ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 2,3
2012

Н. Г. Ляпичева, **О. М. Никонова** (Москва, ЦЭМИ РАН).
DNS-сервер за межсетевым экраном: особенности использования.

Как обсуждалось ранее [1], внедрение многоязычных доменных имен (IDN) в масштабах Интернета породило ряд проблем, связанных с неоднородностью сетевой среды, прежде всего — с моральным устареванием сетевого оборудования и серверов (что часто приводит к использованию устаревшего программного обеспечения). Это обстоятельство, в дополнение к другим, активизирует модернизацию сетевой среды Интернета.

В нашем случае модернизация была направлена на повышение производительности граничного маршрутизатора, устаревающего морально и физически. В условиях ограниченности финансирования было принято нестандартное решение вопроса: вместо полнофункционального маршрутизатора был установлен недорогой (менее 100 тыс. руб.) межсетевой экран — устройство адаптивной защиты ASA5510 производства Cisco systems. Данное устройство поддерживает режим «маршрутизатор», и в этом режиме способно обеспечить необходимую функциональность для сети объемом до 500 ПК и серверов.

Рекомендованным принципом размещения DNS является его установка в демилитаризованной зоне — вне сегмента, отделенного сетевым экраном. Однако когда межсетевой экран является граничным маршрутизатором, сервер находится внутри сети, присоединен к одному из интерфейсов, и DNS-трафик обрабатывается согласно встроенным аппаратно-программным функциям контроля. Эти функции отвечают принятым международным стандартам [2], однако некоторые черты активно развивающегося направления — IDN [3] еще не полностью отражены в функциях сетевого экрана и требуют дополнительной настройки.

В частности, функции встроенного контроля пакетов по умолчанию включают проверку длины доменного имени до 255 байт и метки до 63 байт, что уже вызывает появление сообщений об отказе. Другое ограничение по умолчанию — на общую длину пакета — может быть отменено, тогда пакет может иметь длину до 65535 байт.

В то же время преимуществом использования межсетевого экрана в качестве маршрутизатора является отслеживание сессий протокола DNS, что позволяет снизить возможность фальсификации апдейтов, а также инфицированности кэша DNS-сервера внешними источниками.

И к сожалению, межсетевой экран не полностью спасает от атаки «Отказ в обслуживании» — на атакованных интерфейсах производительность падает до пределов, определяемых лимитами их пропускной способности и возможностями атакующих средств. Например, в нашем случае атака DoS, направленная на сервера DNS в целом и на сервер внутренней сети в частности, исходящая от скомпрометированного сервера Linux SUSE, привела к полному отказу в обслуживании в том сегменте, где он установлен, и в сегменте DNS. Остальная сеть осталась частично работоспособной за счет использования вторичного сервера, замедление работы вызывается дефицитом

памяти и возможностей процессора на межсетевом экране. Отмечено замедление работы электронной почты, т. к. почтовый антиспамовый шлюз установлен в том же сегменте.

СПИСОК ЛИТЕРАТУРЫ

1. *Ляпичева Н. Г.*, *Никонова О. М.* Проблемы DNS-сервиса и их роль в борьбе со спамом. — Обозрение прикл. и промышл. матем., 2011, т. 18, в. 5. с. 670–672
2. RFC6195, RFC1035, RFC3490, RFC3492, RFC4035, RFC5507, RFC5891 http://www.faqs.org/rfcs/
3. Repository of IDN Practices http://www.iana.org/domains/idn-tables