

УДК 004.732:004.056
ББК 32.973.202
А97

А97 Ачилов Р. Н.

Построение защищенных корпоративных сетей. – М.: ДМК Пресс, 2013. – 250 с.: ил.

ISBN 978-5-94074-884-7

В книге рассказано обо всем, что необходимо для построения защищенной от внешних воздействий корпоративной сети – о том, как создать собственный удостоверяющий центр для выдачи SSL-сертификатов, как выдавать, отзывать, преобразовывать и просматривать сертификаты. Как установить SSL-сертификат в ОС или браузер, как его использовать, работая с защищенным ресурсом и какие ошибки при этом возникают.

Описывается, как с помощью сертификатов защитить корпоративную электронную почту на всех этапах ее передачи – от почтовой программы пользователя до сервера получателя; как установить веб-интерфейс к хранимой на сервере почте, позволяющий просматривать ее в защищенном режиме с любой точки мира.

Также уделено внимание защите служебных коммуникаций, в частности подключения из скриптов для управления серверами. В книге приводится большое число примеров конфигурационных файлов с подробным пояснением параметров, а также скриптов на языке Bourne Shell 1.x.

Издание предназначено для системных и сетевых администраторов UNIX, администраторов средств информационной безопасности.

УДК 004.732:004.056
 ББК 32.973.202

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-94074-884-7

© Ачилов Р. Н., 2012
 © Оформление, издание, ДМК Пресс, 2013



Предисловие	6
--------------------------	----------

Введение	8
-----------------------	----------

Глава 1

Корпоративный «паспортный стол»	12
--	-----------

1.1. Создание удостоверяющего центра	13
---	-----------

1.1.1. Файловая структура CA.....	13
-----------------------------------	----

1.1.2. Конфигурационный файл openssl.cnf.....	15
---	----

1.1.3. Задание subjectAltName.....	25
------------------------------------	----

1.1.4. Создание ключа CA	26
--------------------------------	----

1.1.5. Скрипты по управлению CA.....	28
--------------------------------------	----

1.2. Генерация запроса на сертификат	38
---	-----------

1.2.1. Создание запроса на сертификат с помощью OpenSSL	40
---	----

1.2.2. Создание запроса на сертификат с помощью Crypto4 PKI	46
---	----

1.2.3. Создание запроса на сертификат с помощью Certreq.exe.....	50
--	----

1.3. Создание сертификата	55
--	-----------

1.4. Отзыв сертификата. Управление списками отзыва.....	59
--	-----------

1.5. Передача сертификата по сетям общего пользования	62
--	-----------

1.6. Дополнительные операции с сертификатами.....	65
--	-----------

Глава 2

Сертификаты в браузерах Интернет.....	71
--	-----------

2.1. Установка сертификатов в браузеры	72
---	-----------

2.1.1. В системное хранилище Windows.....	73
---	----

2.1.2. В браузер Mozilla Firefox.....	80
---------------------------------------	----

4 ОГЛАВЛЕНИЕ

2.1.3. В браузер Opera.....	84
2.2. Доступ к ресурсам, защищенным сертификатами	88
2.2.1. Из браузера Internet Explorer.....	89
2.2.2. Из браузера Mozilla Firefox.....	92
2.2.3. Из браузера Opera.....	95
2.2.4. Из браузера Google Chrome	97
2.3. Общие ошибки при использовании сертификатов	98
2.3.1. Подключение без сертификата	99
2.3.2. Невозможно проверить подлинность сертификата.....	101
2.3.3. Срок действия сертификата истек или еще не начинался.....	104
2.3.4. Сертификат отозван	107
2.3.5. Другие ошибки сертификатов.....	109

Глава 3

Сквозная аутентификация в электронной почте..... 110

3.1. Аутентификация в AD с помощью PAM- и NSS-сервисов...	114
3.2. Настройка модулей nss_ldap и pam_ldap.....	117
3.2.1. Настройка nss_ldap.conf.....	117
3.2.2. Настройка pam_ldap.conf	121
3.2.3. Примеры конфигурационных файлов модулей NSS и PAM	122
3.2.4. Изменения на сервере контроллера домена	123

Глава 4

Защита электронной почты 130

4.1. Сертификаты в sendmail	131
4.1.1. Простое шифрование.....	134
4.1.2. Шифрование с взаимной перекрестной проверкой	139
4.1.3. Шифрование при приеме от локального пользователя.....	145
4.2. Сертификаты в почтовых серверах для локального офиса	150
4.2.1. Использование сертификатов в POP3-сервере qpopper...	151
4.2.2. Использование сертификатов в IMAP-сервере dovecot	154
4.3. Сертификаты в клиентских почтовых программах.....	158
4.3.1. Сертификаты в программе Mozilla Thunderbird	159
4.3.2. Сертификаты в программе Microsoft Outlook 2007	164

4.3.3. Сертификаты в Opera Mail.....	167
4.3.4. Сертификаты в почтовых программах мобильных устройств.....	169

Глава 5

Корпоративный веб-портал	172
5.1. Сертификаты в веб-сервере Apache	174
5.2. Установка Horde Groupware Webmail Edition.....	179
5.3. Настройка Horde Groupware Webmail Edition.....	187
5.3.1. Настройки портала в целом (модуль horde).....	188
5.3.2. Настройки функциональных модулей портала	198
5.3.3. Дополнительные настройки в конфигурационных файлах....	200
5.4. Пользовательские настройки и почтовые функции Horde4	207
5.4.1. Пользовательские настройки портала	208
5.4.2. Почтовые функции Horde4	215
5.5. Функции календаря, задач и заметок в Horde4.....	220

Глава 6

Защита служебных коммуникаций	230
6.1. Удаленная работа на сервере UNIX без ввода пароля ...	233
Заключение	241
Глоссарий	242
Внешние ссылки и литература	245
Предметный указатель	247