Улучшение безопасности и надежности DNS

Carlos Vicente

Network Startup Resource Center

UNIVERSITY OF OREGON

Что грозит DNS?

- Авария сервера
- Взлом сервера
- Атаки типа “отказ от обслуживания” (DoS)
- Атаки с усилением
- Отравление кэша
- Атаки, направленные на конкретный сервер, использующие информацию о зоне
- И другие
  - http://www.dnssec.net/dns-threats

Атаки DoS

- Перегрузка целевой машины запросами ”снаружи”, так что она не может обрабатывать нормальные запросы
- Когда ваши серверы DNS подвергаются атаке типа ”отказ от обслуживания”:
  - Ваши клиенты не могут получать информацию о других доменах
  - Остальной интернет не может получать информацию о ваших доменах
  - Итог примерно такой, как если бы вы не были подключены к Интернету

Атаки с усилением

- Также известны как ”отражающие атаки”
- Серверы DNS используются как инструменты атаки
  - Посылают ответы на запросы, исходные адреса которых были сфальсифицированы
- Машина, которой принадлежит сфальсифицированный адрес, является жертвой

4 November 2010 Last updated at 11:33 ET

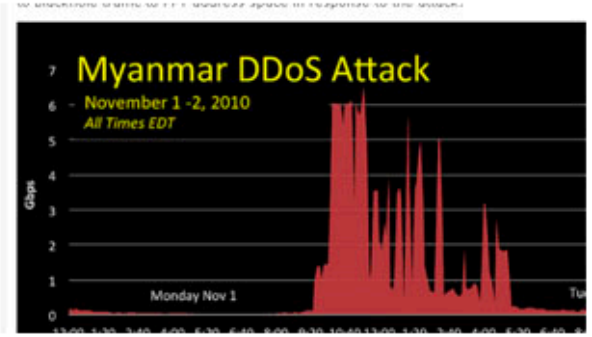
Burma hit by massive net attack ahead of election

An ongoing computer attack has knocked Burma off the internet, just days ahead of its first election in 20 years.

The attack started in late October but has grown in the last few days to overwhelm the nation's link to the net, said security firm Arbor Networks.

Reports from Burma say the disruption is ongoing.

The attack, which is believed to have started on 25 October, comes ahead of closely-watched national elections on 7 November.



Huge amounts of traffic easily overwhelmed Burma's links to the net

International observers and foreign journalists are not being allowed into the country to cover the polls.

It will raise suspicions that Burma's military authorities could be trying to restrict the flow of information over the election period.

The ruling generals say the polls will mark a transition to democratic

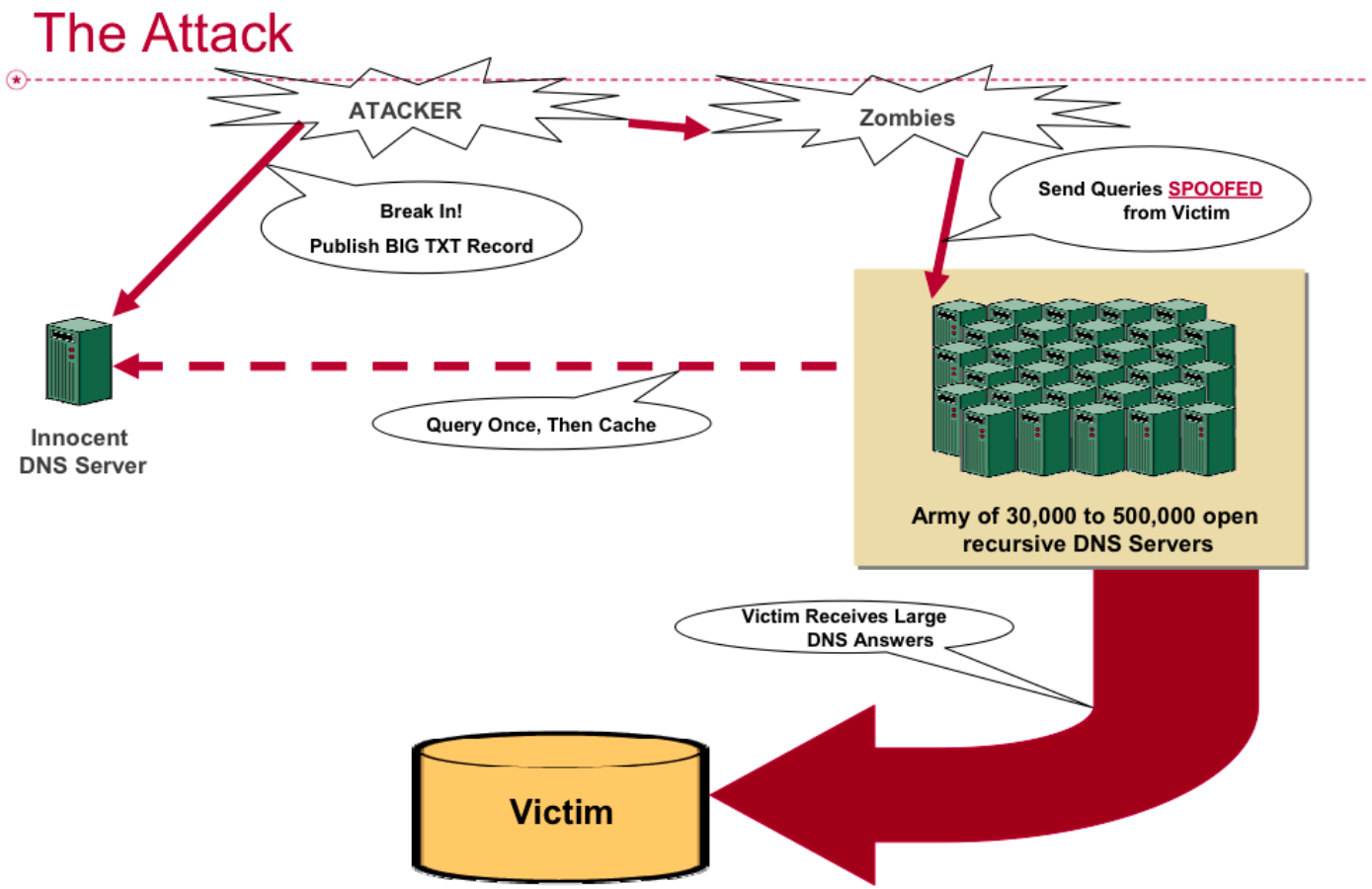
Related stories

Burma election: Q&A

Spanish police smash huge botnet

Cyber wars in Iran

Атаки с усилением



Источник: http://www.nanog.org/meetings/nanog37/presentations/frank-scalzo.pdf

Атаки с усилением

- От них тяжело защитить пользователей
  - Невозможно фильтровать тысячи серверов по IP
  - Можно переместить сервис на другой IP, и попросить провайдера блокировать трафик к старому IP
- Избегайте принимать участие в атаке
  - Фильтрование входа/выхода (IETF BCP 38)
  - Ограничение доступа к рекурсивным серверам
    - Однако, авторитетные сервера могут продолжать быть использованными в атаках
- Что нам НЕ следует делать
  - Ограничивать размер пакетов DNS (это ломает DNSSEC)

Отравление кэша

- Атакующий обманывает кэширующий сервер, так что тот запоминает неправильный фальшивый ответ
  - www.mybank.com -> 1.2.3.4
    - 1.2.3.4 – web-сервер атакующего, маскирующийся под ваш банк!
  - Одна успешная атака затрагивает многих (если не всех) пользователей

The Register®

Hardware Software Music & Media Networks **Security** Public Sector Business Science Od

Crime Malware Enterprise Security Spam ID

Print Retweet Facebook Alert

Cache-poisoning attack snares top Brazilian bank

Google Adsense spoofed

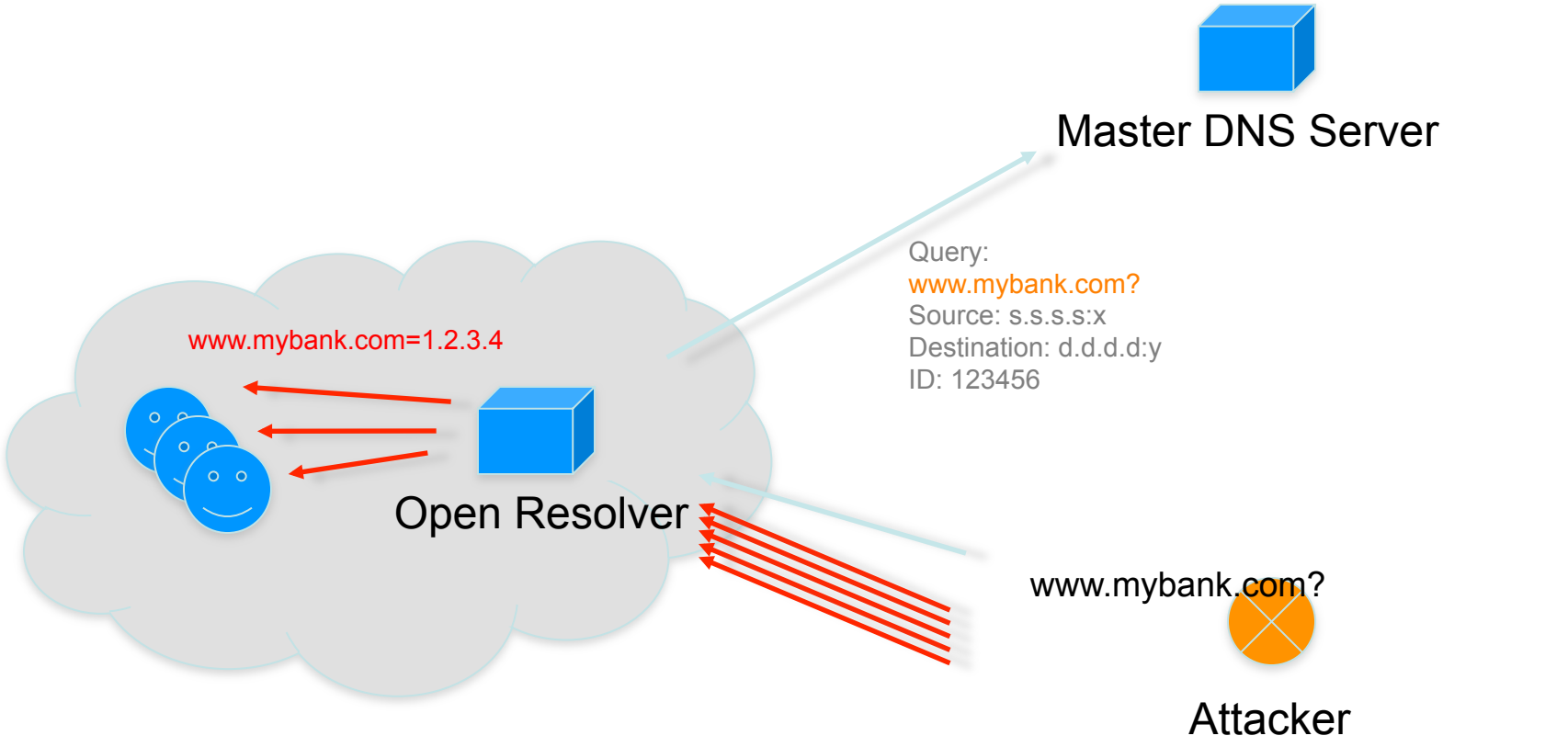
By **Dan Goodin in San Francisco** • **Get more from this author**

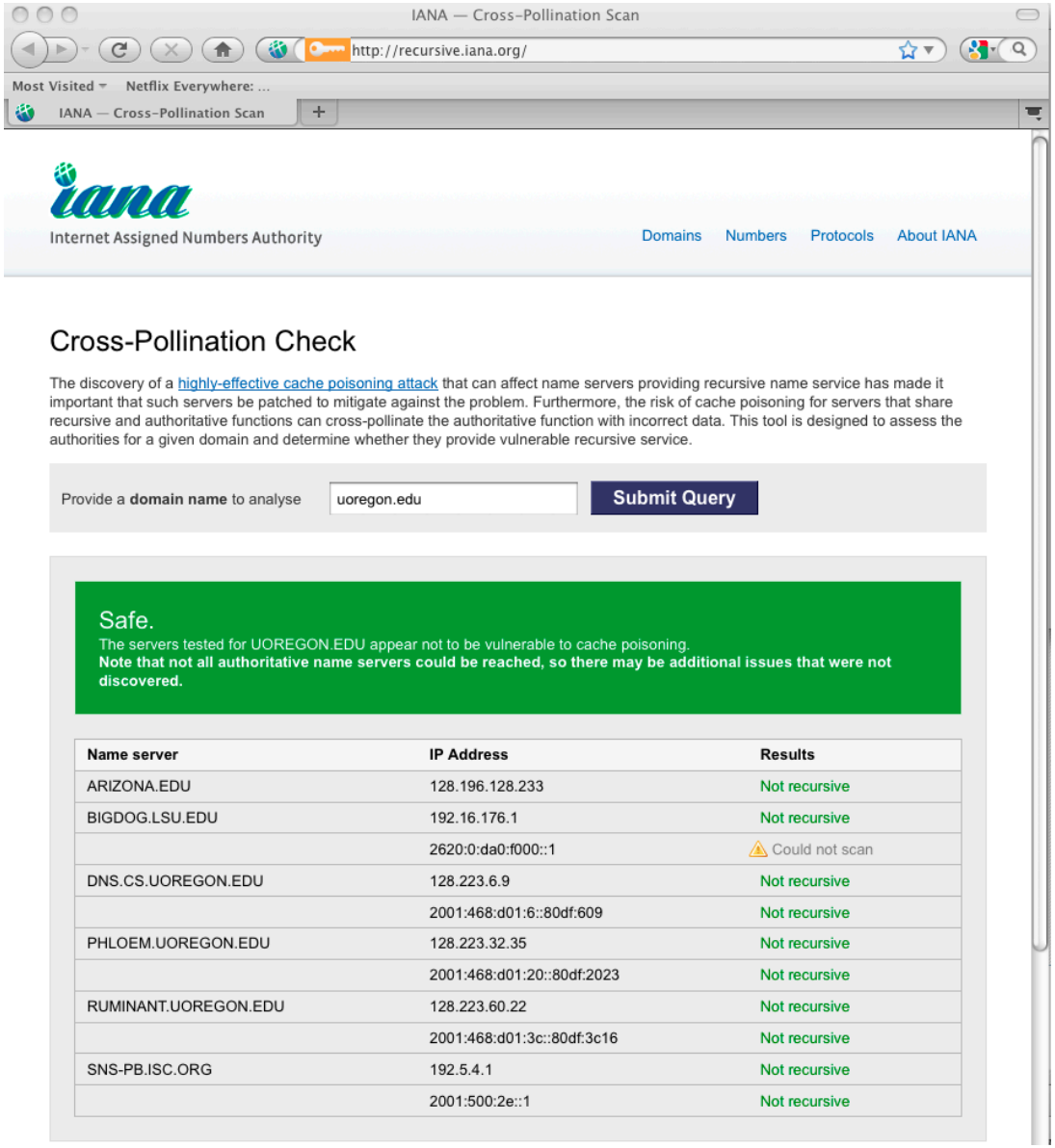
Posted in Crime, 22nd April 2009 00:32 GMT

One of Brazil's biggest banks has suffered an attack that redirected its customers to fraudulent websites that attempted to steal passwords and install malware, according to an unconfirmed report.

According to this Google translation of an article penned in Portuguese, the redirection of Bradesco was the result of what's known as a cache poisoning attack on Brazilian internet service provider NET Virtua.

Отравление кэша




IANA — Cross-Pollination Scan
http://recursive.iana.org/
Most Visited
Netflix Everywhere: ...
IANA — Cross-Pollination Scan
iana
Internet Assigned Numbers Authority
Domains
Numbers
Protocols
About IANA
Cross-Pollination Check
The discovery of a highly-effective cache poisoning attack that can affect name servers providing recursive name service has made it important that such servers be patched to mitigate against the problem. Furthermore, the risk of cache poisoning for servers that share recursive and authoritative functions can cross-pollinate the authoritative function with incorrect data. This tool is designed to assess the authorities for a given domain and determine whether they provide vulnerable recursive service.
Provide a domain name to analyse
uoregon.edu
Submit Query
Safe.
The servers tested for UOREGON.EDU appear not to be vulnerable to cache poisoning.
Note that not all authoritative name servers could be reached, so there may be additional issues that were not discovered.
Name server
IP Address
Results
ARIZONA.EDU
128.196.128.233
Not recursive
BIGDOG.LSU.EDU
192.16.176.1
Not recursive
2620:0:da0:f000::1
Could not scan
DNS.CS.UOREGON.EDU
128.223.6.9
Not recursive
2001:468:d01:6::80df:609
Not recursive
PHLOEM.UOREGON.EDU
128.223.32.35
Not recursive
2001:468:d01:20::80df:2023
Not recursive
RUMINANT.UOREGON.EDU
128.223.60.22
Not recursive
2001:468:d01:3c::80df:3c16
Not recursive
SNS-PB.ISC.ORG
192.5.4.1
Not recursive
2001:500:2e::1
Not recursive

Опасности скачивания зоны

- Скачивание зоны было придумано для распространения зоны между авторитетными серверами
- Скачивания довольно дороги в смысле потребляемых ресурсов
  - Могут быть использованы в атаках DoS
- Если у взломщика есть вся ваша зона целиком, это сильно упрощает его работу:
  - Ему не надо сканировать вашу сеть
  - Он лучше понимает структуру вашей сети

Авторитетный и рекурсивный

Функия	Информация	Целевая аудитория
Авторитетный	Ваши домены	Интернет
Рекурсивный	Все прочие домены	Ваши пользователи

Разделение труда

- Физическое разделение авторитетных и рекурсивных серверов дает вам:
  - Более простое управление
    - Применяйте ограничения, для чего и кем могут использоваться разные сервера
  - Более простую отладку
    - Рассмотрите ситуацию, в которой ваш клиент, зону которого вы обслуживаете, меняет провайдера зоны и не говорит вам об этом

Авторитетный – опции BIND

```
options {
   version "9999.9.9”;
   allow-transfer { peers; };
   blackhole { attackers; };
   recursion no;
   allow-query { any; };
   …
};
```

Авторитетный – фильтры IP

- Тут особо нечего фильтровать
  - Порты udp/53 и tcp/53 должны быть открыты для всего мира.
- Просто не гоняйте никаких других сервисов на этой машине
  - Ни web-сервера, ни почтового сервер, и т.д.
  - Сделайте его по настоящему простым

Авторитетный - расположение

- Располагайте ваши сервера топологически и географически разнесенными
  - Договоритесь с другим оператором, или
  - Есть компании, предлагающие вторичный сервис
  - Попросите поддержку anycasta, DNSSEC и IPv6!
  - Смотрите RFC 2182

Рекурсивный – опции BIND

```
options {
   version "9999.9.9”;
   recursive-clients 5000;
   allow-transfer { none; };
   blackhole { attackers; };
   allow-recursion { customers; };
   allow-query { customers; };
   dnssec-enable yes;
   dnssec-validation yes;
   …
};
```

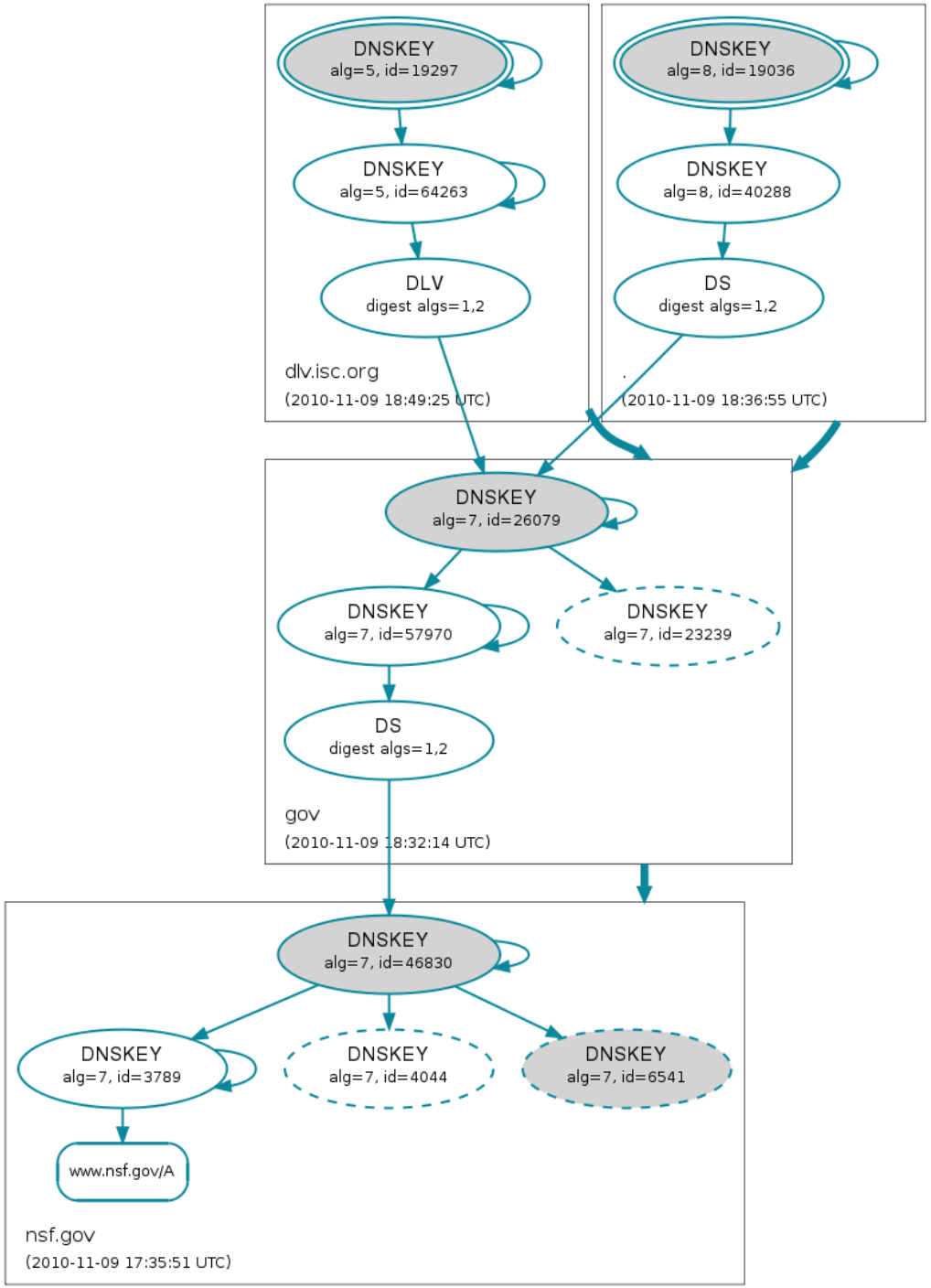
Рекурсивный – фильтры IP

- udp/53 и tcp/53 открыты только для клиентов
  - Блокируйте пакеты сразу по получении, не допускайте их до демона DNS
  - Не забудьте фильтровать и IPv6, если он настроен
  - Может быть просто сделано, используя
    - iptables на Linux
    - ipfw на FreeBSD

Валидация DNSSEC

- Корневая зона теперь подписана!
- Единственный правильный способ избежать отравления кэша
- DNSSEC начал использоваться университетами и исследовательскими организациями, крупные провайдеры тоже стали присоединяться:
  - http://www.dnssec.comcast.net/

Источник:
dnsviz.net



Валидация DNSSEC

```
 options {
    dnssec-enable yes;
    dnssec-validation yes;
}


managed-keys {
"." initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR
+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/
RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/
VHL496M/QZxkjf5/
Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQ
pzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA
+Uk1ihz0=";
};
```

DNSSEC: следствия, относящиеся к размеру пакетов

- Ответы легко превышают старый максимум (512 байт по UDP)
- Два решения:
  - Использование EDNS0: клиент дает знать, что он поддерживает UDP пакеты большего размера
  - Использование TCP
- В обоих случаях, убедитесь что все звенья пути между клиентами и DNS-серверами это поддерживают
  - Обратите внимание на конфигурацию брандмауэров (файерволов)

Отказоустойчивость для клиентов

- Клиенты авторитеных серверов (другие рекурсивные сервера)
  - Хорошо переключаются между серверами используя несколько записей NS
- Клиенты рекурсивных серверов (системы разрешения имен)
  - Плохо переключаются между серверами
  - Пользователи сразу жалуются
  - Сервисы перестают работать из-за таймаутов

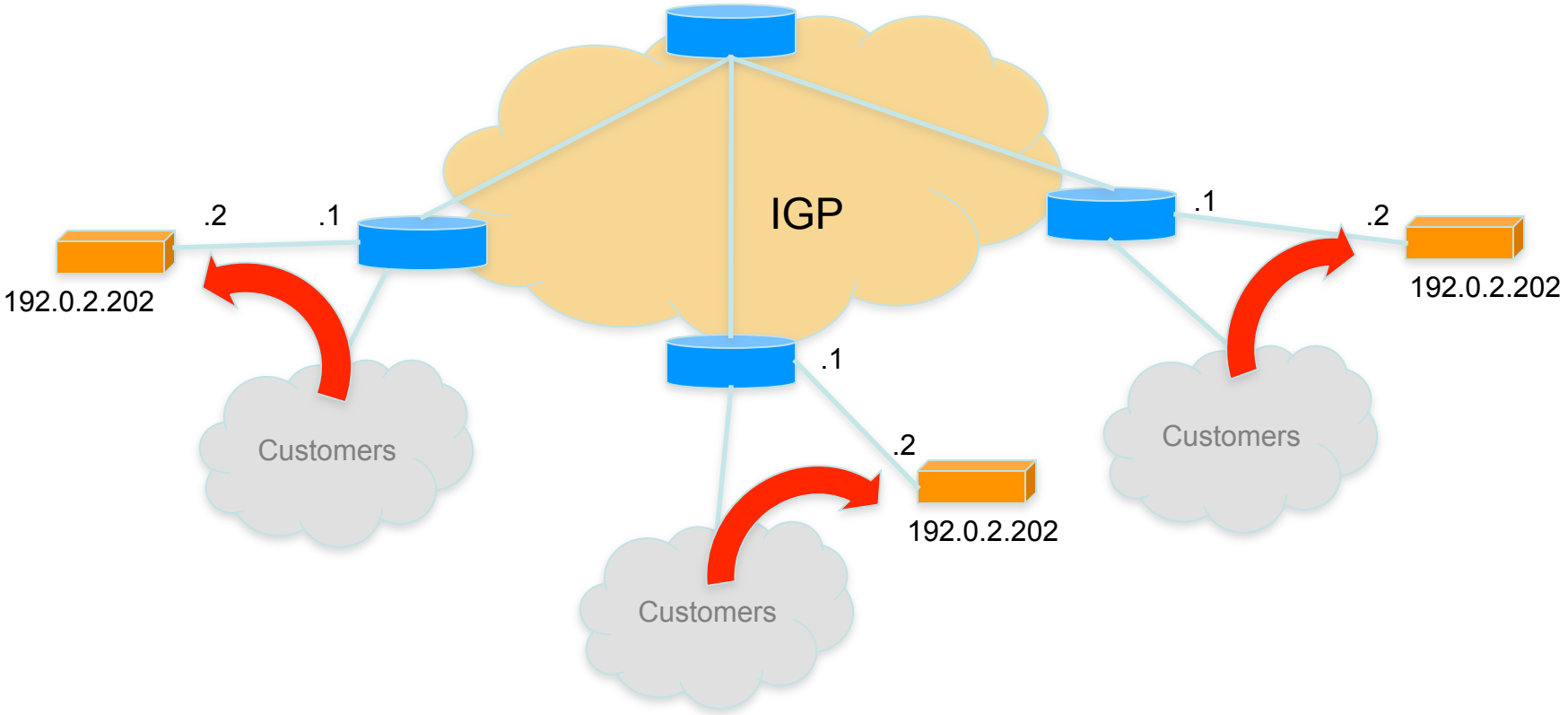
Anycast

- Один и тот же IP адрес анонсируется несколькими роутерами таким образом, что отправитель запроса достигает топологически ближайшей машины, отвечающей по этому адресу
- Прекрасное решение для улучшения DNS:
  - Балансировка
  - Отказоустойчивость
  - Изолирование атак DoS
  - Изолирование отравленных кэшей

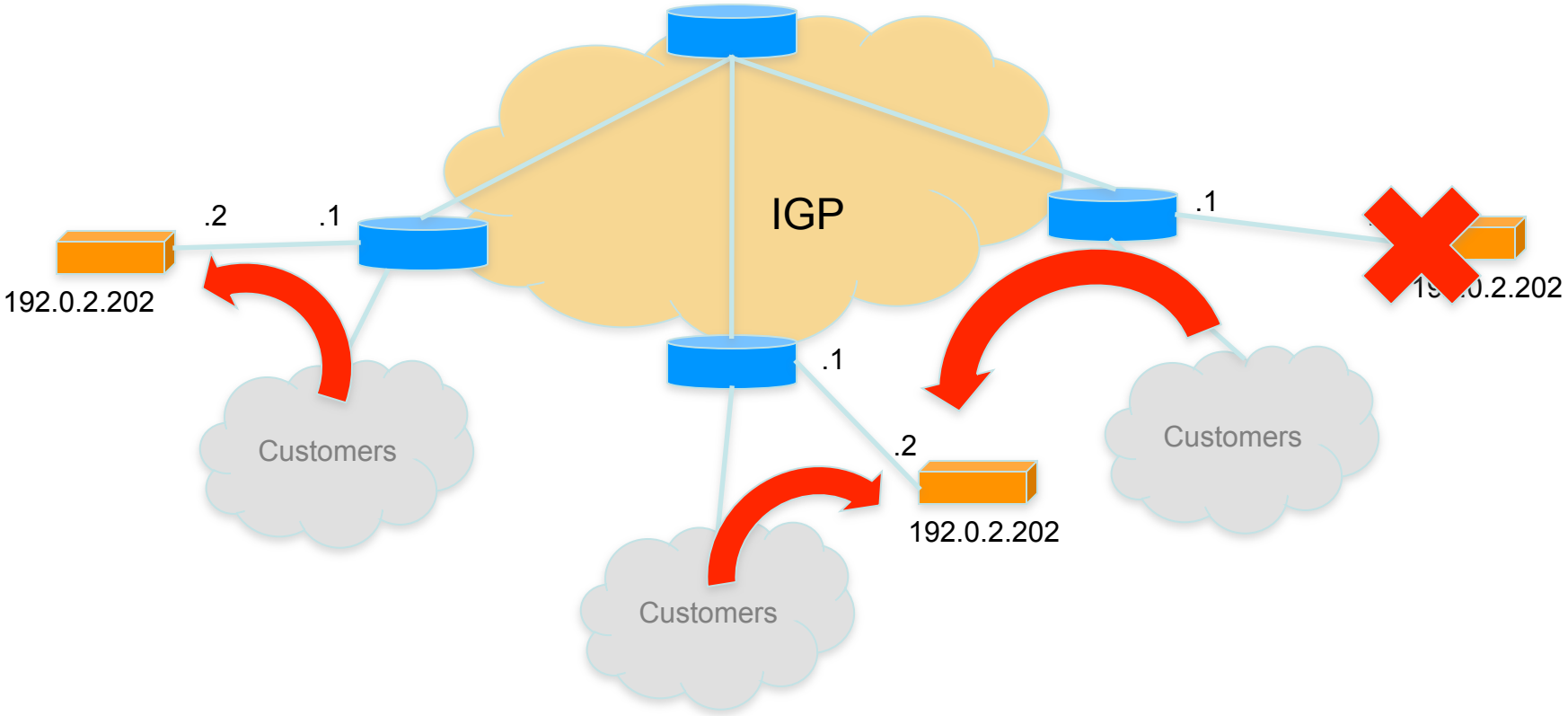
Anycast DNS

- Два подхода
  - Гонять демон роутинга на DNS-сервере
    - Zebra, и т.д.
    - Анонсирование префиксов должно быть связано с запуском и остановкой DNS-сервиса и его авариями
  - Использовать IP SLA с роутерами Cisco
    - Проверьте, что сервис работает, прежде чем вставлять префикс в роутинговый домен
    - Нет необходимости доверять вашим сисадминам процедуру вставки маршрута в ваш роутинговый домен ;-)
    - Конфигурация сервера становится проще

Топология anycast



Топология anycast



Anycast DNS – Cisco IP SLA

```
ip sla 1
 dns www.mydomain.com name-server 192.0.2.202
 timeout 500
 frequency 10
ip sla schedule 1 life forever start-time now

track 1 ip sla 1
ip route 192.0.2.100 255.255.255.255 192.0.2.200 track 1 tag 999

route-map V4-STATIC permit 10
 match tag 999

router isis mynet
 redistribute static ip metric 100 route-map V4-STATIC level-1
```

Anycast – серверные интерфейсы

```
eth0      Link encap:Ethernet  HWaddr F0:4D:A2:01:65:42
          inet addr:192.0.2.202  Bcast:192.0.2.203  Mask:255.255.255.252

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0

lo:1      Link encap:Local Loopback
          inet addr:192.0.2.100  Mask:255.255.255.255
```

Управление конфигурацией

- Храните файлы зон и конфигурации в системе контроля версий
  - *SVN*, *Git*, *и т.д.*
- Генерируйте файлы зон, вместо того чтобы редактировать их вручную
  - *http://netdot.uoregon.edu*
  - *http://www.nictool.com/info/*
  - *http://www.debianadmin.com/bind-dns-server-web-interfacefrontend-or-gui-tools.html*
- Используйте программы управления конфигурацией для распространения этих файлов, перезапуска сервисов и т.д.
  - *Puppet*, *CFEngine*, и т.д.
  - Запускайте проверку синтаксиса перед загрузкой

```
named-checkzone mydomain.com zonefile
```

Используйте разные ОС и DNS программы

- Рассмотрите возможность использование нескольких разных DNS программ (Bind, Unbound, NSD, и т.д.) на разных операционных системах
  - Защищает от полной катастрофы при обнаружении критической ошибки в софте, однако...
  - Управление конфигурацие усложняется

Регулярные проверки зоны

- Периодически запускайте проверки на
  - Противоречивые, отсутствующие либо плохие данные
  - Вылавливание часто встречающихся ошибок конфигурации
  - RFC 1912
- Попробуйте dnscheck
  - https://github.com/dotse/dnscheck

Наблюдайте за логами

- Используйте программу анализа логов DNS и поднимайте тревогу в случае важных сообщений
  - Swatch, Tenshi, и т.д.
  - Отслеживайте:
    - Синтаксические ошибки в зонах
    - Проблемы скачивания
    - Ошибки валидации DNSSEC
    - и т.д.

Отслеживание доступности – Nagios

- Используйте *check_dns* для того, чтобы быть уверенным в том, что сервер и в самом деле отвечает на запросы
  - Просто пинг сервера недостаточен
- Его можно использовать и для проверки того, что важные записи типа A присутствуют:
  - www, smtp, imap,…
- Убедитесь, что тревога поднимается правильно даже если DNS не работает!

Отслеживание доступности – Nagios

Service 'DNS' On Host 'ns1'

01-01-2010 00:00:00 to 11-07-2010 21:08:40
Duration: 310d 21h 8m 40s

[Availability report completed in 0 min 16 sec]

Service State Breakdowns:

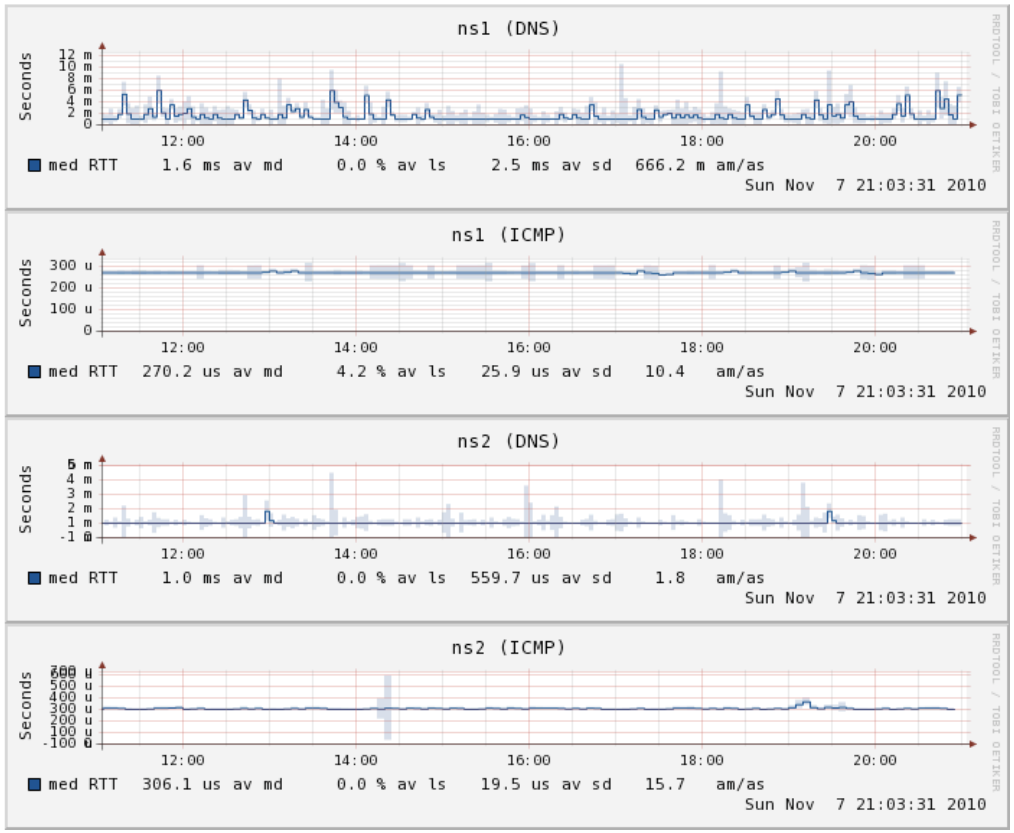
State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	90d 22h 8m 40s	29.247%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**90d 22h 8m 40s**	**29.247%**	**100.000%**
WARNING	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
UNKNOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
CRITICAL	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	219d 23h 0m 0s	70.753%	
	Total	219d 23h 0m 0s	70.753%	
All	Total	310d 21h 8m 40s	100.000%	100.000%

Отслеживание задержек

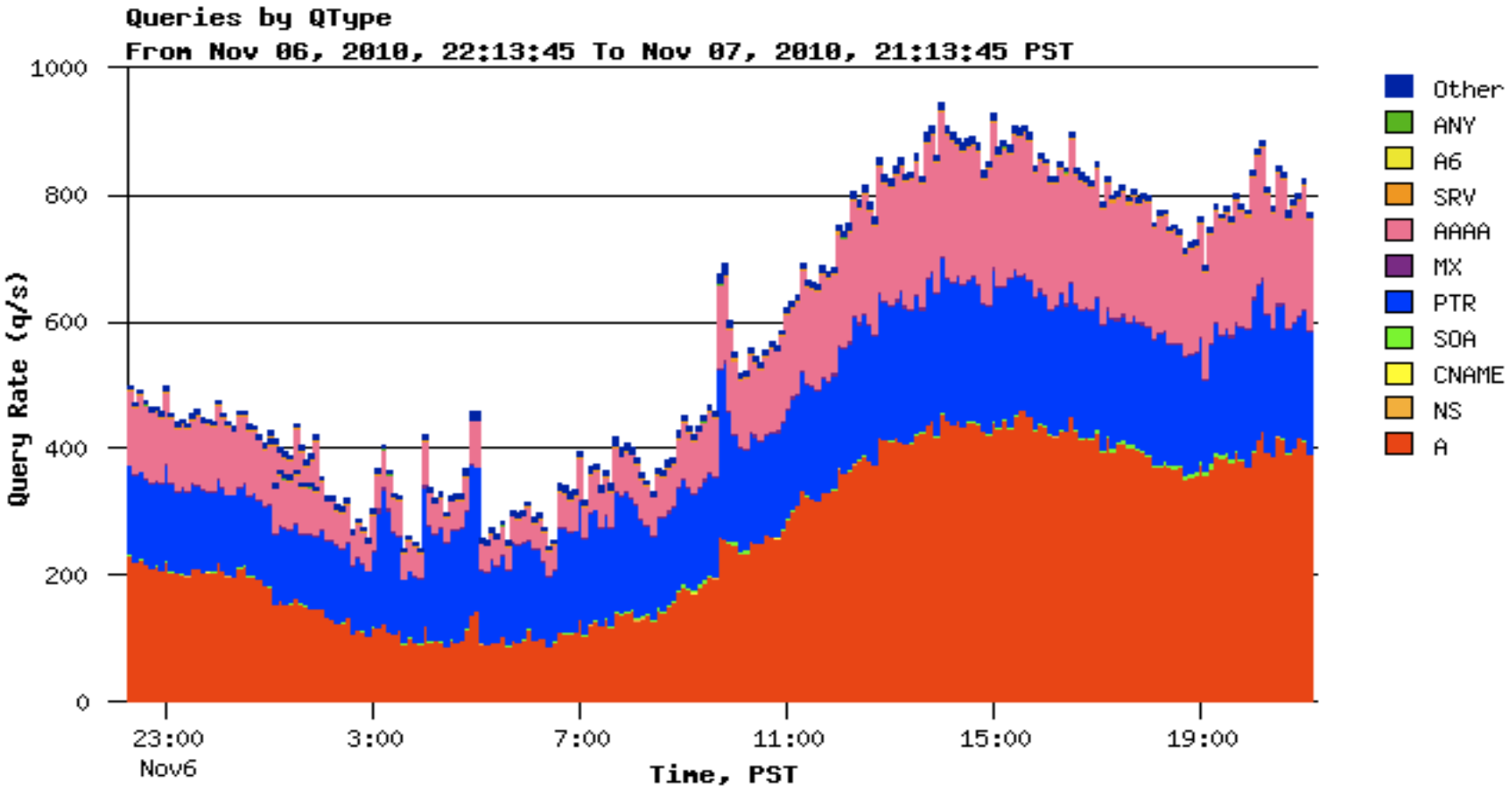
- Важно смотреть за
  - Задержками в сети
  - Задержками DNS сервиса

Отслеживание задержек - Smokeping

Recursive



Статистика запросов - DSC



Вопросы?

- Спасибо