,
To: DARPM-NW at BBN-TENEXB, GOODENOUGH at USC-ISIB,
To: GEOFF at SRI-KL, GOODRICH at I4-TENEX, GOODWIN at USC-ISI,
To: GOVINSKY at SRI-KL, DEAN at I4-TENEX, TEG at MIT-MULTICS,
To: CCG at SU-AI, EPG-SPEC at SRI-KA, GRISS at USC-ECL,
To: BJG at RAND-UNIX, MCCUTCHEN at SRI-KL, GROBSTEIN at SRI-KL,
To: MOBAH at I4-TENEX, GUSTAFSON at USC-ISIB, GUTHARY at SRI-KL,
To: GUTTAG at USC-ISIB, GUYTON at RAND-RCC,
To: ETAC-AD at BBN-TENEXB, HAGMANN at USC-ECL, HALE at I4-TENEX,
To: HALFF at USC-ISI, DEHALL at MIT-MULTICS,
To: HAMPEL at LLL-COMP, HANNAH at USC-ISI,
To: NORSAR-TIP at USC-ISIC, SCRL at USC-ISI, HAPPY at SRI-KL,
To: HARDY at SRI-KL, IMPACT at SRI-KL, KLH at SRI-KL,
To: J33PAC at USC-ISI, HARRISON at SRI-KL, WALSH at SRI-KL,
To: DRCPM-FF at BBN-TENEXB, HART at AMES-67, HART at SRI-KL,
To: HATHAWAY at AMES-67, AFWL at I4-TENEX, BHR at RAND-UNIX,
To: RICK at RAND-UNIX, DEBE at USC-ISIB, HEARN at USC-ECL,
To: HEATH at UCLA-ATS, HEITMEYER at BBN-TENEX, ADTA at SRI-KA,
To: HENDRIX at SRI-KL, CH47M at BBN-TENEXB, HILLIER at SRI-KL,
To: HISS at I4-TENEX, ASLAB at USC-ISIC, HOLG at USC-ISIB,
To: HOLLINGWORTH at USC-ISIB, HOLLOWAY at HARV-10,
To: HOLMES at SRI-KL, HOLSWORTH at SRI-KA, HOLT at LLL-COMP,
To: HOLTHAM at LL, DHOLZMAN at RAND-UNIX, HOPPER at USC-ISIC,
To: HOROWITZ at USC-ISIB, VSC at USC-ISI, HOWARD at LLL-COMP,
To: HOWARD at USC-ISI, PURDUE at USC-ISI, HUBER at RAND-RCC,
To: HUNER at RADC-MULTICS, HUTSON at AMES-67, IMUS at USC-ISI,
To: JACOBS at USC-ISIE, JACOBS at BBN-TENEXB,

1978: Первый спамер, Гари Тверк!

To: JACQUES at BBN-TENEXB, JARVIS at PARC-MAXC,
To: JEFFERS at PARC-MAXC, JENKINS at PARC-MAXC,
To: JENSEN at SRI-KA, JIRAK at SUMEX-AIM, NICKIE at SRI-KL,
To: JOHNSON at SUMEX-AIM, JONES at SRI-KL, JONES at LLL-COMP,
To: JONES at I4-TENEX, RLJ at MIT-MC, JURAK at USC-ECL,
To: KAHLER at SUMEX-AIM, MWK at SU-AI, KAINE at USC-ISIB,
To: KALTGRAD at UCLA-ATS, MARK at UCLA-SECURITY, RAK at SU-AI,
To: KASTNER at USC-ISIB, KATT at USC-ISIB,
To: UCLA-MNC at USC-ISI, ALAN at PARC-MAXC, KEENAN at USC-ISI,
To: KEHL at UCLA-CCN, KELLEY at SRI-KL, BANANA at I4-TENEX,
To: KELLOGG at USC-ISI, DDI at USC-ISI, KEMERY at SRI-KL,
To: KEMMERER at UCLA-ATS, PARVIZ at UCLA-ATS, KING at SUMEX-AIM,
To: KIRSTEIN at USC-ISI, SDC at UCLA-SECURITY,
To: KLEINROCK at USC-ISI, KLEMBA at SRI-KL, CSK at USC-ISI,
To: KNIGHT at SRI-KL, KNOX at USC-ISI, KODA at USC-ISIB,
To: KODANI at AMES-67, KOOIJ at USC-ISI, KREMERS at SRI-KL,
To: BELL at SRI-KL, KUNZELMAN at SRI-KL, PROJX at SRI-KL,
To: LAMPSON at PARC-MAXC, SDL at RAND-UNIX, JOJO at SRI-KL,
To: SDC at USC-ISI, NELC3030 at USC-ISI,
To: LEDERBERG at SUMEX-AIM, LEDUC at SRI-KL, JSLEE at USC-ECL,
To: JACOBS at USC-ISIE, WREN at USC-ISIB, LEMONS at USC-ISIB,
To: LEUNG at SRI-KL, J33PAC at USC-ISI, LEVIN at USC-ISIB,
To: LEVINTHAL at SUMEX-AIM, LICHTENBERGER at I4-TENEX,
To: LICHTENSTEIN at USC-ISI, LIDDLE at PARC-MAXC,
To: LIEB at USC-ISIB, LIEBERMAN at SRI-KL, STANL at USC-ISIE,
To: LIERE at I4-TENEX, DOCB at USC-ISIC, LINDSAY at SRI-KL,
To: LINEBARGER at AMES-67, LIPKIS at USC-ECL, SLES at USC-ISI,

1978: Первый спамер, Гари Тверк!

To: LIS at SRI-KL, LONDON at USC-ISIB, J33PAC at USC-ISI,
To: LOPER at SRI-KA, LOUVIGNY at SRI-KL, LOVELACE at USC-ISIB,
To: LUCANIC at SRI-KL, LUCAS at USC-ISIB, DCL at SU-AI,
To: LUDLAM at UCLA-CCN, YNGVAR at SRI-KA, LYNCH at SRI-KL,
To: LYNN at USC-ISIB, MABREY at SRI-KL, MACKAY at AMES-67,
To: MADER at USC-ISIB, MAGILL at SRI-KL, KMAHONEY at BBN-TENEX,
To: MANN at USC-ISIB, ZM at SU-AI, MANNING at USC-ISI,
To: MANTIPLY at I4-TENEX, MARIN at I4-TENEX, SCRL at USC-ISI,
To: HARALD at SRI-KA, GLORIA-JEAN at UCLA-CCN, MARTIN at USC-ISIC,
To: WMARTIN at USC-ISI, GRM at RAND-UNIX, MASINTER at USC-ISI,
To: MASON at USC-ISIB, MATHIS at SRI-KL, MAYNARD at USC-ISIC,
To: MCBREARTY at SRI-KL, MCCALL at SRI-KA, MCCARTHY at SU-AI,
To: MCCLELLAND at USC-ISI, DORIS at RAND-UNIX, MCCLURG at SRI-KL,
To: JOHN at I4-TENEX, MCCREIGHT at PARC-MAXC, MCCRUMB at USC-ISI,
To: DRXTE at SRI-KA
cc: BPM at SU-AI

MCKINLEY@USC-ISIB
MMCM@SRI-KL
OT-ITS@SRI-KA
BELL@SRI-KL
MEADE@SRI-KL
MARTIN@USC-ISI
MERRILL@BBN-TENEX
METCALFE@PARC-MAXC

1978: Первый спамер, Гари Тверк!

JMETZGER@USC-ISIB
MICHAEL@USC-ISIC
CMILLER@SUMEX-AIM
MILLER@USC-ISI
SCI@USC-ISI
MILLER@USC-ISIC
MITCHELL@PARC-MAXC
MITCHELL@USC-ISI
MITCHELL@SUMEX-AIM
MLM@SU-AI
JPDG@TENEXB
MOORE@USC-ISIB
WMORE@USC-ISIB
JAM@SU-AI
MORAN@PARC-MAXC
ROZ@SU-AI
MORGAN@USC-ISIB
MORRIS@PARC-MAXC
MORRIS@I4-TENEX
OT-ITS@SRI-KA
LISA@USC-ISIB
MOSHER@SRI-KL
MULHERN@USC-ISI
MUNTZ;BIN(1529)@UCLA-CCN
MYERS@USC-ISIC
MYERS@RAND-RCC
DRCPM-FF-FO@BBN-TENEXB

1978: Первый спамер, Гари Тверк!

NAGEL@USC-ISIB
NAPKE@SRI-KL
NARDI@SRI-KL
NAYLOR@USC-ISIE
LOU@USC-ISIE
NESBIT@RAND-RCC
NEUMANN@SRI-KA
NEVATIA@USC-ECL
NEWBY@USC-ISI
NEWEKK@SRI-KA
NIELSON@SRI-KL
NLL@SUMEX-AIM
NILSSON@SRI-KL
NITZAN@SRI-KL
NOEL@USC-ISIC
NORMAN@PARC-MAXC
NORTON@SRI-KL
JOAN@USC-ISIB
NOURSE@SUMEX-AIM
PDG@SRI-KL
OMALLEY@SRI-KA
OCKEN@USC-ISIC
OESTREICHER@USC-ISIB
OGDEN@SRI-KA
OKINAKA@USC-ISIE
OLSON@I4-TENEX
ORNSTEIN@PARC-MAXC

1978: Первый спамер, Гари Тверк!

PANKO@SRI-KL
TED@SU-AI
PARK@SRI-KL
PBARAN@USC-ISI
PARKER@USC-ISIB
PEARCE@USC-ISI
PEPIN@USC-ECL
PERKINS@USC-ISIB
PETERS@SRI-KL
AMPETERSON@USC-ISI
ASLAB@USC-ISIC
EPG-SPEC@SRI-KA
PEZDIRTZ@LLL-COMP
CHARLIE@I4-TENEX
UCLA-DOC@USC-ISI
WPHILLIPS@USC-ISI
PIERCY@MOFFETT-ARC
PINE@SRI-KL
PIPES@I4-TENEX
PIRTLE@SRI-KL
POGGIO@USC-ISIC
POH@USC-ISI
POOL@BBN-TENEX
POPEK@USC-ISI
POSTEL@USC-ISIB
POWER@SRI-KL
PRICE@USC-ECL
RANDALL@USC-ISIB
RANDALL@SRI-KA
RAPHAEL@SRI-KL
RAPP@RAND-RCC
RASMUSSEN@USC-ISIC
RATTNER@SRI-KL
RAY@ILL-NTX
FNWC@I4-TENEX
BRL@SRI-KL
RETZ@SRI-KL
SKIP@USC-ISIB
RICHARDSON@USC-ISIB
RICHES@USC-ECL
GWEN@USC-ECL
OP-RIEDEL@USC-ISIB
RIES@LLL-COMP
RINDFLEISCH@SUMEX-AIM
OP-ROBBINS@USC-ISIB
ROBINSON@SRI-KL
JROBINSON@SRI-KL
RODRIQUEZ@SRI-KL
MARTIN@USC-ISI
ROM@USC-ISIC
ROMIEZ@I4-TENEX
ROSE@USC-ISI
ROSEN@SRI-KL
BARBARA@I4-TENEX
ROTHENBERG@USC-ISIB
RUBIN@SRI-KL
JBR@SU-AI
RUBINSTEIN@BBN-TENEXD
RUDY@USC-ECL
RUGGERI@SRI-KA
RULIFSON@PARC-MAXC
DALE@USC-ISIB
SACERDOTI@SRI-KL
SAGALOWICZ@SRI-KL
ALS@SU-AI
SANTONI@USC-ISIC
SATTERTHWAITE@PARC-MAXC
SAWCHUK@USC-ECL
CPF-CC@USC-ISI
SCHELONKA@USC-ISI
SCHILL@USC-ISIC
SCHILLING@USC-ISI
SCHULZ@SUMEX-AIM
SCOTT@SUMEX-AIM
CPF-CC@USC-ISI
OP-SEATON@USC-ISIB
SENNE@LL
NORM@RAND-UNIX
AFWL@14-TENEX
SHEPPARD@LL-ASG
SHERWIN@USC-ISI

1978: Первый спамер, Гари Тверк!

SHERWOOD@SRI-KL
SHORT@SRI-KL
SHORTLIFE@SUMEX-AIM
SHOSHANI@BBN-TENEX
MARTIN@USC-ISI
UCLA-NMC@USC-ISIE
SDL@USC-ISIC
SKOCYPEC@USC-ISI
SLES@USC-ISI
SLOTTOW@UCLA-CCN
NOAA@14-TENEX
SMALL@USC-ISI
DAVESMITH@PARC-MAXC
DSMITH@RAND-UNIX
SMITH@SUMEX-AIM
SMITH@USC-ECL
MARCIE@I4-TENEX
USARSGEUR@USC-ISI
LOGICON@USC-ISI
EPA@SRI-KL
SONDEREGGER@USC-ISIB
SPEER@LL
AMICON-RN@USC-ISI
SPROULL@PARC-MAXC
PROJX@SRI-KL
STEF@SRI-KA
STEFIK@SUMEX-AIM
STEPHENS@SRI-KA
CFD@I4-TENEX
STOCKHAM@SRI-KA
STOTZ@USC-ISIB
ALLEN@UCLA-SECURITY
STOUTE@MIT-ML
STRADLING@SRI-KL
STROLLO@PARC-MAXC
UCLA-0638@UCLA-CCN
CRT@SRI-KA
SUNSHINE@RAND-UNIX
SUTHERLAND@SRI-KL
SUTHERLAND@RAND-UNIX
SUTHERLAND@PARC-MAXC
SUTTON@USC-ISIC
SWEER@SUMEX-AIM
TAFT@PARC-MAXC
TAYLOR@USC-ISIB
TAYLOR@PARC-MAXC
TAYNAI@SUMEX-AIM
TEITELMAN@PARC-MAXC
TENENBAUM@SRI-KL
GREEP@RAND-UNIX
TERRY@SUMEX-AIM
TESLER@PARC-MAXC
THACKER@PARC-MAXC
PWT@RAND-UNIX
TIPPIT@USC-ISIE
TOBAGI@USC-ISIE
TOGNETTI@SUMEX-AIM
TORRES@SRI-KL
TOWNLEY@HARV-10
ELINA@UCLA-ATS
TUCKER@SUMEX-AIM
TUGENDER@USC-ISIB
LLLSRG@MIT-MC
UNCAPHER@USC-ISIB
NOSC@SRI-KL
UNTULIS@SRI-KL
MIKE@UCLA-SECURITY
AARDVARK@UCLA-ATS
UZGALIS;BIN(0836)@UCLA-CCN
VANGOETHEM@UCLA-CCN
VANMIEROP@USC-ISIB
VANNOUHUYS@SRI-KL
VEIZADES@SUMEX-AIM
VESECKY@USC-ISI
AV@MIT-DMS
VICTOR@USC-ISIC
VIDAL@UCLA-SECURITY
OP-VILAIN@USC-ISIB
RV@RAND-UNIX
SDL@USC-ISIC
VOLPE@SRI-KL

1978: Первый спамер, Гари Тверк!

VONNEGUT@I4-TENEX
VU@SRI-KL
WACTLAR@CMU-10A
WAGNER@USC-ISI
WAHRMAN@RAND-UNIX
WALDINGER@SRI-KL
WALKER@UCLA-SECURITY
WALKER@SRI-KL
WALLACE@PARC-MAXC
EVE@UCLA-SECURITY
LOGICON@USC-ISI
DON@RAND-UNIX
WATSON@USC-ISIC
WEIDEL@USC-ECL
WEINBERG@SRI-KL
JLW@MIT-AI
LAUREN@UCLA-SECURITY
WEISSMAN@I4-TENEX
WELLS@USC-ISIC
GERSH@USC-ISI
WETHEREL@LLL-COMP
RWW@SU-AI
SCRL@USC-ISI
TWHELLER@SRI-KA
MABREY@SRI-KL
WHITE@PARC-MAXC
WHITE@SUMEX-AIM
WIEDERHOLD@SUMEX-AIM
WILBER@SRI-KL
EPG-SPEC@SRI-KA
WILCOX@SUMEX-AIM
WILCZYNSKI@USC-ISIB
WILE@USC-ISIB
OP-WILLIAMS@USC-ISIB
WILSON@USC-ISIB
TW@SU-AI
SCI@USC-ISI
WISNIEWSKI@RAND-UNIX
WOLF@SRI-KL
PAT@SU-AI
NELC3030@USC-ISI
WYATT@HARV-10
LEO@USC-ISIB
YEH@LLL-COMP
YONKE@USC-ISIB
YOUNGBERG@SRI-KA
ZEGERS@SRI-KL
ZOLOTOW@SRI-KL
ZOSEL@LLL-COMP

1978: Первый спамер, Гари Тверк!

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

Первый антиспам

ON 2 MAY 78 DIGITAL EQUIPMENT CORPORATION (DEC) SENT OUT AN ARPANET MESSAGE ADVERTISING THEIR NEW COMPUTER SYSTEMS. THIS WAS A FLAGRANT VIOLATION OF THE USE OF ARPANET AS THE NETWORK IS TO BE USED FOR OFFICIAL U.S. GOVERNMENT BUSINESS ONLY. APPROPRIATE ACTION IS BEING TAKEN TO PRECLUDE ITS OCCURRENCE AGAIN.

IN ENFORCEMENT OF THIS POLICY DCA IS DEPENDENT ON THE ARPANET SPONSORS, AND HOST AND TIP LIAISONS. IT IS IMPERATIVE YOU INFORM YOUR USERS AND CONTRACTORS WHO ARE PROVIDED ARPANET ACCESS THE MEANING OF THIS POLICY.

THANK YOU FOR YOUR COOPERATION.

MAJOR RAYMOND CZAHOR

CHIEF, ARPANET MANAGEMENT BRANCH, DCA

Специфика дизайна SMTP

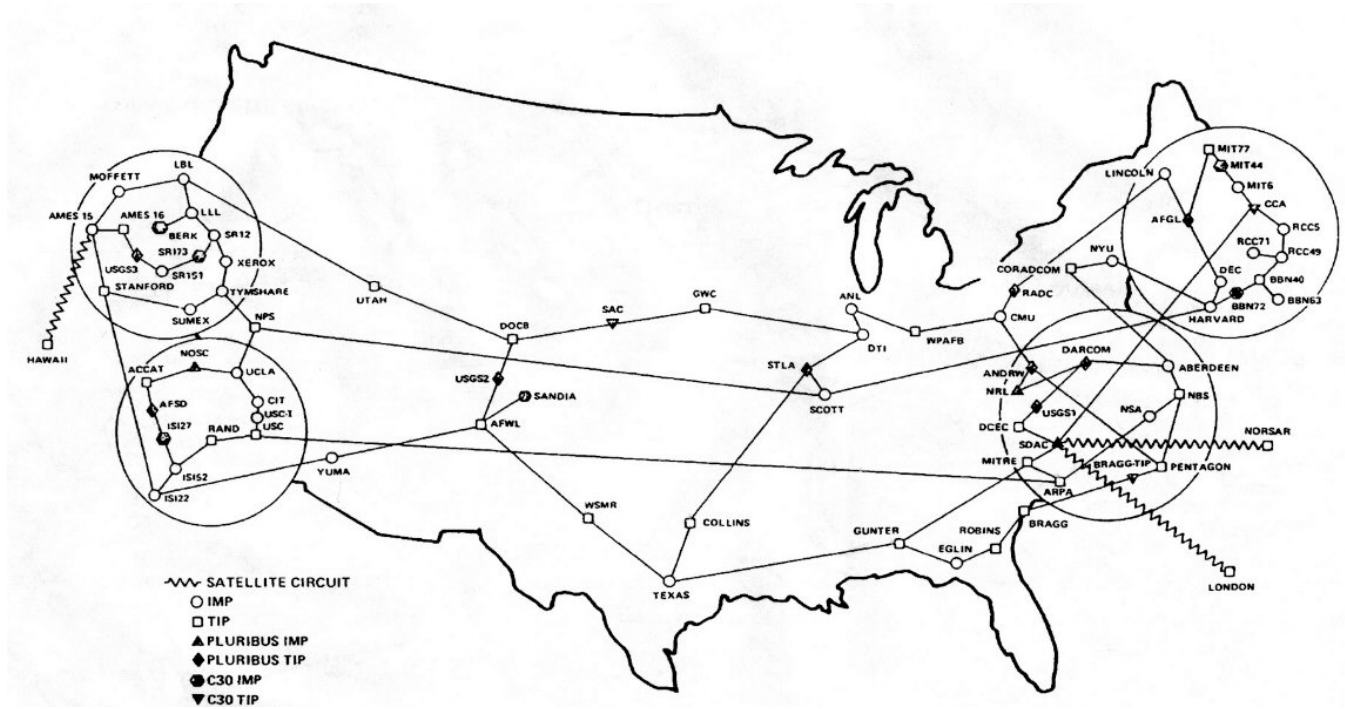
Hop-by-hop. Ретрансляция узел-узел

Store-and-forward. С промежуточным хранением

Всегда пытается доставить!

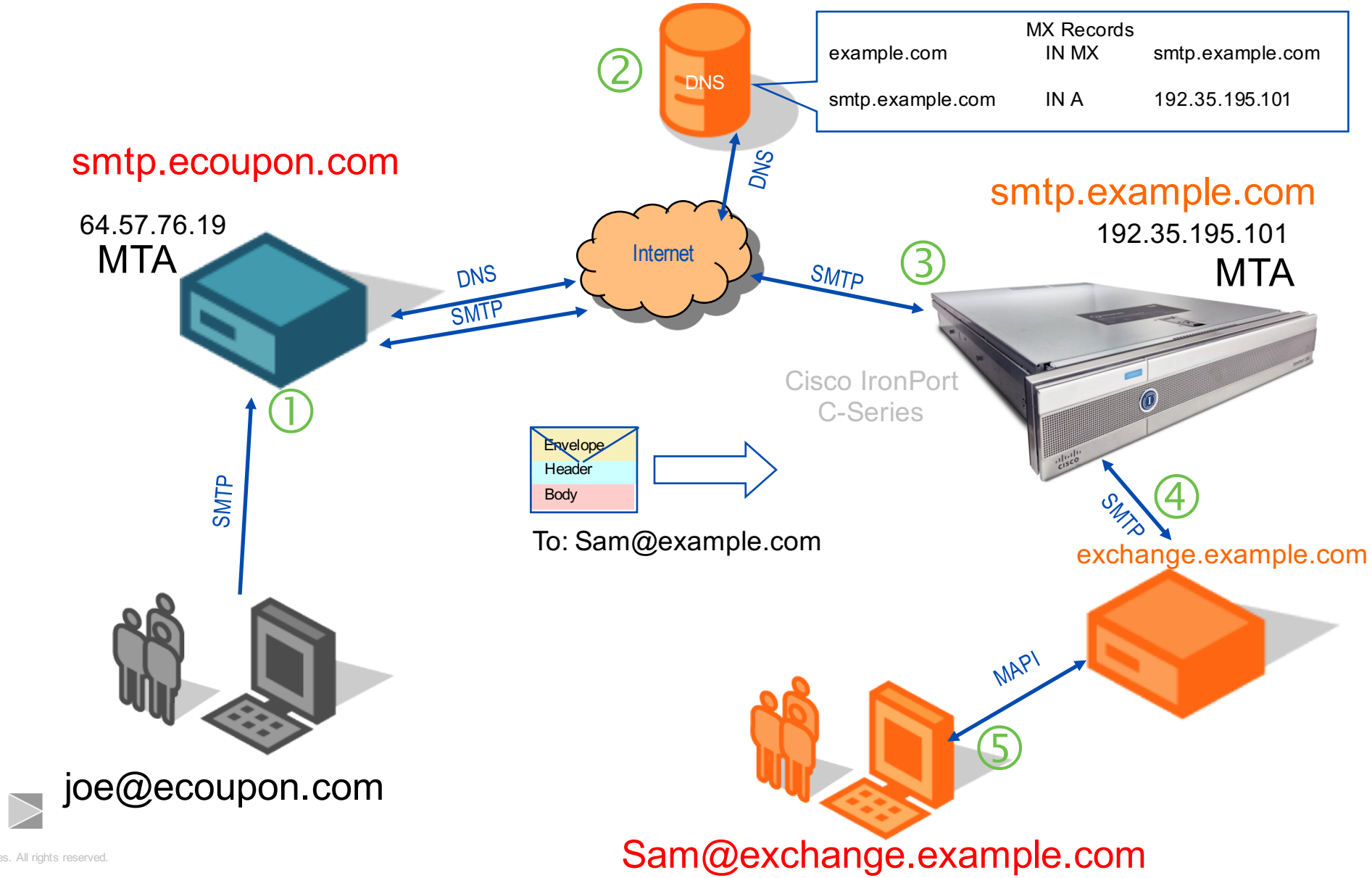
7-бит ASCII

Скрытая аутентификация

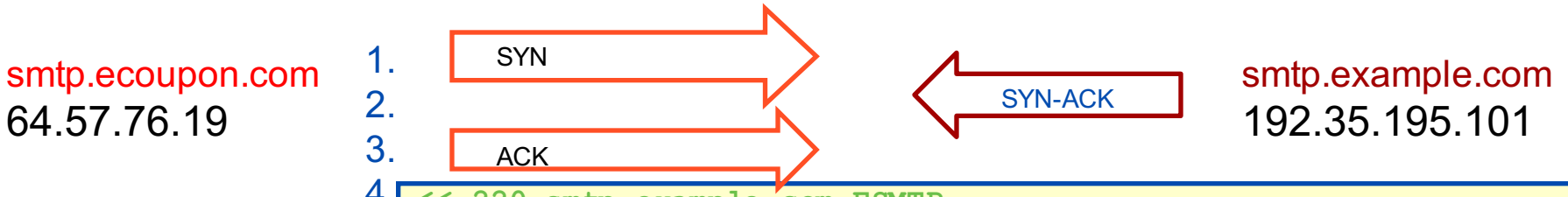


27

Как работает SMTP



Еще немного терминологии



Envelope

```
<< 220 smtp.example.com ESMTP
>> HELO mail.ecoupon.com
<< 250 smtp.example.com
>> MAIL FROM: <joe@ecoupon.com>
<< 250 sender <joe@ecoupon.com> ok
>> RCPT TO: <Sam@example.com>
<< 250 recipient <Sam@example.com> ok
```

Headers

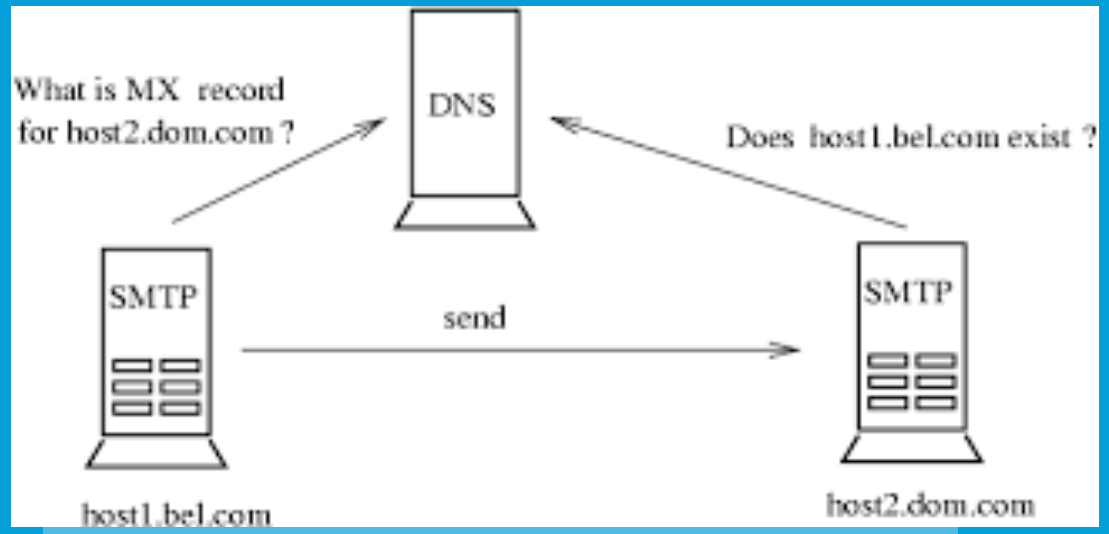
```
>> DATA
<< 354 go ahead
>> From: joe Dude <joe@ecoupon.com>
>> To: Sam Snakeskin <Sam@example.com>
>> Subject: Overslept Again! :-(
>> Date: Mon, 5 March 2008 20:57:13 -0700
>> X-SpamScore: 100
>>
```

Body

```
>> Sam!!
>> I screwed up my alarm again and I'm going to be late to
>> this morning's meeting.  Can you cover for me?
>> -joe
>> .
<< 250 ok
>> QUIT
<< 221 smtp.example.com
```

Простой сеанс SMTP связи

```
Connected to alln-mx-01.cisco.com.
Escape character is '^]'.
220 alln-inbound-a.cisco.com ESMTP
HELO dir.ua
250 alln-inbound-a.cisco.com
MAIL FROM:<prod@dir.ua>
250 sender <prod@dir.ua> ok
RCPT TO:<prodiono@cisco.com>
250 recipient <prodiono@cisco.com> ok
DATA
354 go ahead
Subject: The simplest email message
From: Pavel Rodionov <prod@dir.ua>
To: Pavel Rodionov (prodiono) <prodiono@cisco.com>

Just basic headers and a short body.
.
250 ok:  Message 5395042 accepted
QUIT
221 alln-inbound-a.cisco.com
Connection closed by foreign host.
```



Маршрутизация Email: DNS MX записи

Что такое MX записи?

- DNS RR определен в RFC5321
- Определяет **mailhost** – шлюз SMTP– для зоны (домен или FQDN)
- Также определяет **preference value** (“приоритет”)
  - Со шлюзами SMTP (**mail exchangers)** с самым низким “preference value” контакт устанавливается в первую очередь
  - Со шлюзами SMTP с одинаковым ”preference value” контакт устанавливается по очереди
- Обычно спамеры вначале пытаются отправить письмо через шлюз с более высоким “preference value” (низкий приоритет)
- DNS MX обеспечивают
  - Отказоустойчивость (разный приоритет)
  - (довольно неплохую) Балансировку (одинаковый приоритет)

MX примеры

```
$ host -t mx cisco.com
cisco.com mail is handled by 10 alln-mx-01.cisco.com.
cisco.com mail is handled by 20 rcdn-mx-01.cisco.com.
cisco.com mail is handled by 30 aer-mx-01.cisco.com.

$ host -t mx yahoo.com
yahoo.com mail is handled by 1 mta5.am0.yahoodns.net.
yahoo.com mail is handled by 1 mta7.am0.yahoodns.net.
yahoo.com mail is handled by 1 mta6.am0.yahoodns.net.

$ host -t mx rada.gov.ua
rada.gov.ua mail is handled by 10 webmail.rada.gov.ua.
```

Маршрутизация email на Cisco ESA: SMTP Routes

SMTP Routes

Success — SMTP Route for "issp.ua" was submitted.

SMTP Routes List — Items per page: 20

Add Route... | Clear All Routes | Import Routes...

Receiving Domain	Destination Hosts	All Delete
issp.ua	usedns	☐
pacifica.kz	10.148.254.250	☐
skibastards.org	10.148.154.251	☐
All Other Domains	*(not defined)*	

Export Routes... | Delete

Bounces: Управляющий протокол Email

Что такое Bounces?

- Отправитель уведомляет получателя о различных состояниях ошибок с помощью bounces
- Кратко, отправителю передаются численные коды ошибок (и, возможно, некоторый текст, который сопровождает эти ошибки)
- Действия по получению Bounces зависят от отправителя
- Спамботы обычно не понимают bounces
  - Простой путь обнаружения спамеров
  - Greylisting
- Bounce spam: редко но эффективно!
- Это звучит странно, но bounces никогда не должны отбрасываться/игнорироваться/сбрасываться

Bounces по серьезности

Soft Bounces

421 Please Try Again Later

- Временные ошибки
- Отправитель снова поместит сообщения в очередь и попытается еще раз
- Период по умолчанию: 4 часа

Hard Bounces

500 No Such User

- Постоянные ошибки
- Отправитель сбросит сообщение и уведомит пользователя по email

Bounces по источнику

Inline (в процессе общения) Bounces

```
220 alln-inbound-i.cisco.com ESMTP
EHLO dir.ua
250-alln-inbound-i.cisco.com
250-8BITMIME
250-SIZE 33554432
250 STARTTLS
MAIL FROM: provocateur@internet.org
250 sender <provocateur@internet.org> ok
RCPT TO: ren.zhengfei@huawei.com
550 #5.1.0 Address rejected.
```

Out-of-band (Отложенные) Bounces

```
MAIL FROM: <>
From: Mail Delivery Subsystem <MAILER-DAEMON@cisco.com>
To: <prodiono@cisco.com>
Subject: Returned mail: see transcript for details

The original message was received at Wed, 19 Nov 2014
08:42:04 -0600
from localhost.localdomain [127.0.0.1]

----The following addresses had permanent fatal errors ----
-
<asdfg@cisco.com>
    (reason: 550 5.1.1 <asdfg@cisco.com>... User unknown)

   ----- Transcript of session follows -----
... while talking to outbound.cisco.com.:
DATA
<<< 550 5.1.1 <asdfg@cisco.com>... User unknown
550 5.1.1 <asdfg@cisco.com>... User unknown
```


38

Примеры Bounces

```
To: <prodiono@cisco.com>
From: Mail Delivery System <MAILER-DAEMON@rcdn-iport-2.cisco.com>
Subject: Delivery Status Notification (Failure)

The following message to <mshademan@hr-communication.com> was undeliverable.

The reason for the problem:

5.4.7 - Delivery expired (message too old) 'timeout’
```

```
220 mx1.hc4-93.c3s2.smtpi.com ESMTP
EHLO linux.hr
250-mx1.hc4-93.c3s2.smtpi.com
250-8BITMIME
250-SIZE 10485760
250 STARTTLS
MAIL FROM: prod@linux.hr
250 sender <prod@linux.hr> ok
RCPT TO: prod@dir.ua
452 Too many recipients received this hour
```


39

Примеры Bounces

```
220 mx1.hc4-93.c3s2.smtpi.com ESMTP
ehlo bla
250-mx1.hc4-93.c3s2.smtpi.com
250-8BITMIME
250-SIZE 10485760
250 STARTTLS
mail from: spammer@spamspam.spam
250 sender <spammer@spamspam.spam> ok
RCPT TO: prod@dir.ua
550 #5.7.1 Your access to submit messages to
this e-mail system has been rejected.
```

```
To: <prodiono@cisco.com>
From: Mail Delivery System <MAILER-DAEMON@rcdn-iport-
6.cisco.com>
Subject: Delivery Status Notification (Failure)

The following message to
<Waleed_Al-
Basheer/Bahrain/GBM/NBR@d06ml300.portsmouth.uk.ibm.com>
was
undeliverable.
The reason for the problem:
5.1.2 - Bad destination host 'DNS Hard Error looking up
d06ml300.portsmouth.uk.ibm.com (MX): NXDomain'
```

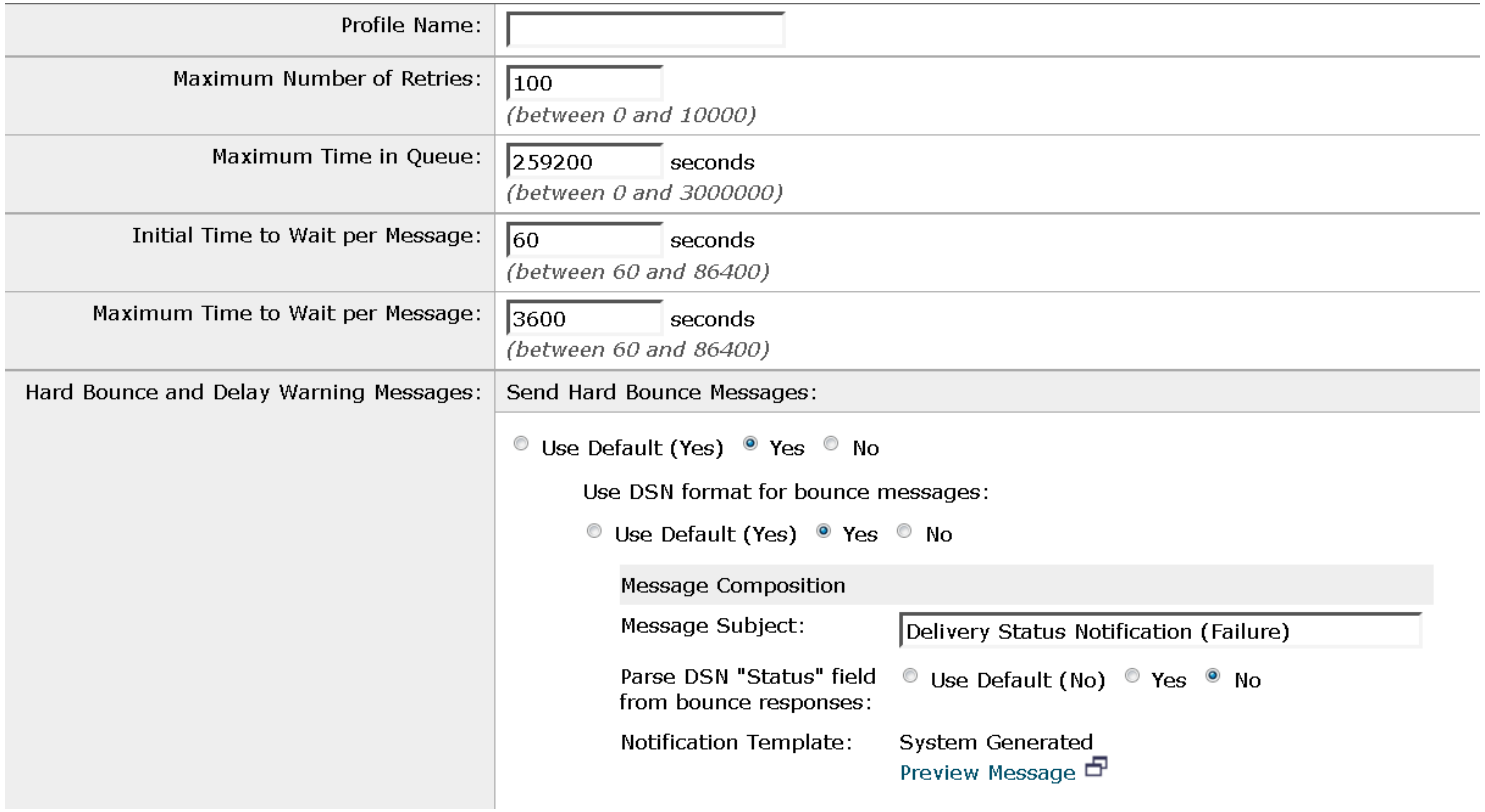

40

Опасность Bounces

- Bounce сообщения могут использоваться для доставки Spam
- Не попадайтесь на фишинговые bounce сообщения – это механизм уведомления, они почти никогда не просят вас что-то предпринять!
- Spambots вызывает bounce спам с перенаправленными bounces
- Backscatter атака – наиболее выгодный Email DDoS
  1. Наймите botnet
  2. Подделайте миллионы сообщений на несуществующих получателей и поставьте обраный адрес вашей цели DDoS
  3. Пронаблюдайте, как их почтовая система упадет под потоком Bounce сообщений.
- Эффективные контрмеры – SPF, DMARC и BATV (все поддерживаются Cisco Email Security)

41

Cisco Email Security: профили Bounces



- Профиль по умолчанию будет пытаться доставить сообщение 3 дня
- Вы можете создать дополнительные профили и назначить их на каждый домен!

42

Cisco Email Security: Bounce Verification

Bounce Verification

Success — New current key added.

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled

Edit Settings

Bounce Verification Address Tagging Keys

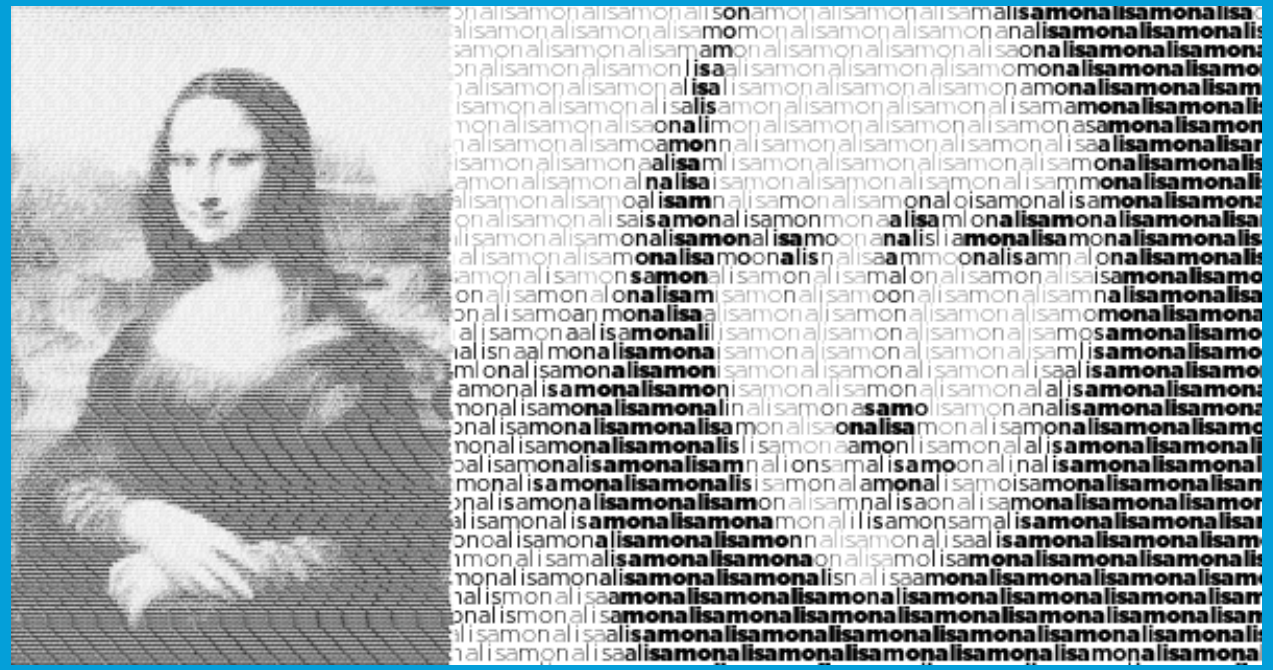
New Key... Clear All Keys

Address Tagging Keys	Status
123456	Current *(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)*

Purge Keys Not used in one month

Key: Current | Previously used

43

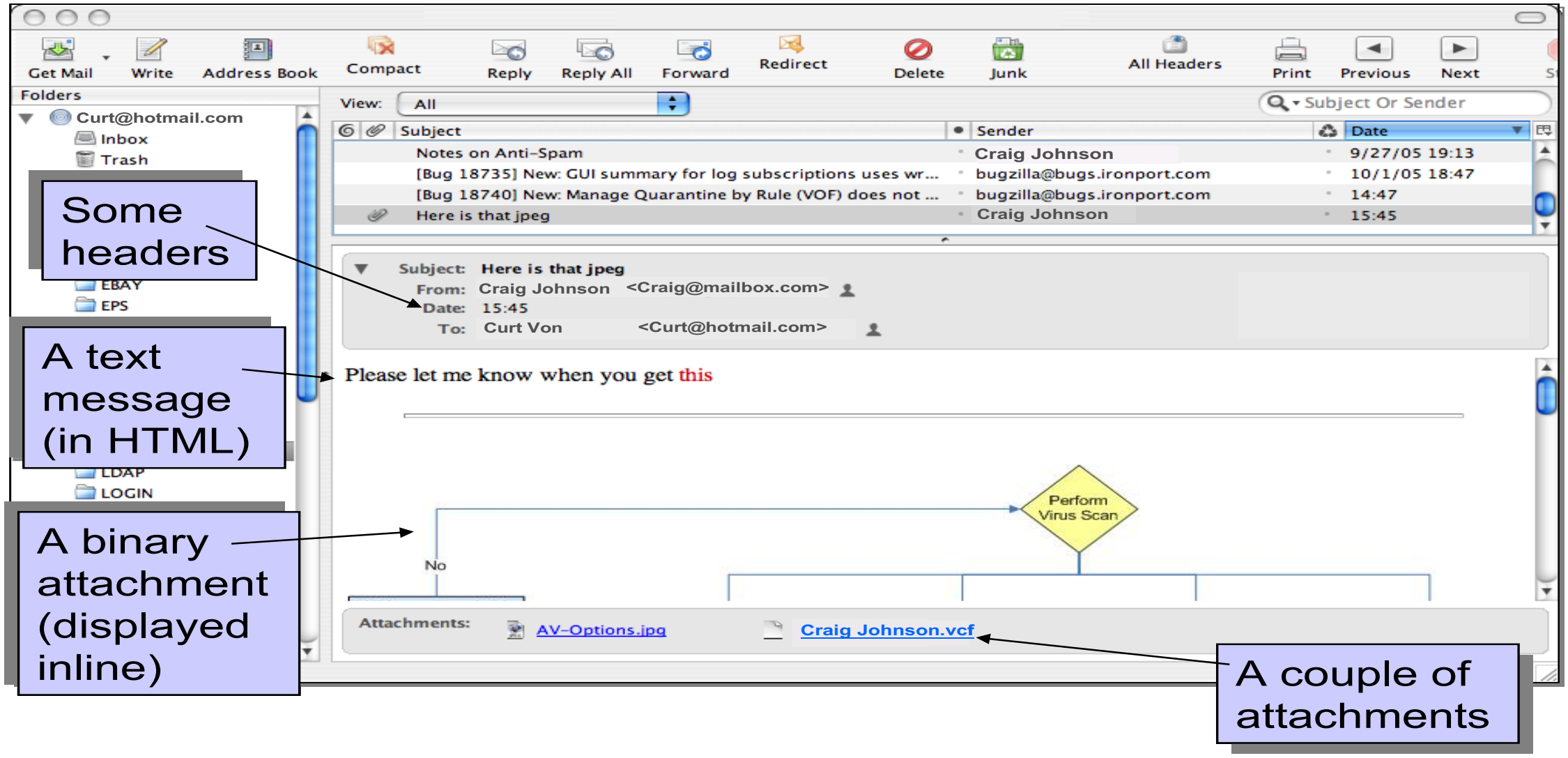


MIME: Отправка любого контента через 7-бит ASCII

Что такое MIME?

- Multipurpose Internet Mail Extensions, определен в RFC2045-2049
- Метод кодирования любого контента, чтобы передать его через 7-бит SMTP
- Дальнейшее развитие добавило поддержку определенного контента для зашифрованных и подписанных данных
- Позже он начал широко использоваться в других технологиях: HTTP, FTP, общая кодировка данных (mime типы)

Анатомия почтового сообщения



46

Анатомия почтового сообщения (2)

```
From: Craig Johnson<Craig@mailbox.com>
Subject: Here is that jpeg
To: Curt Von <curt@hotmail.com>
MIME-version: 1.0
Content-type: multipart/mixed; boundary="Boundary_11111"

This is a multi-part message in MIME format.

--Boundary_11111
Content-type: multipart/alternative;
 boundary="Boundary_22222"

  --Boundary_22222
  Content-type: text/plain; format=flowed; charset=us-ascii
  Content-transfer-encoding: 7bit

  Please let me know when you get this!

  --Boundary_22222
  Content-type: text/html; charset=us-ascii
  Content-transfer-encoding: 7bit

  <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
  <html>
  ...
  </html>

  --Boundary_22222--

--Boundary_11111
```

MIME multipart/mixed + Boundary_11111

Преамбула

MIME multipart/alternative + Boundary_22222

Alternative Text Part

Alternative HTML Part

Closing multipart/alternative (Boundary_22222)

Next container boundary

Анатомия почтового сообщения

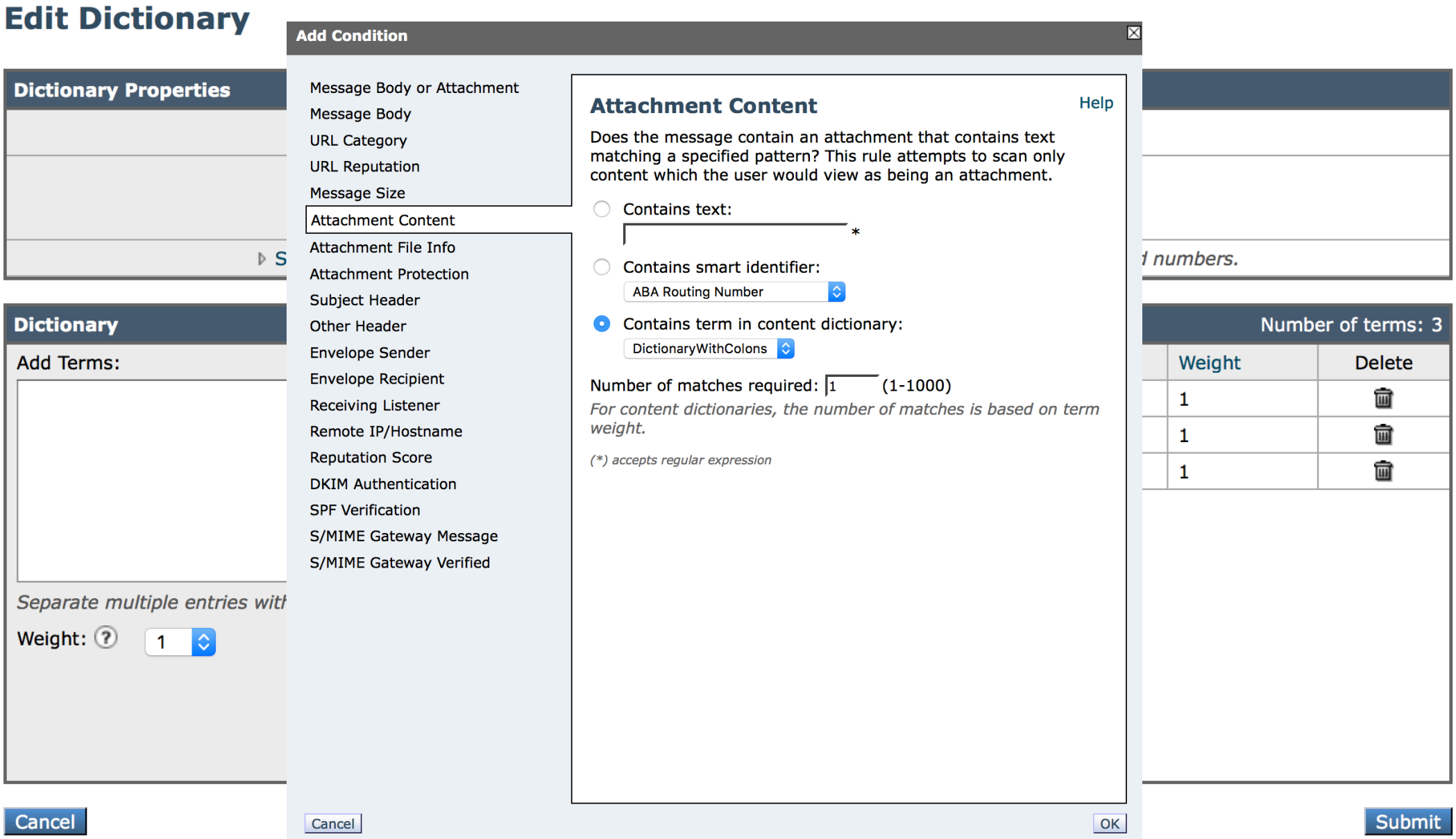
```
Content-type: image/jpeg; name=AV-Options.jpg
Content-transfer-encoding: base64
Content-disposition: inline;
 filename=Antivirus-Options.jpg

/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRof
KACiiigAooooAKKKKACiiigAooooAKKKKACiiigD/9k=

--Boundary_11111
Content-type: text/plain; CHARSET=us-ascii; name="Craig Johnson.vcf"
Content-transfer-encoding: 7bit
Content-disposition: inline; filename="Craig Johnson.vcf"

BEGIN:VCARD
VERSION:3.0
N:Johnson;Craig;;;
...
END:VCARD

--Boundary_11111--
```

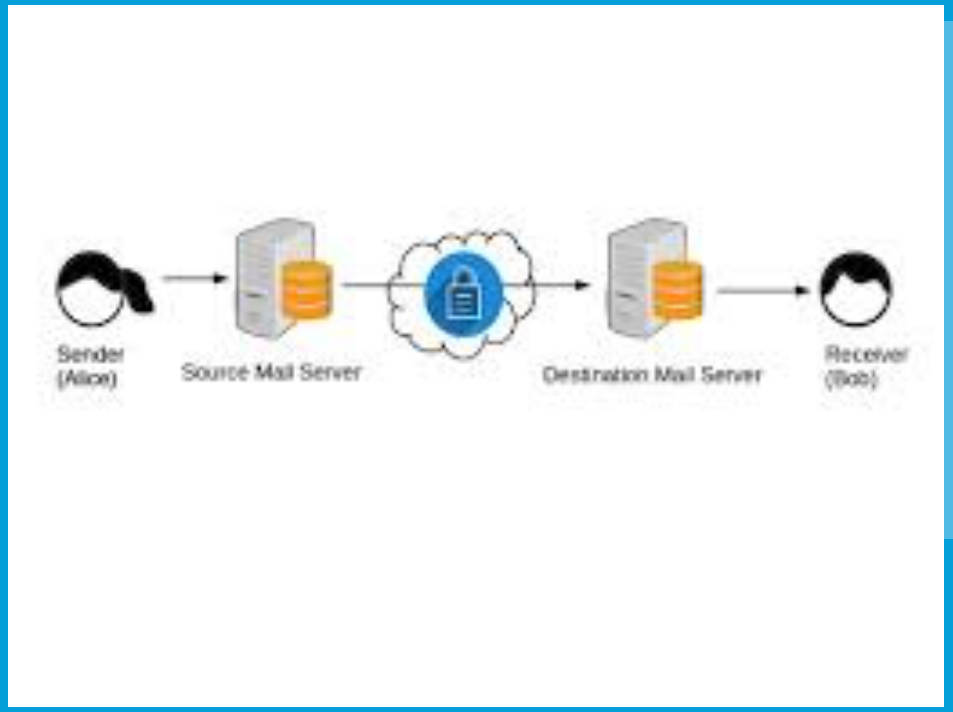
Изображение в письмое

Присоединенный Text/plain vcard

Закрытие

Cisco ESA: Обработка тела письма





Добавленные функции безопасности SMTP

ESMTP

- Базовый “Простой протокол передачи почтовых сообщений» стал быстро стал слишком простым!
- ESMTP позволяет определить расширения базового сервиса
- Наболее часто используемые расширения SMTP:

AUTH

STARTTLS

8BITMIME

SIZE

Что такое STARTTLS?

- SMTP расширение, определенное в RFC3207
- Сервер сообщает о поддержке TLS с помощью уведомления “STARTTLS” в ответе на EHLO
- Клиент инициирует TLS с помощью простой команды без аргументов: STARTTLS
- Почтовый шлюз НЕ ДОЛЖЕН требовать использовать STARTTLS
- Если требуется TLS, используйте порт 587/TCP (“mail submission”)

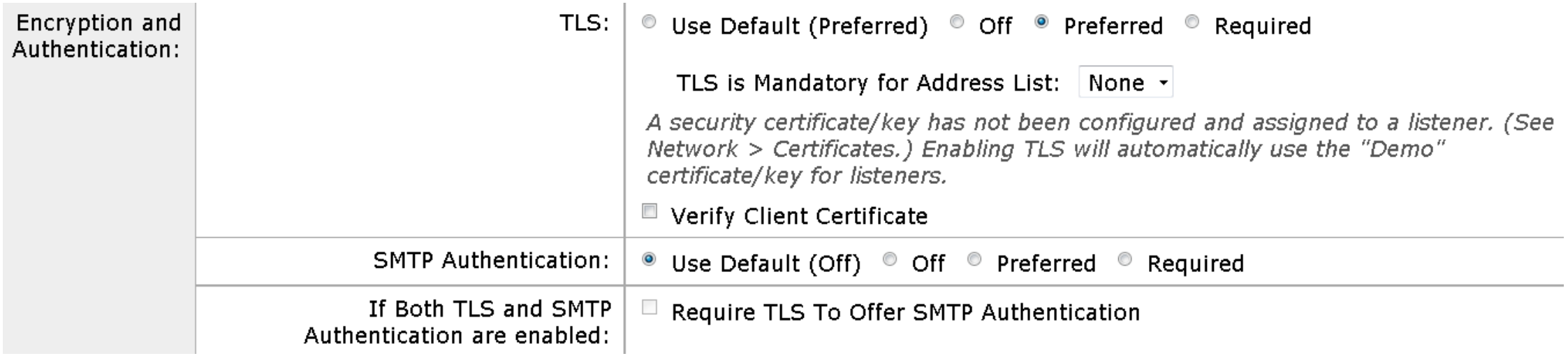
SMTP общение и STARTTLS

```
$ gnutls-cli -s -p 25 --crlf –insecure mx1.hc4-93.c3s2.smtpi.com

220 mx1.hc4-93.c3s2.smtpi.com  ESMTP
EHLO dir.ua
250-mx1.hc4-93.c3s2.smtpi.com
250-8BITMIME
250-SIZE 104857600
250 STARTTLS
STARTTLS
220 Go ahead with TLS
*** Starting TLS handshake
- Ephemeral Diffie-Hellman parameters
[…]
- Key Exchange: DHE-RSA
- Cipher: AES-128-CBC
- MAC: SHA1
- Compression: NULL
MAIL FROM: prod@dir.ua
250 sender <prod@dir.ua> ok
RCPT TO: prod@dir.ua
250 recipient <prod@dir.ua> ok
QUIT
221 mx1.hc4-93.c3s2.smtpi.com
- Peer has closed the GnuTLS connection
```


53

Cisco Email Security: установки TLS

- TLS настройки для входящей и исходящей почты выключены по умолчанию
- Три уровня безопасности, по умолчанию предпочтительный
- Обязательный устанавливается для каждой группы, домена или списка адресов



54

Что такое SMTP AUTH?

- SMTP расширение, определенное в RFC4954
- Сервер показывает поддержку аутентификации с помощью уведомления “AUTH” в ответе на EHLO, после чего уведомляет о поддерживаемых методах аутентификации.
- Клиент аутентифицируется с помощью команды AUTH и выбранного метода
- По умолчанию транзации аутентификации SMTP **не зашифрованы**
  - Но большинство SMTP серверов требуют, чтобы перед командой AUTH были согласованы параметры TLS
- Расширение SMTP AUTH аутентифицирует **соединение,** а не сообщения!
- **Рекомендация: используйте VPN для подключения к внутренней почтовой системе (в случае Exchange можно дополнительно использовать OWA)**
  - Если это по каким-то причинам невозможно, откройте для аутентификации порт 587/TCP на Email Appliance

SMTP соединение и SMTP AUTH

```
220 mx1.hc4-93.c3s2.smtpi.com ESMTP
EHLO dir.ua
250-mx1.hc4-93.c3s2.smtpi.com
250-8BITMIME
250-SIZE 104857600
250-AUTH PLAIN LOGIN
250 AUTH=PLAIN LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
aGRvZ2FuCg==
334 UGFzc3dvcmQ6
cGFzdm9yZGNpbmEK
235 2.7.0 Authentication successful
```

BASE64 encoded: “Username:”

BASE64 encoded: “prod”

BASE64 encoded: “Password:”

Nope…

56

Что такое фишинг?

phish·ing *noun* \ˈfi-shiŋ\

мошенничество, при котором пользователя email вводят в заблуждение, что позволяет нелегально использовать его персональную или конфиденциальную информацию.

Merriam-Webster Online Dictionary

Краткая история фишинга

- Первое использование: 1996, alt.online-service.america-online
- 2001

  Переместился в Internet, нацелен на платежные системы

  Легко обнаружить, ошибки в сообщениях…
- 2003

  На заднем плане открыт легитимный сайт, а на переднем – поддельное окно ввода информации.

  Gartner сообщает о глобальных потерях от фишинга на уровне 2.4 млрд US$.
- 2004

  Внедрение проверки данных на реальных сайтах

  Создание полностью нелегальных сайтов или воображаемых банков и финансовых фирм.

Напоминание о терминологии

smtp.ecoupon.com
64.57.76.19

1. SYN
2. SYN-ACK
3. ACK
4.

smtp.example.com
192.35.195.101

Envelope

```
<< 220 smtp.example.com ESMTP
>> HELO mail.ecoupon.com
<< 250 smtp.example.com
>> MAIL FROM: <joe@ecoupon.com>
<< 250 sender <joe@ecoupon.com> ok
>> RCPT TO: <Sam@example.com>
<< 250 recipient <Sam@example.com> ok
```

Headers

```
>> DATA
<< 354 go ahead
>> From: joe Dude <joe@ecoupon.com>
>> To: Sam Snakeskin <Sam@example.com>
>> Subject: Overslept Again! :-(
>> Date: Mon, 5 March 2008 20:57:13 -0700
>> X-SpamScore: 100
>>
```

Body

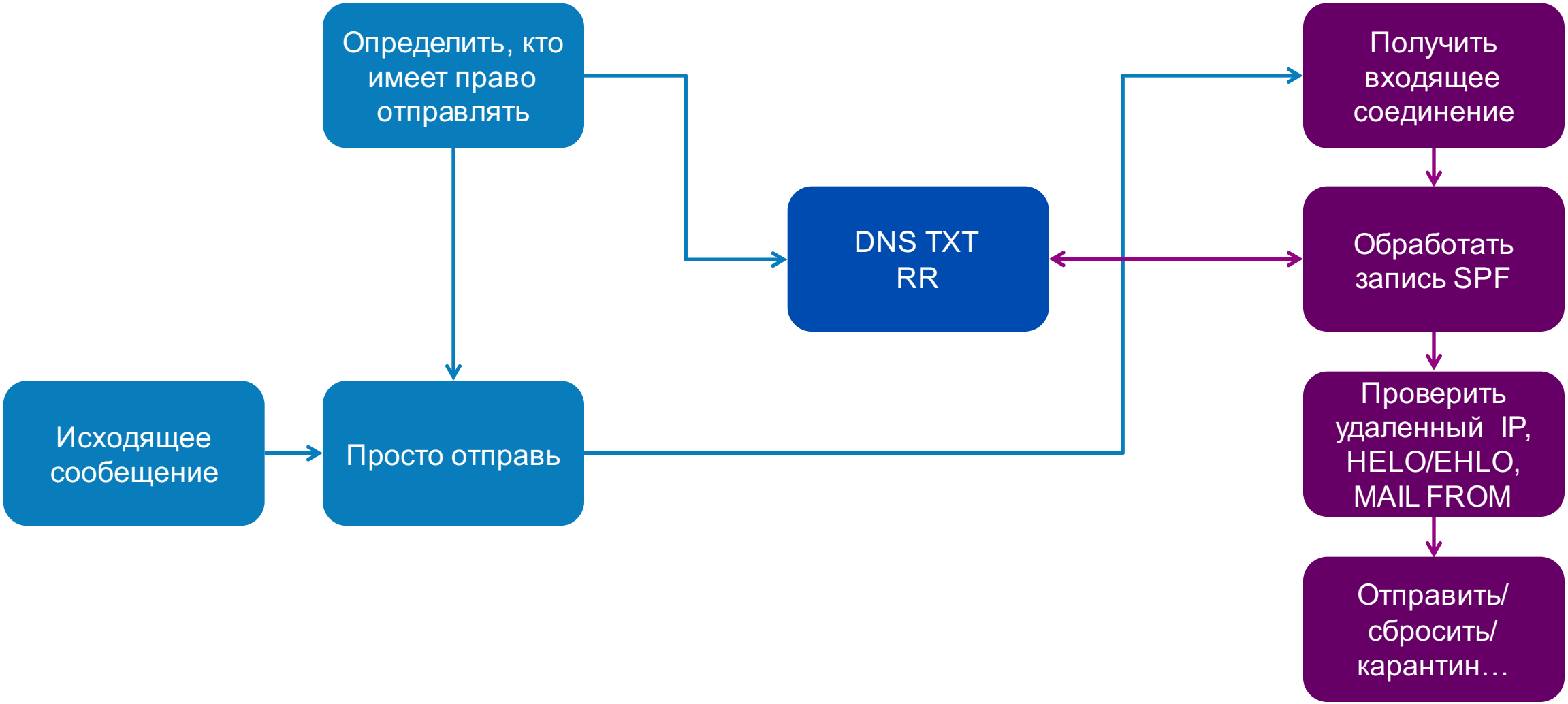
```
>> Sam!!
>> I screwed up my alarm again and I'm going to be late to
>> this morning's meeting.  Can you cover for me?
>> -joe
>> .
<< 250 ok
>> QUIT
<< 221 smtp.example.com
```

Защита инфраструктуру email: SPF

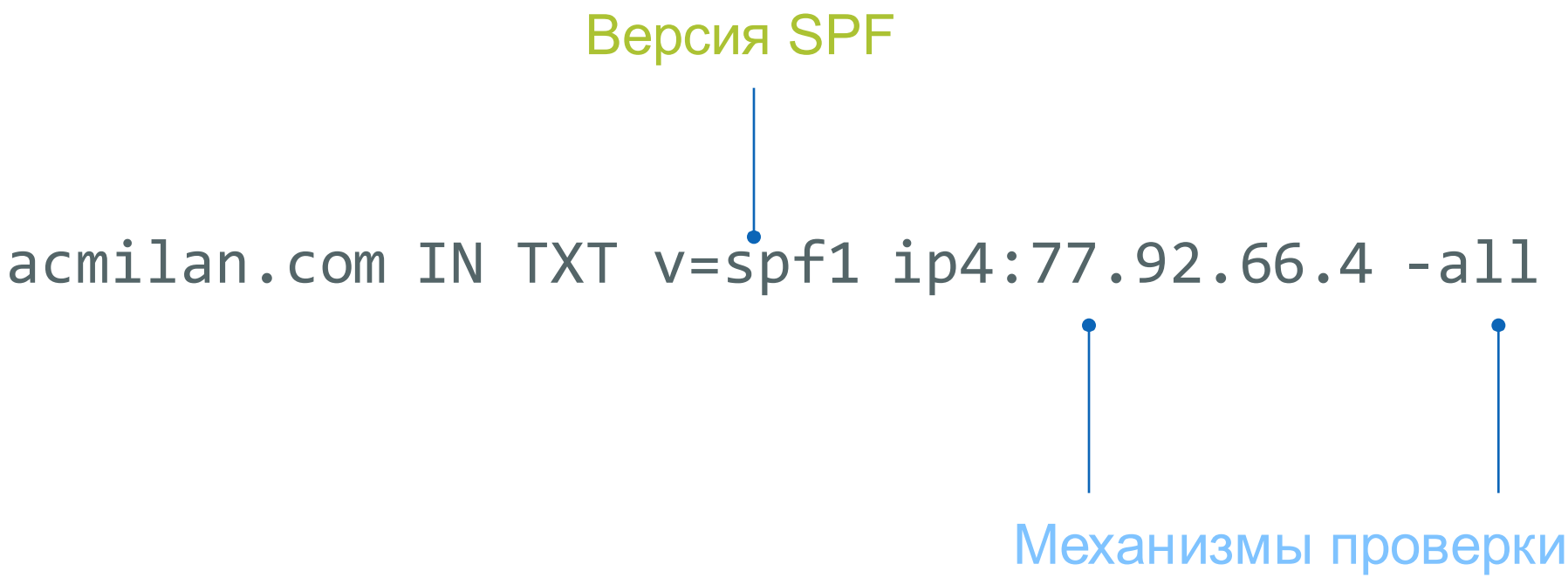
Sender Policy Framework
Краткие сведения

- Определен в RFC7208, заменил RFC4408(bis) в апреле 2014
- В двух словах: Позволяет получателям проверять IP адрес отправителя с помощью просмотра списка авторизованных шлюзов Email для определенного домена в DNS записях
- Использует записи DNS TXT(16) (раньше могла использоваться запись SPF (тип 99)
  - SPF RR была отменена в RFC7208 из-за неиспользования и возможного непонимания
- Может проверять SMTP HELO и MAIL FROM (FQDN)

Работа SPF

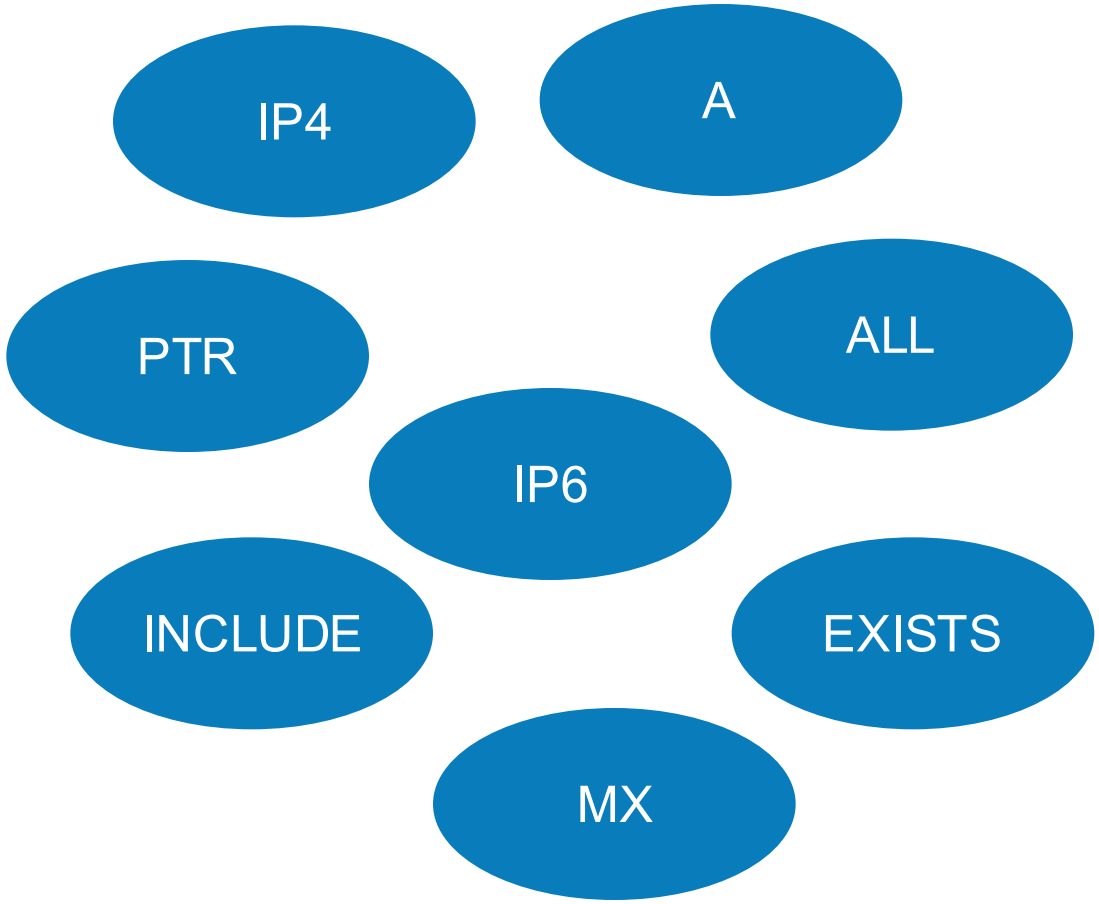


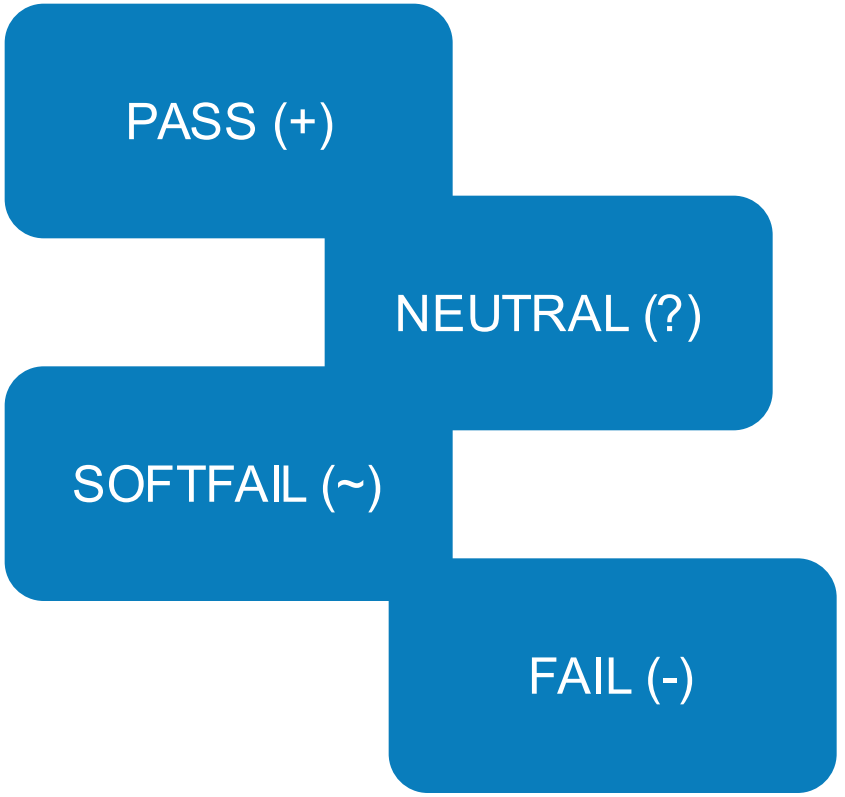
Семантика SPF записи



Семантика SPF записи

- Механизмы и квалификаторы





Примеры записей SPF

```
cisco.com IN TXT “v=spf1 ip4:173.37.147.224/27 ip4:173.37.142.64/26
ip4:173.38.212.128/27 ip4:173.38.203.0/24 ip4:64.100.0.0/14 ip4:72.163.7.160/27
ip4:72.163.197.0/24 ip4:144.254.0.0/16 ip4:66.187.208.0/20 ip4:173.37.86.0/24" "
ip4:64.104.206.0/24 ip4:64.104.15.96/27 ip4:64.102.19.192/26
ip4:144.254.15.96/27 ip4:173.36.137.128/26 ip4:173.36.130.0/24 mx:res.cisco.com
~all”

amazon.com IN TXT “v=spf1 include:spf1.amazon.com include:spf2.amazon.com
include:amazonses.com –all”

amazon.ses.com IN TXT “v=spf1 ip4:199.255.192.0/22 ip4:199.127.232.0/22
ip4:54.240.0.0/18 ~all”

openspf.org IN TXT “v=spf1 –all”
```

starlightmedia.tv. IN TXT "v=spf1 mx ~all"

npu.gov.ua. IN TXT "v=spf1 +mx -all”

rada.gov.ua. IN TXT

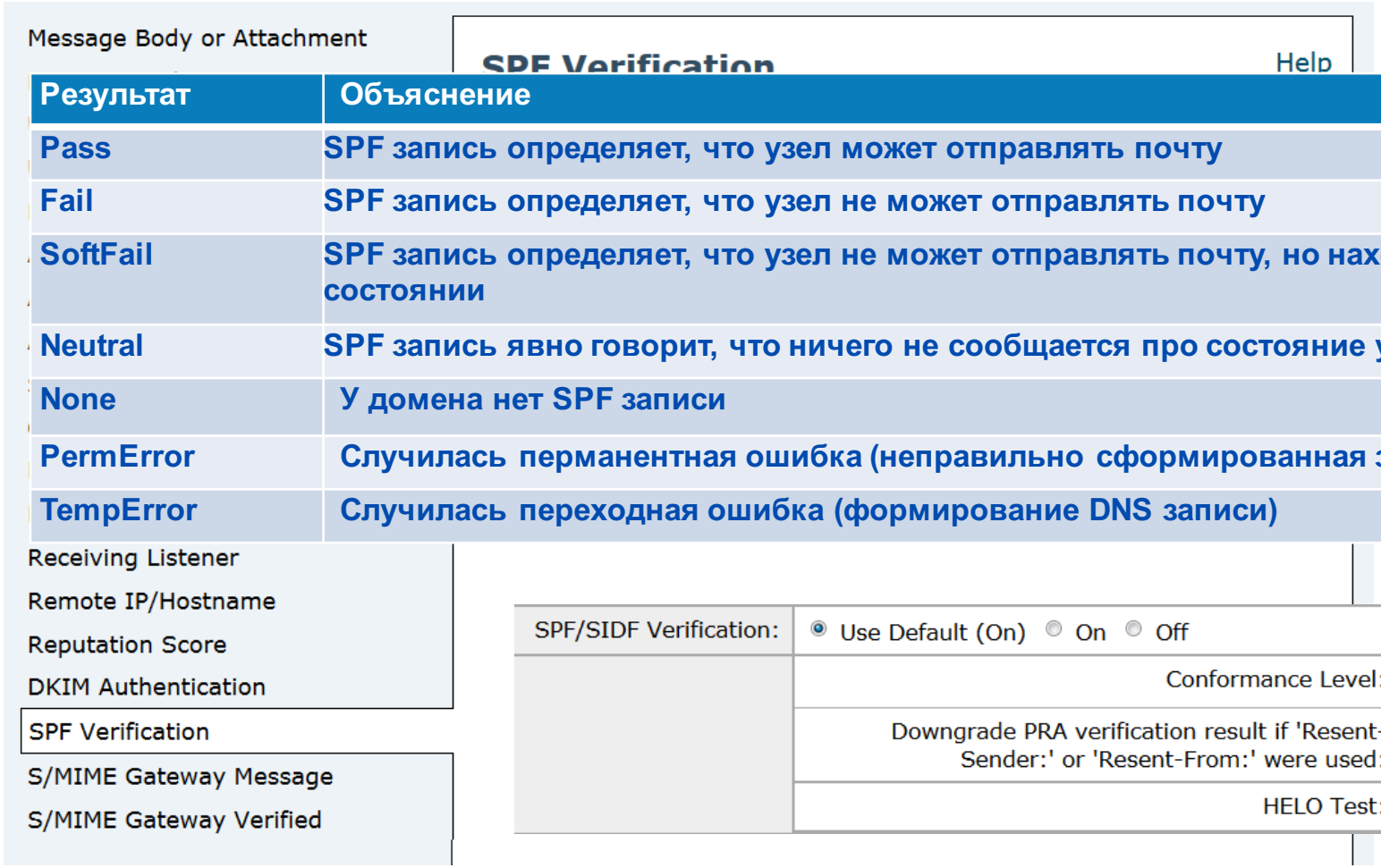
president.gov.ua. IN TXT

Что не делает SPF

- Основная цель SPF – это проверить, пришло ли сообщение от легитимного узла.
- Проверяет только конверт – заголовки еще можно подделать!

  Дополняющая технология, SenderID, проверяет возможного отправителя (“Purported Responsible Address”) в заголовках, но имеет много недостатков
- Не гарантирует целостность сообщения
- Не предотвращает междоменной подделки

SPF на ESA



- Когда включен SPF, ESA штампует заголовки сообщения

Результат	Объяснение	Действие
Pass	SPF запись определяет, что узел может отправлять почту	accept
Fail	SPF запись определяет, что узел не может отправлять почту	reject
SoftFail	SPF запись определяет, что узел не может отправлять почту, но находится в переходном состоянии	accept but mark
Neutral	SPF запись явно говорит, что ничего не сообщается про состояние узла	accept
None	У домена нет SPF записи	accept
PermError	Случилась перманентная ошибка (неправильно сформированная запись SPF	unspecified
TempError	Случилась переходная ошибка (формирование DNS записи)	accept or reject

Лучшие практики SPF

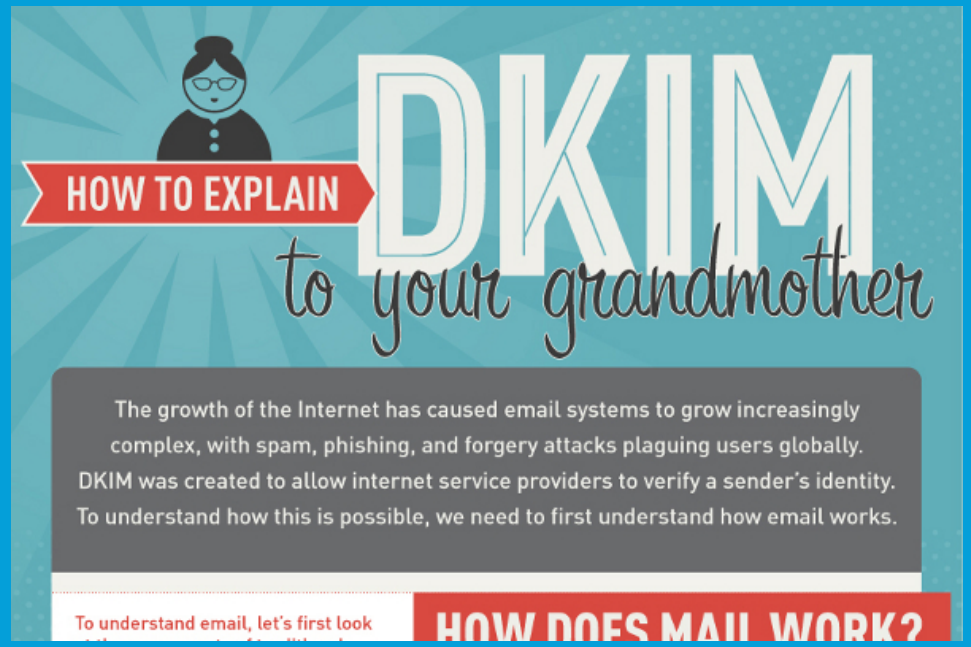
- Включайте в ваши записи “`-all`”
- Пересмотрите все легитимные сервера, которые отправляют почту от вашего имени

  Мигрирующие пользователи должны использовать или SMTP authentication, или VPN для отправки email. VPN предпочтительнее с точки зрения безопасности и правильного дизайна.
- Добавьте HELO/EHLO идентификацию ваших relay узлов в записи SPF
- Не забудьте добавить SPF записи для ваших поддоменов

  Для всех ваших доменов/поддоменов, которые не отправляют почту, публикуйте нулевые SPF записи

```
nomail.domain.com.      IN  TXT  "v=spf1 -all"
```

- MX механизм включайте только для тех **входящих** серверов, которые действительно отправляют **исходящую** почту.



Защита инфраструктуры email: DKIM

Domain Keys Identified Mail

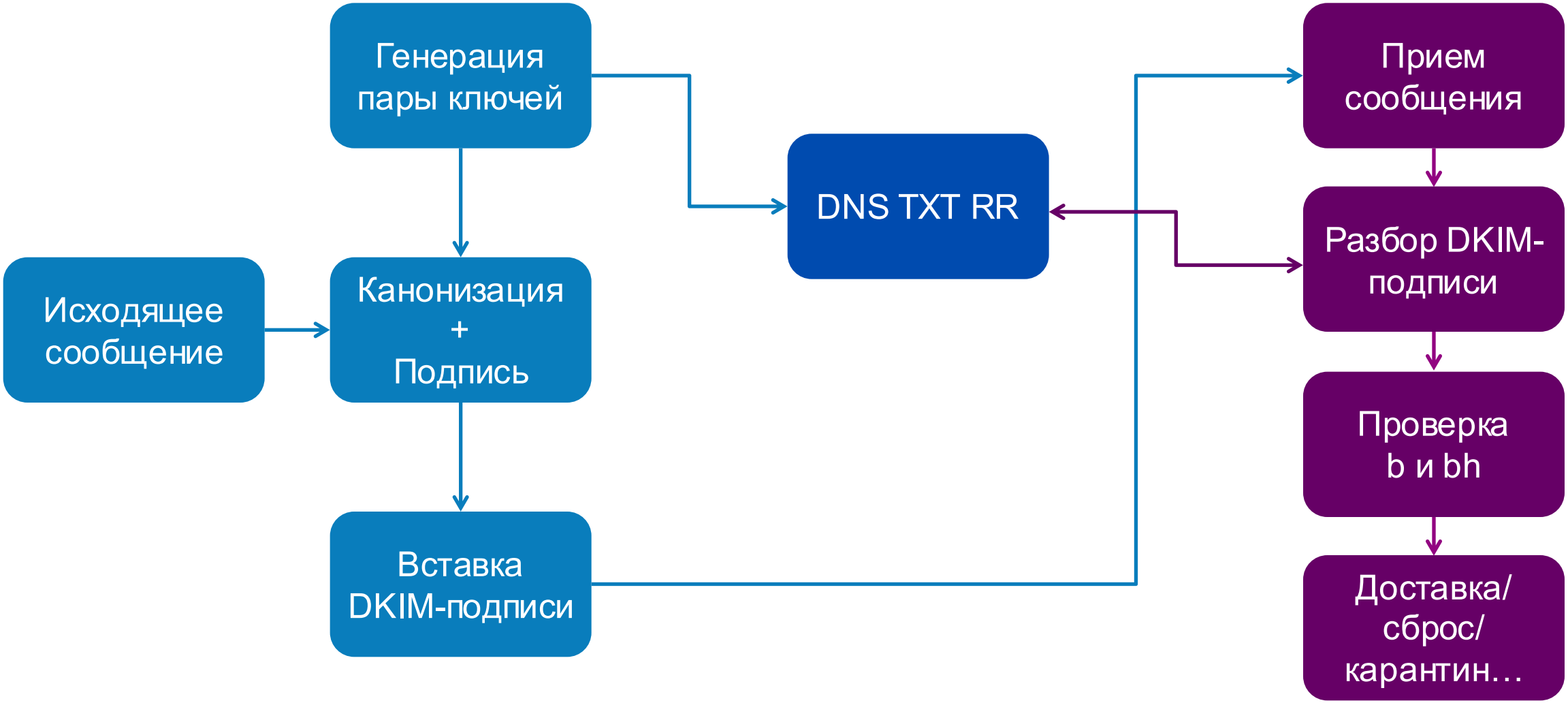
- Определено в RFC5585

  Дополнительные RFCs: RFC6376 (DKIM подписи), RFC5863 (DKIM развитие, развертывание и работа), RFC5617 (Author Domain Signing Practices (ADSP))

- В двух словах: определяет метод криптографической подписи исходящих сообщений на шлюзе, включая проверочные данные в заголовок письма и пути для получателей для проверки целостности сообщений

- Использует записи DNS TXT для публикации публичных ключей

Работа DKIM



71

DKIM подпись

Алгоритмы

Схема канонизации

Идентификатор домена

Селектор

Подписанные заголовки

Хеш заголовков

Хеш тела

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:date:message-id:subject:from:to:content-type;
        bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+ADlVSR6I0zrYofA=;
        b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLh
        srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B
        JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh
        Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq
        ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ
        SyGhUFeuqwxJoCJcghGf7edZ0OIgZtEcuxLMcgl+mpSje2YIfeXgFRg==
```

Извлечение публичного ключа DKIM

- DNS запрос:

<selector>._domainkey.<SDID>

- например:

```
20120113._domainkey.gmail.com IN TXT “k=rsa\;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabg
bFwh+eBCsSTrqmwIYYvywlbhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyo
xcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD0" "7y2+07wlNWwIt
8svnxgdxGkVbbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIh
kx4xYSIc9oSwVmAl5OctMEeWUwg8IstjqZ8BZeTWbf41fbNhte7Y+YqZOwq1S
d0DbvYAD9NOZK9vlfuac0598HY+vtSBczUiKERHv1yRbcaQtZFh5wtiRrN04B
LUTD21MycBX5jYchHjPY/wIDAQAB”
```

Проблема с сообщениями DKIM и ADSP

- Самая большая проблема, связанныя с DKIM, это отсутствие прямого уведомления.
  - Неподписанные сообщения могут прийти непроверенные
- ADSP (Author Domain Signing Practices, RFC5617) – это расширение к DKIM
  - DNS-метод для доменов отправителей для уведомления, что они подписывают сообщения
  - Простая запись в DNS типа ”_adsp._domainkey.<domain>”, которая содержить только `dkim=unknown|all|discardable`
- В ноябре 2013 использование ADSP официально прекращено из-за отсутствие развертывания

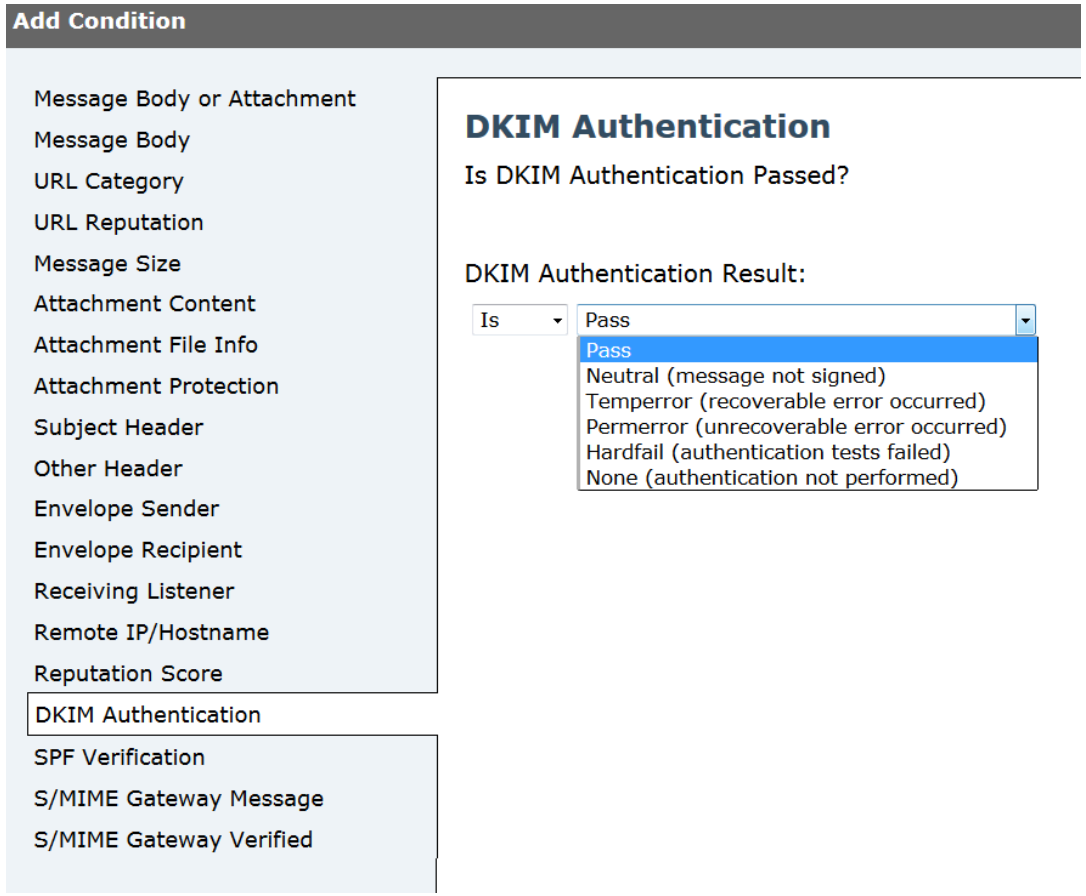
```
_adsp._domainkey.yahoo.com IN TXT “dkim=unknown”
```

DKIM на ESA

- DKIM настройки на ESA

Domain Key/DKIM Signing:	Use Default (Off) On Off
DKIM Verification:	Use Default (Off) On Off
	Use DKIM Verification Profile:

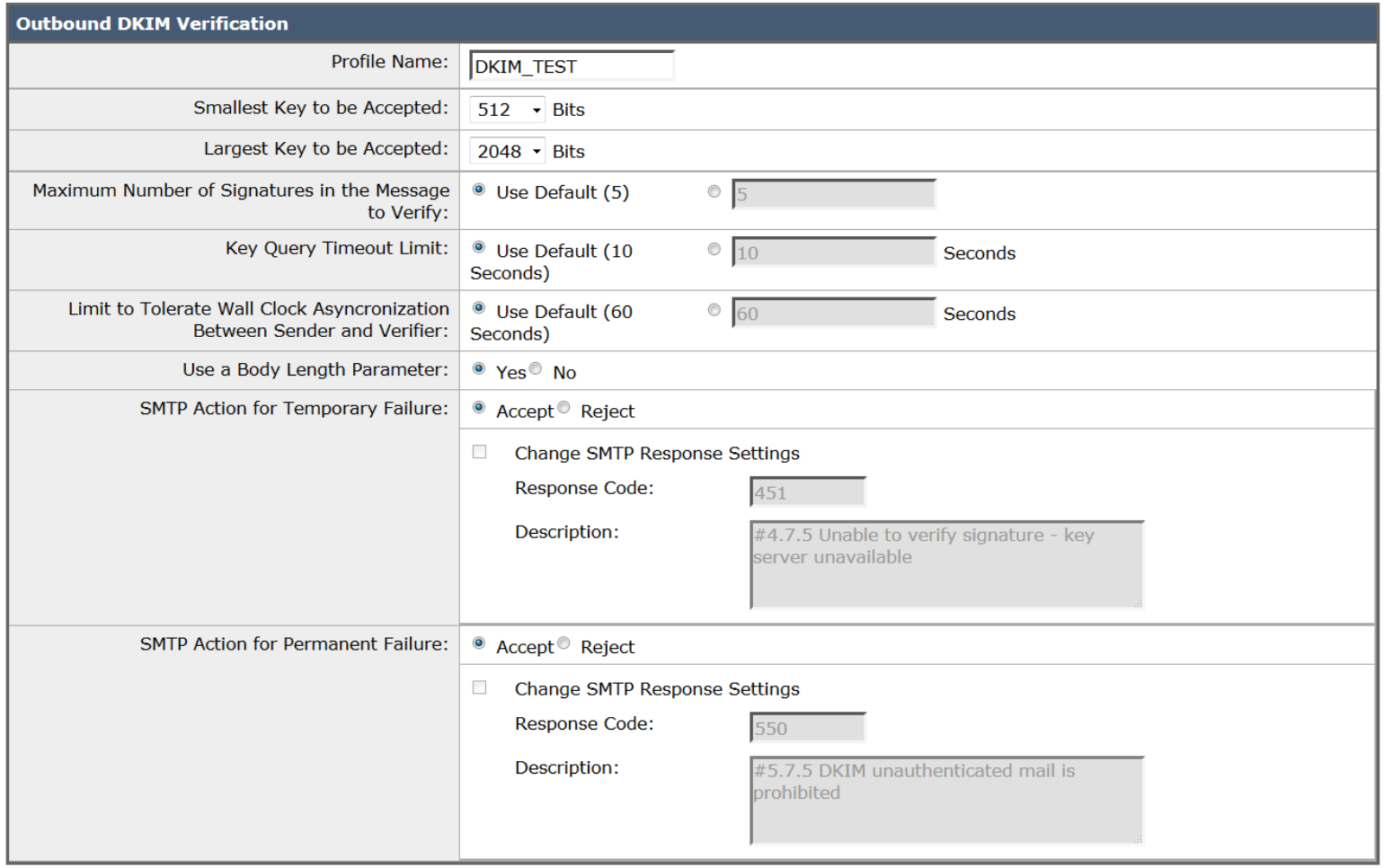
- Используйте фильтр контента для применения политик на основе результатов проверки
- Отправляйте сообщения в карантин для проверки подделок



75

Исходящий DKIM. Подпись сообщений

- Настройки подписи DKIM сообщений

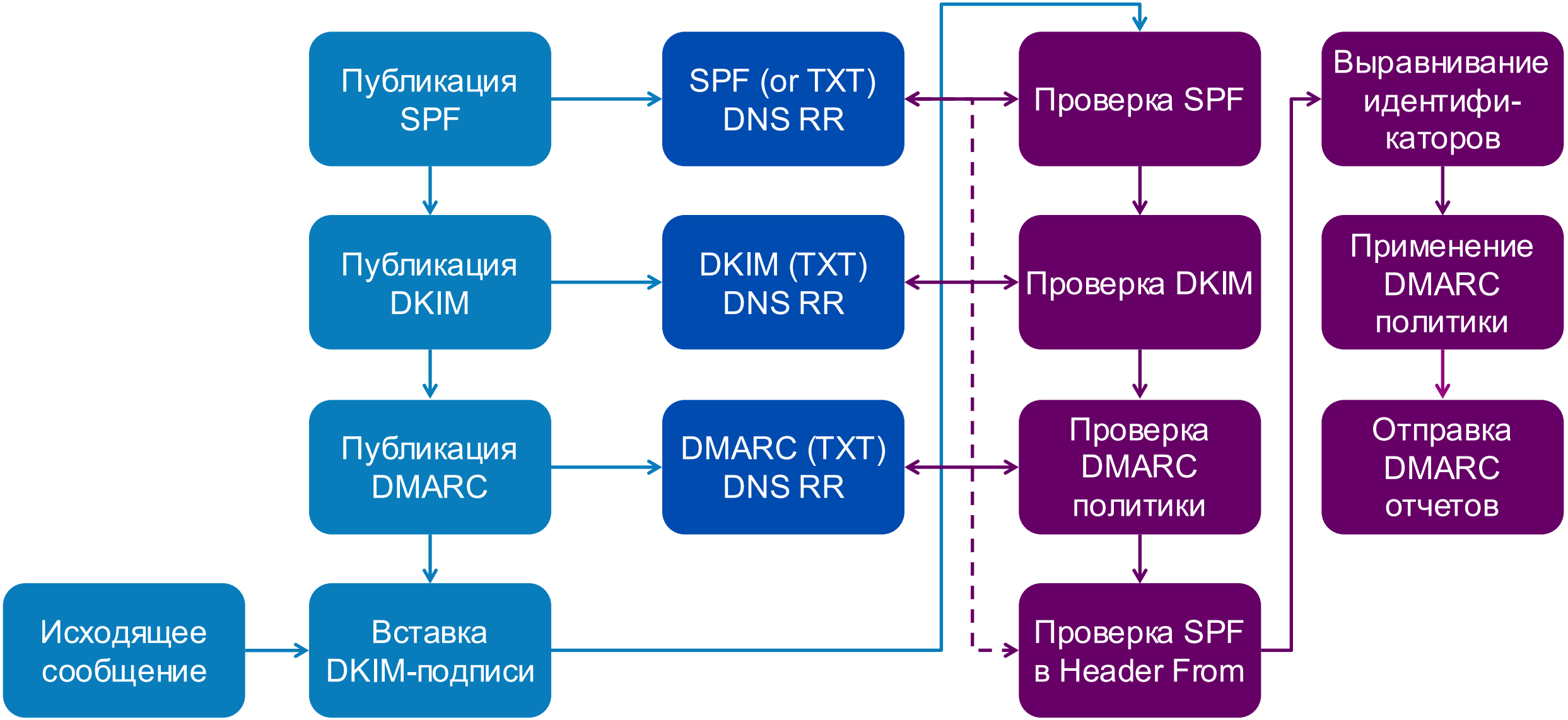


Защита инфраструктуры email: DMARC

Как появился DMARC

- Как DKIM, так и SPF, имеют свои недостатки. Не из-за плохого дизайна, а из-за различной природы каждой из технологий.
- Уведомление о DKIM политиках решается с помощью ADSP, но:
  - Нет возможности увидеть, что ваш домен пытаются подделать
  - Даже если получатель внедряет как SPF, так и DKIM, требований к синхронизации этих технологий нет.
    - Умный атакующий может это использовать для того, чтобы протолкнуть нелегитимные сообщения
- SPF проверяет подлинность HELO/MAILFROM, но не гарантирует проверку или тождественность с Header From
- Таким образом появился DMARC:
  - Использование хороших существующих технологий, предоставление инструментов для их синхронизации и предоставление **отправителям** возможности управлять политиками приема и отброса почты и получение обзора подозрительного трафика!

Работа DMARC



79

DMARC политики

Примеры записей DMARC

```
_dmarc.google.com IN TXT “v=DMARC1\; p=quarantine\; rua=mailto:mailauth-reports@google.com”

_dmarc.cs.helsinki.fi IN TXT “v=DMARC1\; p=reject\; sp=reject\; pct=100\; aspf=r\; rua=mailto:dmarc-reports@cs.helsinki.fi”

_dmarc.microsoft.com IN TXT “v=DMARC1\; p=none\; pct=100\; rua=mailto:d@rua.agari.com\; ruf=mailto:d@ruf.agari.com\; fo=1”

_dmarc.dk-hostmaster.dk IN TXT “v=DMARC1\; p=none\; rua=mailto:dmarc-report@dk-hostmaster.dk\; ruf=mailto:dmarc-report@dk-hostmaster.dk\; adkim=r\; aspf=r\; rf=afrf”
```

Выравнивание идентификаторов DMARC

- DMARC аутентифицирует домен из Header From
- DKIM аутентифицирует домент из DKIM-подписи (“d” тег)
- SPF аутентифицирует домены из MAIL FROM или HELO
- **Выравнивание идентификатора,** это концепция соответствия между Header From и идентификаторов, проверенных DKIM и SPF
- Сообщение **проходит** проверку DMARC, если **один или больше** механизмов аутентификации (DKIM **и/или** SPF) прошел проверку с **правильным выравниванием**

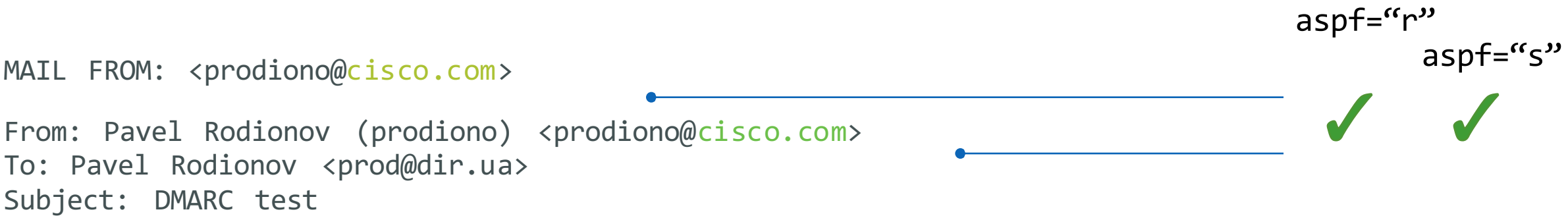
Выравнивание DMARC идентификатора: SPF

```
MAIL FROM: <prodiono@cisco.com>

From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

Выравнивание DMARC идентификатора: SPF

```
MAIL FROM: <prodiono@cisco.com>

From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

Выравнивание DMARC идентификатора: SPF



Выравнивание DMARC идентификатора: SPF

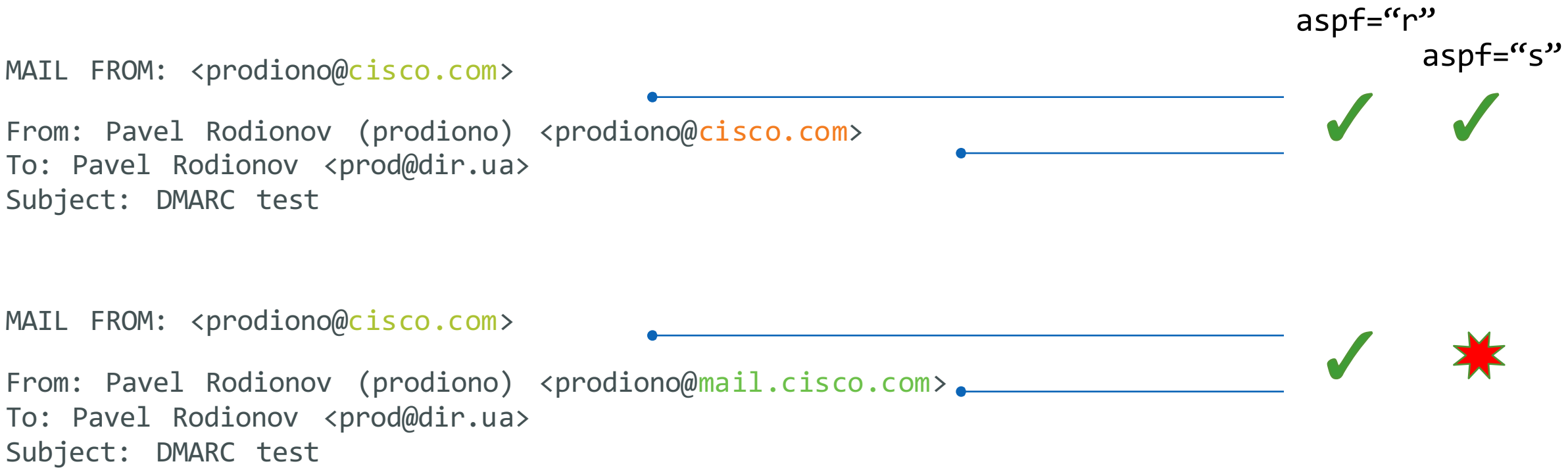
aspf="r"

aspf="s"

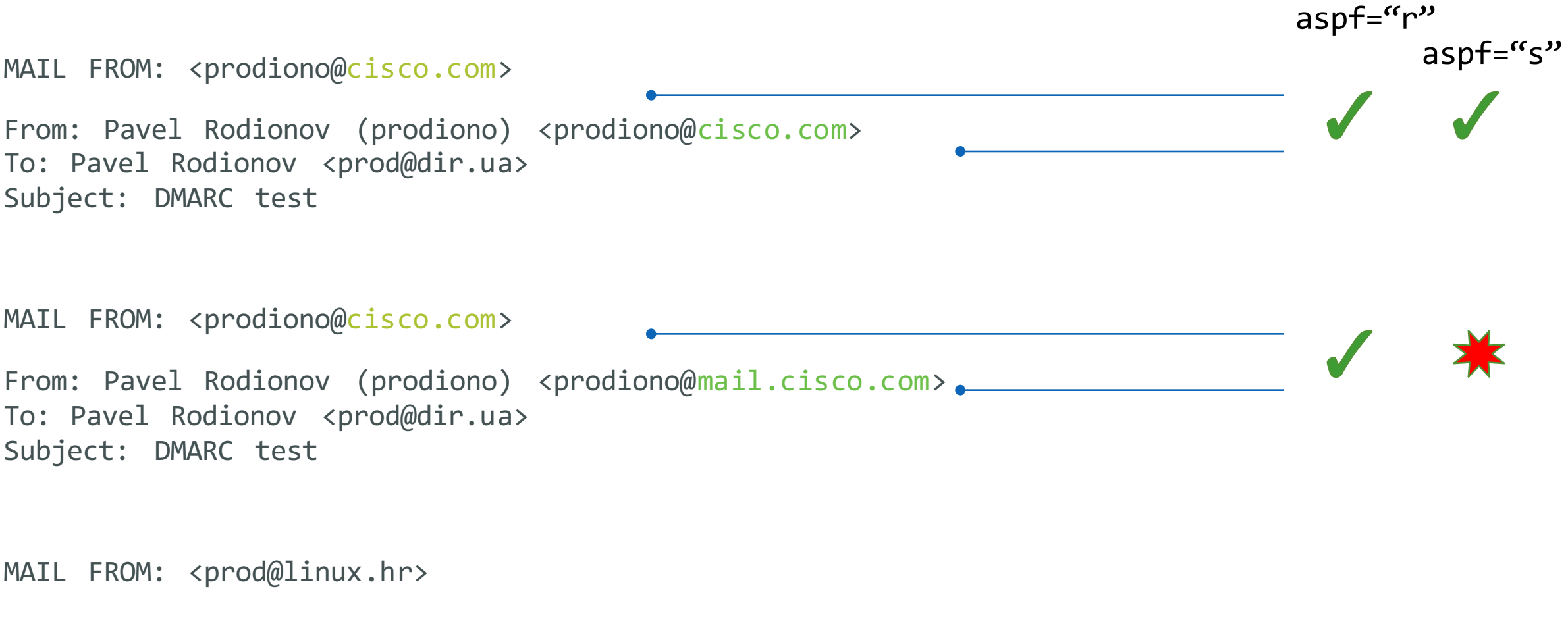
```
MAIL FROM: <prodiono@cisco.com>

From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

```
MAIL FROM: <prodiono@cisco.com>

From: Pavel Rodionov (prodiono) <prodiono@mail.cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

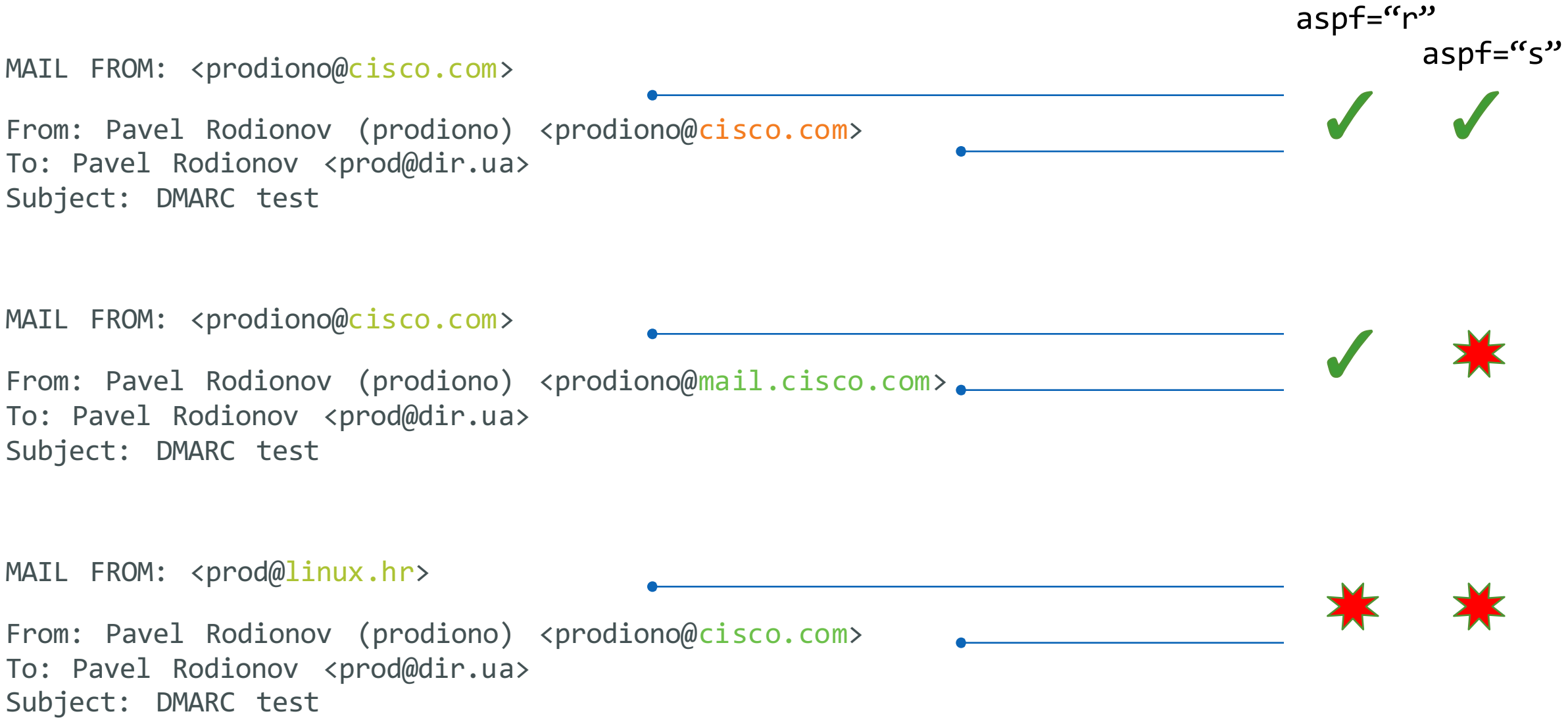
Выравнивание DMARC идентификатора: SPF



Выравнивание DMARC идентификатора: SPF



Выравнивание DMARC идентификатора: SPF

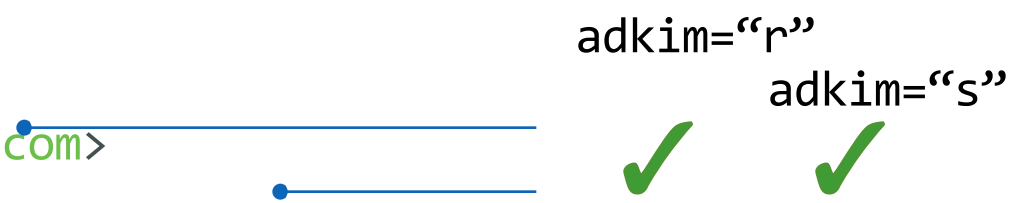


Выравнивание DMARC идентификатора: DKIM

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

Выравнивание DMARC идентификатора: DKIM

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```



Выравнивание DMARC идентификатора: DKIM

```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Pavel Rodionov (prodiono) <prodiono@cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

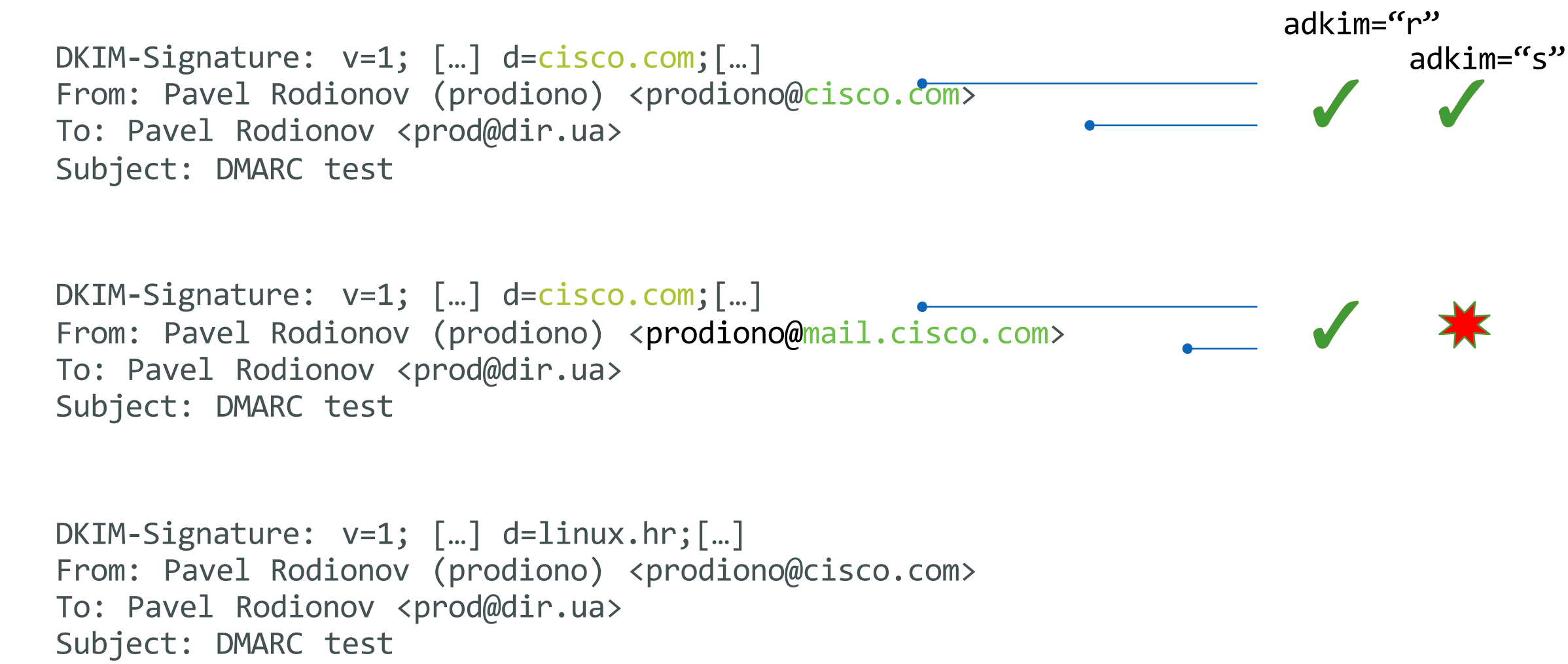
adkim="r" ✓

adkim="s" ✓

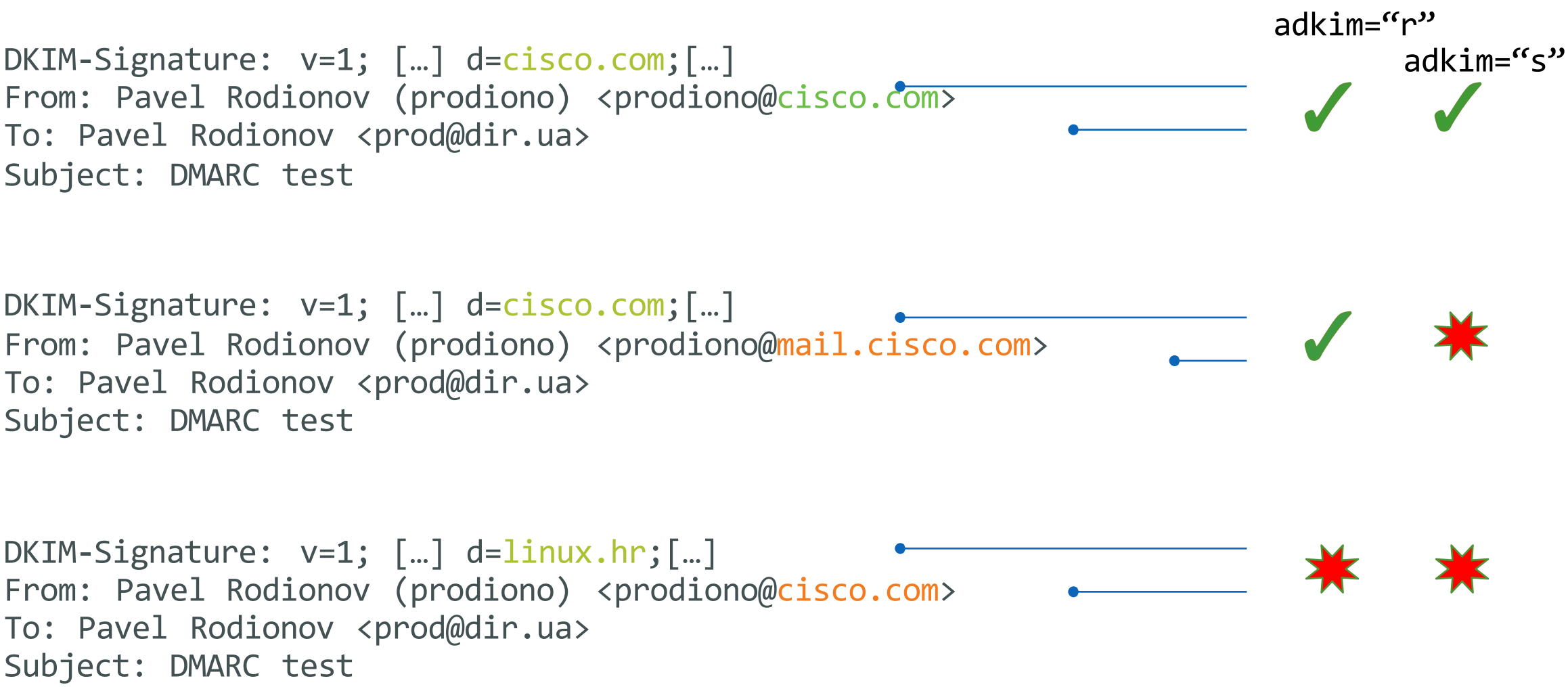
```
DKIM-Signature: v=1; […] d=cisco.com;[…]
From: Pavel Rodionov (prodiono) <prodiono@mail.cisco.com>
To: Pavel Rodionov <prod@dir.ua>
Subject: DMARC test
```

Выравнивание DMARC идентификатора: DKIM

Выравнивание DMARC идентификатора: DKIM



Выравнивание DMARC идентификатора: DKIM



Несколько подписей DKIM? **Любая** должна быть проверена и выровнена.

DMARC на ESA

DMARC

Global Settings	
Specific Senders Bypass Address List:	None Specified
Bypass Verification for Messages with Headers:	None Specified
Schedule for Report Generation:	12:00 AM
Entity Generating Reports:	None Specified
Additional Contact Information for Reports:	None Specified
Send Copy of All Aggregate Reports to:	None Specified
Send Delivery Error Reports:	No

Edit Global Settings...

DMARC Verification Profiles — Items per page 20

Add Profile... Import Profiles...

Profile Name	Reject Policy Message Action	Quarantine Policy Message Action	SMTP Action for Temporary Failure	SMTP Action for Permanent Failure	All Delete
DEFAULT	No Action	No Action	Accept	Accept	

Export Profiles... Delete

Не попадайтесь на крючок

- DMARC обеспечивает
  - Легкую, простую и мощную стандартную аутентификацию сообщений
  - Гибкое и последовательное развертывание
  - Шанс очистить ваш email и усилить безопасность сообщений
  - Простую защиту от фишинговых атак – как со стороны рыбы, так и со стороны наживки

Не попадайтесь на крючок.
Это просто!

Для дополнительной информации

- http://www.openspf.org
- http://www.dkim.org
- http://blogs.cisco.com/security/big-data-in-security-part-v-anti-phishing-in-the-cloud/
- https://support.google.com/mail/answer/3070163?hl=en
- http://tools.ietf.org/html/draft-kucherawy-dmarc-base-04
- http://dmarc.org
- http://dmarcian.com

Thank you.