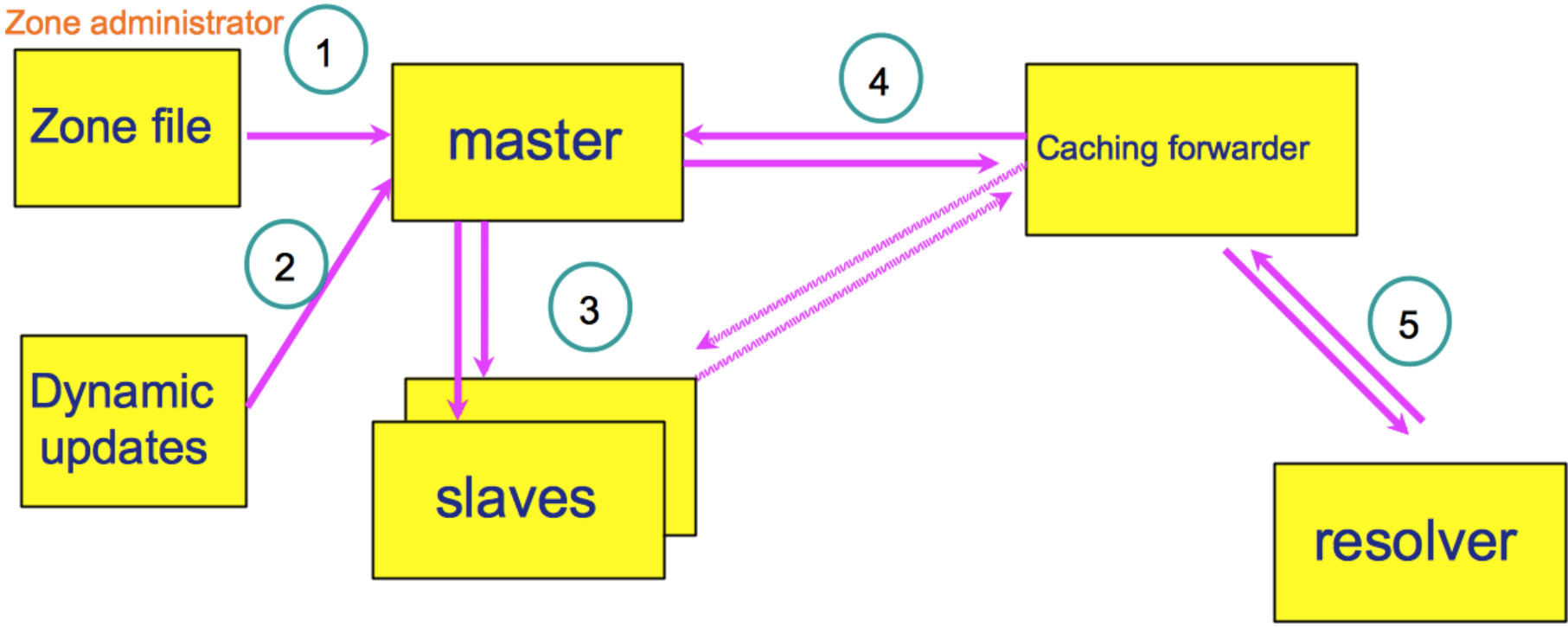
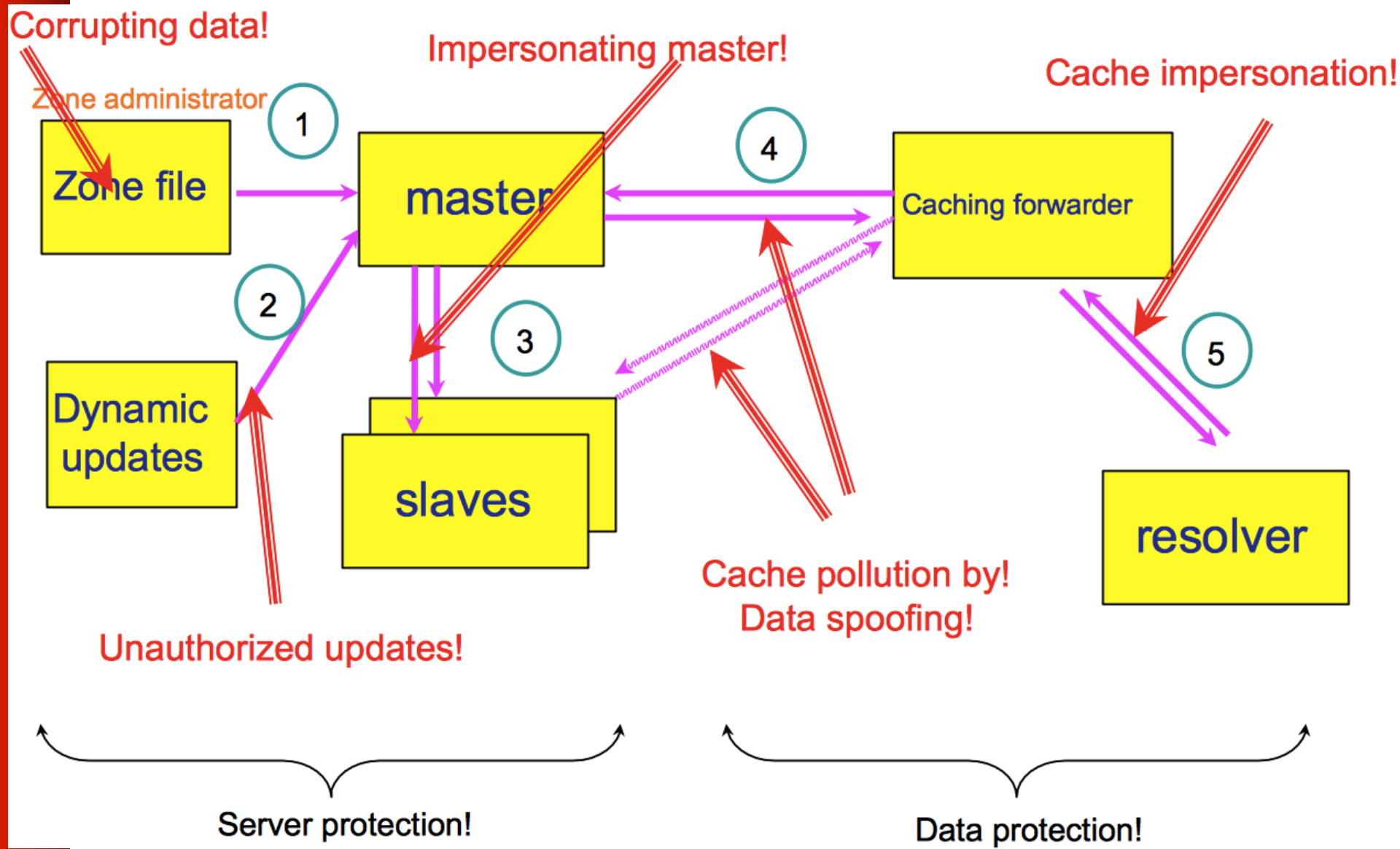
DNS. Эксплуатация и защита данных. Продвинутый курс

Защита DNS - TSIG

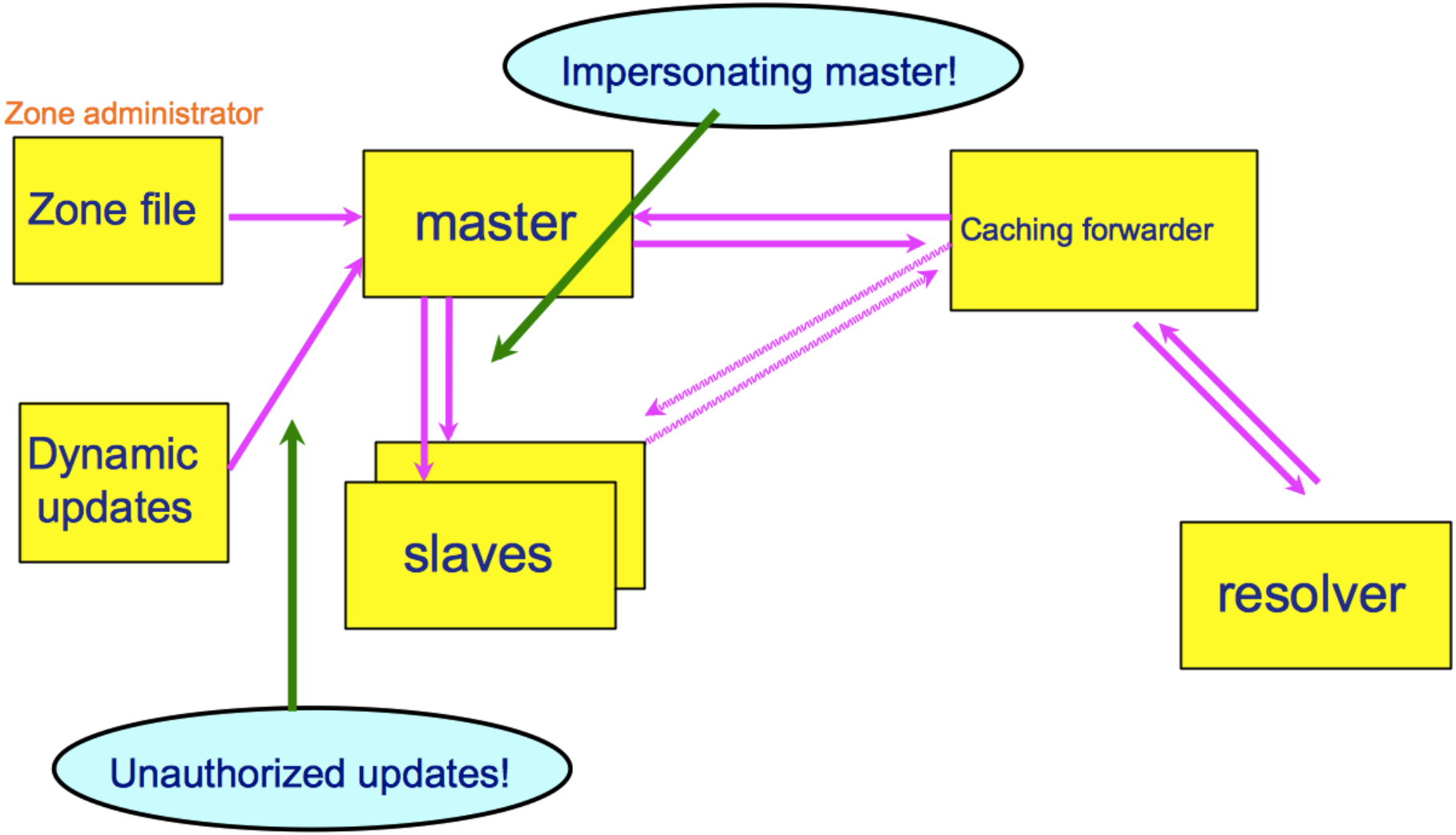
DNS: движение информации



Уязвимости DNS



Уязвимости, от которых защищает TSIG



Что такое TSIG ?

- **Transaction SIGnature – подпись операции**
- Механизм для защиты коммуникации между серверами DNS либо между системой разрешения имен и серверами DNS
- Применяется шифрованый хэш (похоже на цифровую подпись), таким образом что получатель сообщения может проверить, что сообщение не было модифицировано:

  - DNS запрос / ответ

  - отметка времени
- Базируется на знании общего секрета

  - и отправитель и получатель должны быть соответственно настроены

Что такое TSIG ?

- RFC 2845 – TSIG
- Можно также использоваться для санкционирования:

  - скачивания зоны

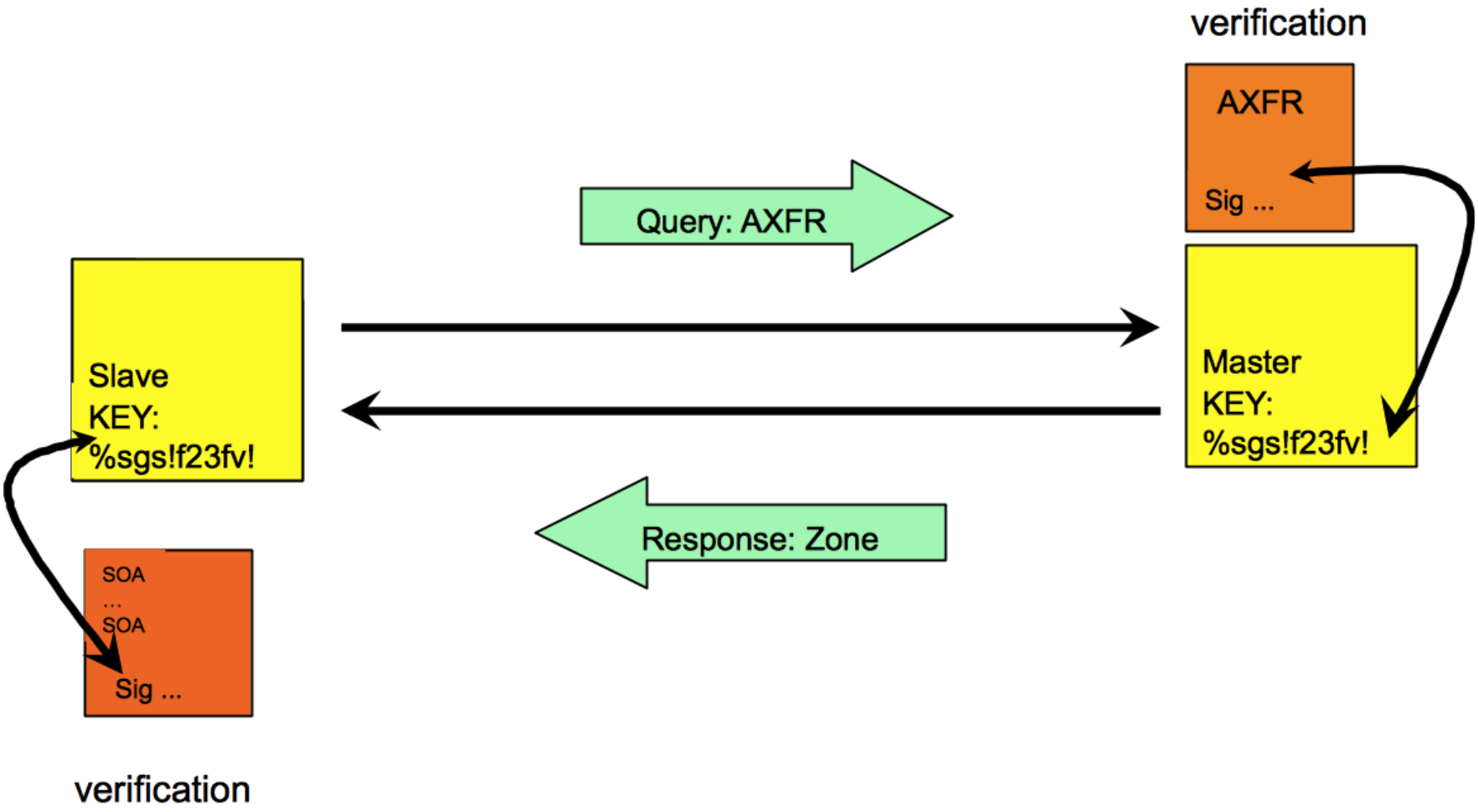
  - динамических обновлений

  - авторизации кэширующих серверов

- Используется в конфигурации сервера – а не в файле зоны

- ACL

Пример TSIG:


verification
AXFR
Sig ...
Query: AXFR
Slave
KEY:
%sgs!f23fv!
Master
KEY:
%sgs!f23fv!
Response: Zone
SOA
...
SOA
Sig ...
verification

TSIG по шагам

1. Создание секрета
2. Передача секрета
3. Конфигурирование сервер
4. Проверка работоспособности

TSIG – имена и секреты

- TSIG имя

  - Имя дается ключу. Имя передается в сообщении, так что получатель знает, какой именно ключ использовал отправитель – потенциально из нескольких возможных

- TSIG секретное значение

  - Значение определяется по время создания ключа
  - Обычно в схеме BASE64

TSIG – создание секрета

- dnssec-keygen

  - Простой инструмент создания разных ключей
  - Здесь используется для создания ключей TSIG

dnssec-keygen -a <algorithm> -b <bits> -n host <key name>

TSIG – создание секрета

- Пример

dnssec-keygen -a HMAC-MD5 –b 128 -n host ns1-ns2.grp2.net

- Создаст ключ примерно такого вида:

Kns1-ns2.grp2.net.+157+15921

- Файлы

  Kns1-ns2.grp2.net.+157+15921.key

  Kns1-ns2.grp2.net.+157+15921.private

TSIG – создание секрета

- Ключи TSIG никогда не помещаются в файлы зоны
- Это может привести к путанице, потому что ключи могут выглядеть похоже на ресурсные записи в DNS:

ns1-ns2.grp2.net. IN KEY 128 157 nEfRx9…bbPn7lyQtE=

TSIG – конфигурация серверов

- Конфигурирование ключа

  - в named.conf, тот же синтаксис что и для оператора rndc:

- Использование ключа:

  - в named.conf, добавьте:

  server x { key ….; };

… где ‘x’ - IP-адрес УДАЛЕННОГО сервера.

Пример конфигурации – named.conf

Первичный сервер 10.10.0.1

```
key ns1-ns2.grp2.net {
    algorithm hmac-md5;
    secret “APlaceToBe”;
};
server 10.10.0.2 {
      keys { ns1-ns2.grp2.net; };
};
zone “my.test.zone” {
      type master;
      file “db.myzone”;
      allow-transfer {
            key ns1-ns2.grp2.net;
      };
};
```

Вторичный сервер 10.10.0.2

```
key ns1-ns2.grp2.net {
    algorithm hmac-md5;
    secret “APlaceToBe”;
};
server 10.10.0.1 {
      keys { ns1-ns2.grp2.net; };
};
zone “my.test.zone” {
      type slave;
      file “db.myzone.slave”;
            masters { 10.10.0.1; };
      };
};
```

TSIG – тестирование при помощи dig

- dig может быть использован для проверки настроек TSIG

  dig @<server> <zone> AXFR –k <TSIG keyfile>

или

  dig @<server> <zone> AXFR –y “TSIG secret”

- Неправильный ключ вернет “Transfer failed”, и соответствующее сообщение уйдет в лог в категорию “security” на запрашиваемом сервере

TSIG – Время!

- TSIG зависит от времени (чтобы защитить от атак, основанных на воспроизведении старых запросов)

  - защита сообщения работает только в течение 5 минут от создания сообщения

  - убедитесь, что время на серверах синхронизировано! (NTP)

  - для проверки, установите время вручную

  - во время эксплуатации, пользуйтесь NTP!

Вопросы

?