Технический Центр Интернет

Внедрение DNSSEC для администраторов доменных имен

Руководство пользователя

На 10 страницах

Информация о документе

Индекс документа	РП
Статус документа	Справочный документ
Дата начала действия документа	01.04.2018
Версия	1
Дата окончания действия документа	

Содержание

1 Введение

Настоящий документ представляет собой руководство пользователя и является справочным документом.

DNSSEC обеспечивает высокий уровень безопасности для организаций, чьё присутствие в сети является существенным компонентом их бизнеса.

По аналогии с протоколом SSL (Secure Sockets Layer) и другими протоколами обеспечения безопасности, DNSSEC является необходимым условием для повышения безопасности предоставляемых пользователям компании услуг. Применение этой технологии повышает доверие к множеству услуг, оказываемых через интернет: электронная коммерция, мобильный банкинг, IP-телефония, удалённое распространение программного обеспечения и другие.

DNSSEC предотвращает перенаправление пользовательского трафика на подставные сайты кибер-преступников, где может быть осуществлена кража данных банковских карт или паролей, осуществлено прослушивание голосового трафика и перехват почтовых сообщений.

2 Общие сведения

2.1 Зачем внедрять DNSSEC

Внедрение DNSSEC позволяет владельцам доменов:

- Защитить свой бренд и данные своих пользователей;
- Снизить риски компрометации данных сайта;
- Завоевать доверие и лояльность своих клиентов;
- Привлечь заботящихся о безопасности пользователей;
- Защитить свой бизнес;
- Заслужить репутацию передовой компании.

2.2 Что необходимо сделать

Технология DNSSEC построена на иерархии доверия. Участники верхнего уровня ручаются за участников, расположенных ниже по иерархии. Это означает, что регистратор (а также интернет-провайдер или хостинг-провайдер) должен поддерживать DNSSEC, чтобы администратор доменного имени также мог использовать DNSSEC.

Для включения DNSSEC для вебсайта или сетевой службы (например, для почтового сервера), необходимо применить электронную подпись к информации о домене. Такая опция предоставляется при регистрации домена или же применяется к существующим доменам.

2.3 С чего начать

1. Проведение исследований:
   - Позиционировать DNSSEC в иерархии средств обеспечения безопасности;
   - Определить возможности, предоставляемые DNSSEC, а также возникающие при внедрении сложности;
   - Провести обучение персонала технической поддержки.
2. Планирование:
   - Пересмотреть и обновить политику безопасности;
   - Узнать, внедрен ли DNSSEC у регистратора доменного имени.
3. Внедрение:
   - Провести лабораторные испытания системы;
   - Перейти на рабочую версию.
4. Принятие участие:
   - Обеспечить обратную связь с сообществом по поводу практики внедрения DNSSEC.

3 Практика применения DNSSEC для администраторов доменных имен

В данном документе будут показаны типовые практики применения DNSSEC. Невозможно охватить все нюансы внедрения по причине возможного различия входных данных. В текущем описании показывается работа на примере сервера доменных имён со следующей конфигурацией:

```
openSUSE 12.2
BIND 9.9.1P4
OpenSSL 1.0.1c
```

В качестве тестового домена используем несуществующий домен `test.ru`.

Предполагается, что владелец домена использует целиком собственную инфраструктуру.

3.1 Основные понятия DNSSEC

Работа DNSSEC основывается на асимметричной криптографии. Данные подписываются закрытым ключом, хранимым в секрете; проверяются – открытым, доступным публично. Обычно для каждой зоны используются два ключа: ZSK (Zone Signing Key – ключ подписания зоны) и KSK (Key Signing Key – ключ подписания ключей). Разделение связано с тем, что при выдаче сервером имён ответов на запросы о доменах накапливается криптографический материал, который может облегчить подбор закрытой части ключа, а следовательно, скомпрометировать его. Для подписания зоны можно издать ключ максимальной длины. Тогда его подбор значительно усложнится, но и скорость подписания зоны существенно упадёт. Поэтому зона подписывается ключом, имеющим меньшую длину и меньший срок действия, а сам ключ подписания зоны подписывается ключом, имеющим большую длину и больший срок действия.

Если зона имеет малый размер, изменения в зону вносятся нечасто – с целью минимизирования затрат на обслуживание имеет смысл использовать систему с единым ключом подписания. Издаётся только ключ KSK, которым подписывается зона и запись о самом себе в зоне (или набор ключей, например на этапе смены ключа или в случае использования нескольких KSK для разных алгоритмов подписи).

С использованием ZSK в файле зоны создаются записи RRSIG для каждого набора записей в зоне (RRSET), кроме неавторитетных записей. По сути RRSIG – это электронная подпись. На этапе подписания зоны указывается период валидности RRSIG, то есть период, в течение которого эта подпись удостоверяет соответствующую запись. Этот период выбирается меньшим, чем период действия ZSK. В течение срока жизни ZSK зона периодически переподписывается всё тем же ZSK, что ведёт к созданию новых RRSIG. Делается это также с целью минимизировать вероятность подбора закрытой части ZSK.

Также в файле зоны создаются записи NSEC или NSEC3. Эти записи связаны с механизмом защиты от внесения недоброжелателем в зону записей о доменах, поскольку при внесении в зону неподписанных записей о доменах сервер всё равно будет их возвращать резолверам, только в неподписанном виде.

3.2 Настройка зоны

Опустим общие вопросы настройки операционной системы и DNS-сервера и перейдём непосредственно к настройке зоны и DNSSEC на `ns1.test.ru`, вторичный сервер `ns2.test.ru`.

Файл настроек:

`BIND:/etc/named.conf`.

Добавим в него строку с настройкой файла, в котором будут описываться зоны:

```
ns1:/etc # echo 'include "/var/lib/named/etc/named.conf.include";' >> /etc/named.conf
```

Также закомментируем строчку:

```
include "/etc/named.conf.include";
```

Создадим файл `/var/lib/named/etc/named.conf.include`:

```
ns1:/var/lib/named/etc # cat named.conf.include
zone "test.ru"{
type master;
file "master/TEST.RU/test.ru";
allow-transfer {192.168.1.1;};
allow-query { any;};
};
```

Создадим файл зоны test.ru:

```
ns1:/var/lib/named/master/TEST.RU               # cat test.ru
$TTL 3600;     1 hour
@                       IN SOA ns     hostmaster.test.ru. (
                        2012111501;   serial
                        7200          ;      refresh (2 hours)
                        3600          ;      retry (1 hour)
                        604800 ;      expire (1 week)
                        1800          ;      minimum (30 minutes)
                                      )
                IN      NS            ns
                IN      NS            ns1
                IN      MX            10     mail
                IN      A             192.168.0.2
www                     IN      A             192.168.0.2
ns1                     IN      A             192.168.0.1
ns2                     IN      A             192.168.1.1
mail                    IN      A             192.168.0.3
```

3.3 Создание ключей зоны

3.4 Схема с раздельными ключами

Классическим случаем является наличие в зоне одного KSK и одного ZSK. В нашем варианте будет два KSK и два ZSK: по паре ключей на каждый из алгоритмов – RSA-SHA-256 и GOST R 34-10.2001.

Исходя из опыта внедрения DNSSEC в доменах верхнего уровня, для RSA-SHA-256 будем использовать длины и период жизни ключей:

- KSK – 2048 бит; 1 год;
- ZSK – 1024 бит; 3 месяца.

Алгоритм ГОСТ жёстко фиксирует длины ключей, период жизни ключей выбираем таким же.

RSA-SHA-256, ZSK:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-keygen -a RSASHA256 -b 1024 test.ru
Generating key pair.....................................++++++
.................++++++
Ktest.ru.+008+20100
```

RSA-SHA-256, KSK:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-keygen -a RSASHA256 -b 2024 -f KSK test.ru
Generating key pair..+++ .....................................+++
Ktest.ru.+008+41584
```

ГОСТ, ZSK:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-keygen -a ECCGOST test.ru
Generating key pair.
Ktest.ru.+012+27315
```

ГОСТ, KSK:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-keygen -a ECCGOST -f KSK test.ru
Generating key pair.
Ktest.ru.+012+33278
```

После операций создания ключей каталог выглядит следующим образом:

```
ns1:/var/lib/named/master/TEST.RU # ll
total 36
-rw-r--r-- 1 root root 427  Nov    15 12:42 Ktest.ru.+008+20100.key
-rw------- 1 root root 1012 Nov    15 12:42 Ktest.ru.+008+20100.private
-rw-r--r-- 1 root root 597  Nov    15 12:43 Ktest.ru.+008+41584.key
-rw------- 1 root root 1768 Nov    15 12:43 Ktest.ru.+008+41584.private
-rw-r--r-- 1 root root 338  Nov    15 12:44 Ktest.ru.+012+27315.key
-rw------- 1 root root 230  Nov    15 12:44 Ktest.ru.+012+27315.private
-rw-r--r-- 1 root root 337  Nov    15 12:44 Ktest.ru.+012+33278.key
-rw------- 1 root root 230  Nov    15 12:44 Ktest.ru.+012+33278.private
-r--r--r-- 1 root root 577  Nov    15 12:40 test.ru
```

В файлах с расширением .`key` содержатся открытые части ключей, в файлах с расширением .`private` – закрытые. 012 – для алгоритма ГОСТ, 008 – для RSA-SHA-256.

Теперь файл зоны необходимо подписать. Не забываем предварительно увеличить серийный номер зоны в файле test.ru (можно использовать ключ –`Nincrement`, тогда серийный номер автоматически увеличится на единицу):

```
ns1:/var/lib/named/master/TEST.RU # dnssec-signzone -S -x -e+3mo test.ru
Fetching KSK 41584/RSASHA256 from key repository.
Fetching ZSK 20100/RSASHA256 from key repository.
Fetching ZSK 27315/ECCGOST from key repository.
Fetching KSK 33278/ECCGOST from key repository.
Verifying the zone using the following algorithms: RSASHA256 ECCGOST.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 1 active, 0 present, 0 revoked
```

```
Algorithm: ECCGOST: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 1 active, 0 present, 0 revoked
test.ru.signed
```

После подписания каталог выглядит следующим образом:

```
ns1:/var/lib/named/master/TEST.RU # ll
total 52
-rw-r--r-- 1 root root      427   Nov 15 12:42 Ktest.ru.+008+20100.key
-rw------- 1 root root      1012  Nov 15 12:42 Ktest.ru.+008+20100.private
-rw-r--r-- 1 root root      597   Nov 15 12:43 Ktest.ru.+008+41584.key
-rw------- 1 root root      1768  Nov 15 12:43 Ktest.ru.+008+41584.private
-rw-r--r-- 1 root root      338   Nov 15 12:44 Ktest.ru.+012+27315.key
-rw------- 1 root root      230   Nov 15 12:44 Ktest.ru.+012+27315.private
-rw-r--r-- 1 root root      337   Nov 15 12:44 Ktest.ru.+012+33278.key
-rw------- 1 root root      230   Nov 15 12:44 Ktest.ru.+012+33278.private
-rw-r--r-- 1 root root      328   Nov 15 12:46 dsset-test.ru.
-r--r--r-- 1 root root      577   Nov 15 12:45 test.ru
-rw-r--r-- 1 root root      8733  Nov 15 12:46 test.ru.signed
```

Необходимо изменить строку в файле `/var/lib/named/etc/named.conf.include`:

```
file "master/TEST.RU/test.ru";
```

на строку:

```
file "master/TEST.RU/test.ru.signed";
```

так как мы теперь используем подписанную зону.

В подписанном файле зоны можно наблюдать по два RRSIG для каждого RR: по алгоритму 8-RSA-SHA-256 и по алгоритму 12-ГОСТ.

Сформируем DS-записи для ключа `Ktest.ru.+012+33278` по ГОСТ, а для ключа `Ktest.ru.+008+41584` – по SHA-256:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-dsfromkey -a GOST Ktest.ru.+012+33278 > ds-gost-test.ru
ns1:/var/lib/named/master/TEST.RU # dnssec-dsfromkey -2 Ktest.ru.+008+41584 > ds-sha256-test.ru
```

Данные DS-записи необходимо разместить в родительской зоне в соответствии с правилами данной зоны (устанавливаются регистратурой доменной зоны).

3.5 Схема с одним ключом

Для небольших зон требования к периоду жизни ключей и к периоду валидности RRSIG снижаются. Также возможно использовать один ключ и для подписания зоны, и для установления цепочки доверия.

Из схемы с раздельными ключами будем использовать ключи KSK по обоим алгоритмам. Приведём начало неподписанного файла зоны к виду:

```
$TTL 3600            ; 1 hour
$include      Ktest.ru.+012+33278.key
$include      Ktest.ru.+008+41584.key
```

Произведём подпись зоны, период валидности RRSIG по умолчанию равен одному месяцу:

```
ns1:/var/lib/named/master/TEST.RU # dnssec-signzone -z -k Ktest.ru.+012+33278 -k
Ktest.ru.+008+41584 test.ru
Verifying the zone using the following algorithms: RSASHA256 ECCGOST.
Zone signing complete:
```

```
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 0 active, 0 stand-by, 0 revoked
Algorithm: ECCGOST: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 0 active, 0 stand-by, 0 revoked
test.ru.signed
```

Зона потребует переподписания в следующих случаях:

- Внесены изменения в зону – добавлены или удалены записи;
- Истекает период валидности RRSIG – заблаговременно до истечения с целью недопущения попадания в кэши резолверов невалидных RRSIG;
- Смена ключа KSK.

Контакты ООО «Технический центр Интернет»

- 127083, Москва, улица 8 Марта, дом 1 строение 12
- Телефон: +7 (495) 730-29-69

Клиентская служба

Клиентская служба Технического центра Интернет:

- Телефон: +7 (495) 730-29-69.