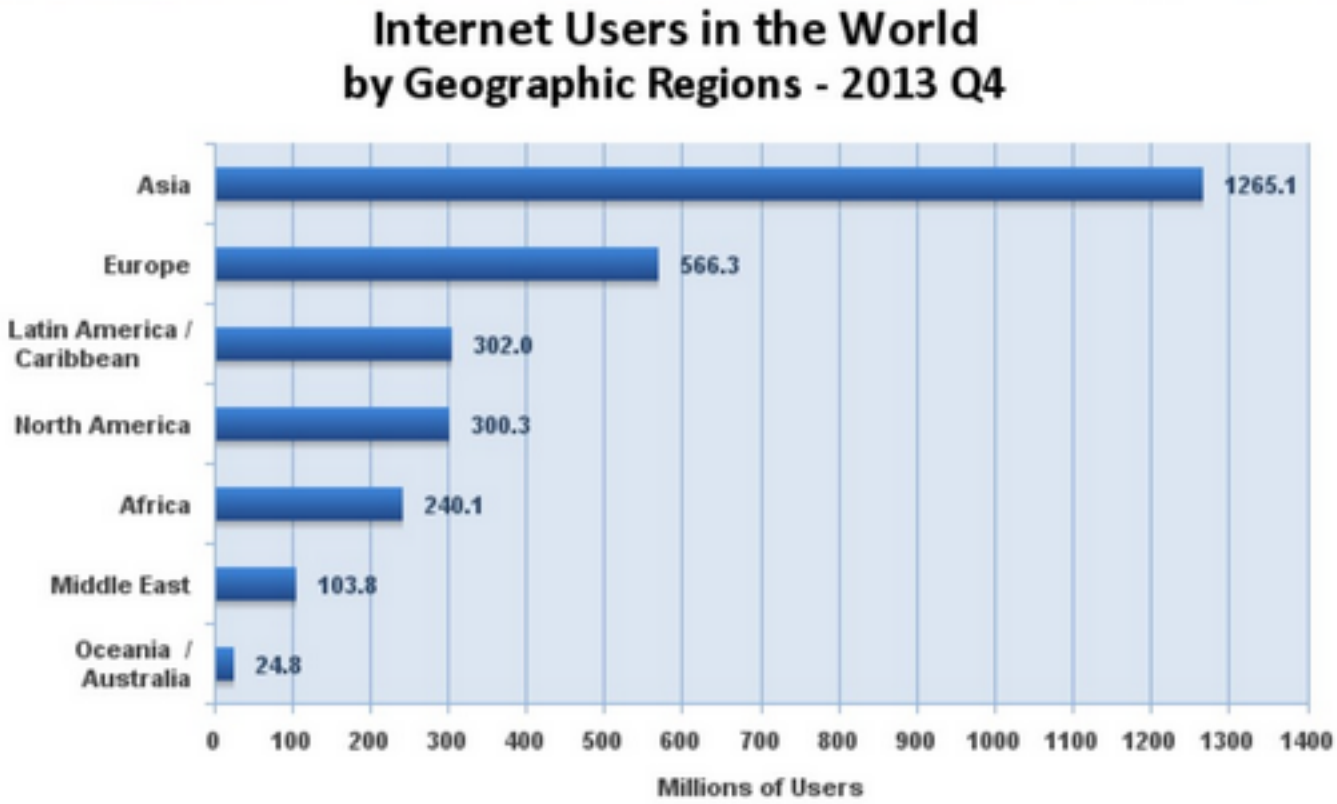
СЕТЕВАЯ БЕЗОПАСНОСТЬ МАГИСТРАЛЬНЫХ КАНАЛОВ

ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЬНЫХ СЕТЯХ

Мировая статистика



Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,802,478,934 Internet users estimated for December 31, 2013

Атаки бывают следующих классов:

- базирующиеся на дефектах протоколов, например, TCP, SMTP, HTTP или DNS;

- использующие дефекты операционной системы;

- поиск и использование слабых мест программ-приложений, включая базы данных, APACHE, а также скриптов, например, CGI;

- эксплуатирующие человеческие слабости (любопытство, алчность и пр., например, троянские кони, spyware);

- особую группу (частично перекрывающуюся с предшествующим пунктом) составляют вирусы, сетевые черви и пр..

ИНСТРУМЕНТАРИЙ ОБНАРУЖЕНИЯ И БОРЬБЫ С АТАКАМИ

IDS, IPS СИСТЕМЫ

- Система обнаружения вторжений (англ. Intrusion Detection System, IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть.

- Система предотвращения вторжений (англ. Intrusion Prevention System, IPS) —система, обнаруживающая вторжения и автоматически защищающая от них.

- Система контроля угроз (англ. Unified Threat Management, UTM). Содержат FireWall, IDS/IPS, антивирус, прокси-сервер, контентный фильтр, антиспам.

МЕТОДЫ IDS/IPS СИСТЕМ. RBID

- RBID-системы (англ. Rule-Based Intrusion Detection).

- Сигнатуры весьма разнообразны и могут определять конкретные параметры от номера порта в пакете до последовательности байт в серии пакетов.

- После того, как сигнатура разработана, её использование обычно довольно эффективно предотвращает нежелательную сетевую активность.

- Временной лаг между созданием нового типа атаки и сигнатуры. Время на внедрение сигнатуры.

МЕТОДЫ IDS/IPS СИСТЕМ. SBID

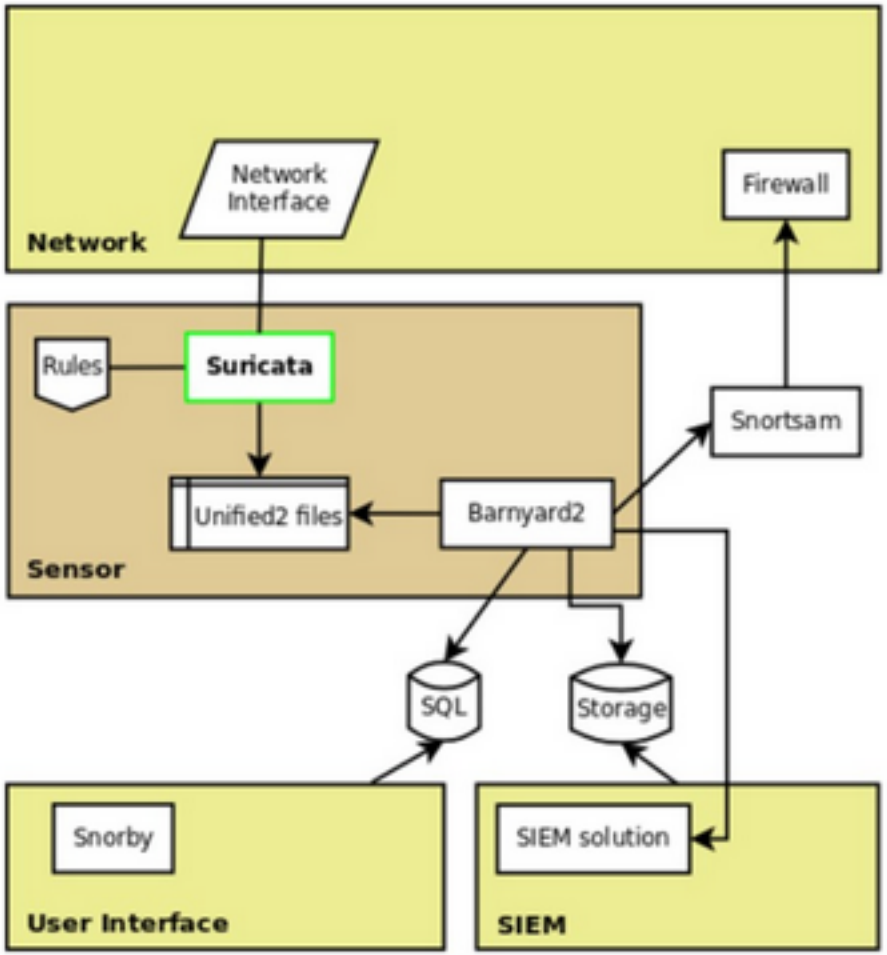
- Статистические системы (SBID)
- Концепция SBID: система определяет «нормальную» сетевую активность и затем весь трафик, не подпадающий под определение «нормального», помечается как аномальный
- Сравнительно высокий уровень ложных срабатываний
- Значительно более наукоемкая разработка

Martin Roesch, 1998г
Система предупреждения и обнаружения сетевых вторжений(NID(P)S)

- RBID-система
- Однопоточный режим
- Блокировка производится средствами штатного пакетного фильтра ОС
- Автоматически определяет и сканирует протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP

- RBID-система
- Многопоточный режим (тестирование на системе 24 CPU и 128 ГБ)
- Аппаратная акселерация на стороне GPU за счет CUDA
- Блокировка производится средствами штатного пакетного фильтра ОС
- Автоматически определяет и сканирует протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP
- Есть возможность подключать наборы правил, созданные другими проектами (SourcefireVRT, OpenSource Emerging Threats и Emerging Threats Pro)
- Встроенные счетчики применяются для детектирования попыток подбора пароля
- Планируется появление механизма IP Reputation

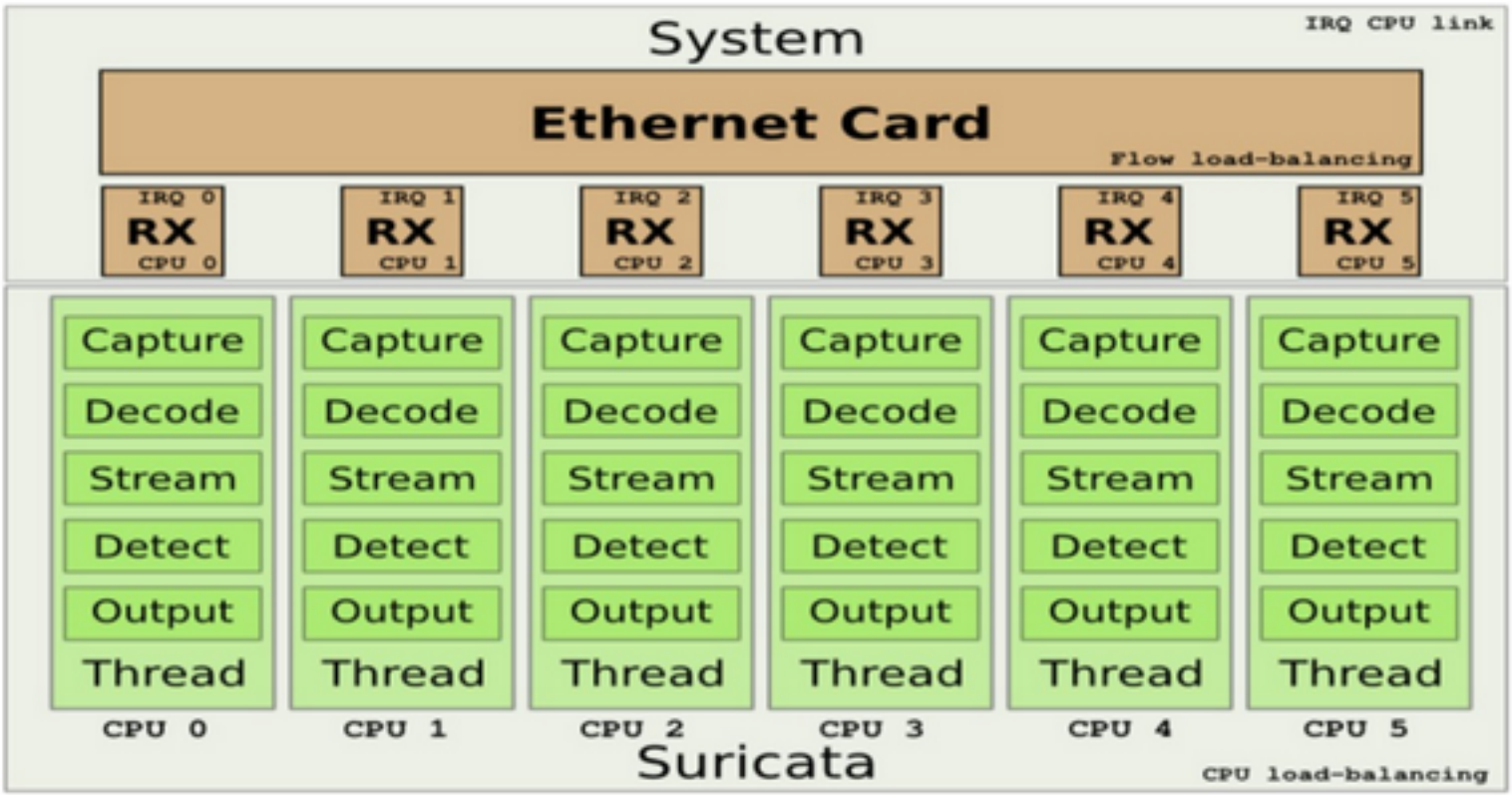
ЭКОСИСТЕМА IPS SURICATA



- ☐ Checkpoint Firewall-1
- ☐ Cisco PIX firewalls
- ☐ Cisco Routers (using ACL's or Null-Routes)
- ☐ Former Netscreen, now Juniper firewalls
- ☐ FreeBSD ipfw2
- ☐ OpenBSD Packet Filter (pf)
- ☐ Linux IPchains
- ☐ Linux IPtables
- ☐ Linux EBtables
- ☐ WatchGuard Firebox firewalls
- ☐ 8signs firewalls for Windows
- ☐ MS ISA Server firewall/proxy for Windows
- ☐ Ali Basel's Tracker SNMP through the SNMP-Interface-down plugin
- ☐ CHX packet filter

АППАРАТНАЯ ПЛАТФОРМА ДЛЯ IDS SURICATA

- CPU: One Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz (16 cores)
- Memory: 32GB
- capture NIC: Intel 82599EB 10-Gigabit SFP+



= 1Mpps!

РЕФЛЕКТОРНАЯ АТАКА

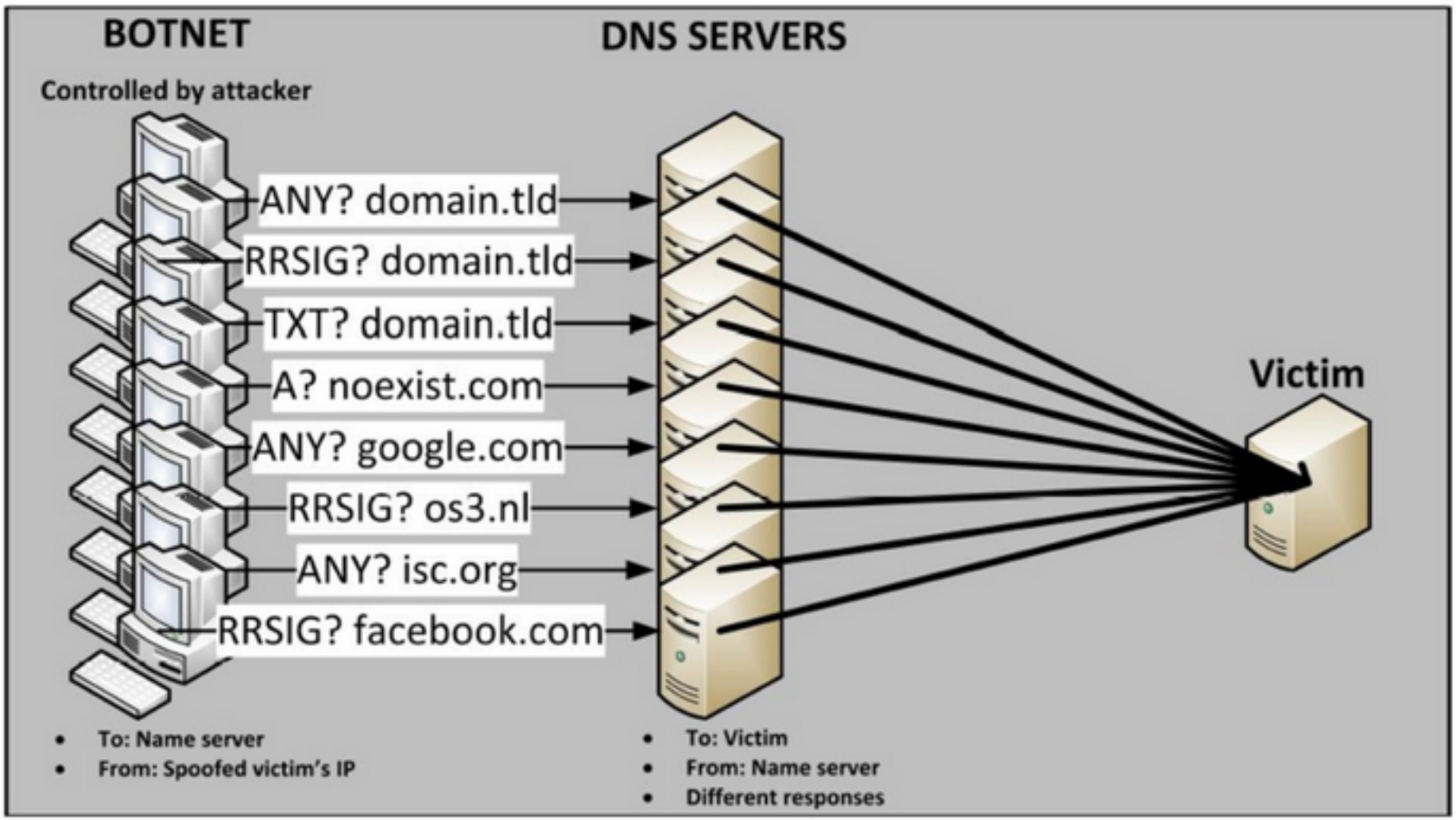
СУТЬ РЕФЛЕКТОРНОЙ АТАКИ

- Использование протокола UDP или ICMP, обеспечивающего передачу дейтаграмм без создания соединения(SNM,DNS). Ключевым фактором является отсутствие необходимости устанавливать соединение, что открывает возможность для спуфинга - подмены IP-адреса отправителя на адрес "жертвы".
- Рефлекторы. Поскольку режимом работы многих услуг, основанных на протоколе UDP, является "запрос-ответ", при подмене адреса отправителя на адрес "жертвы", ответ на запрос будет доставлен именно "жертве".
- Усилители. Для таких услуг как DNS и SNMP зачастую размер ответа во много раз превышает размер запроса.
- Ботнеты. Для эффективных атак такого рода необходима хорошо распределенная сеть источников. Инфицированные компьютеры, объединенные в ботнеты, являются для этого прекрасной стартовой площадкой.

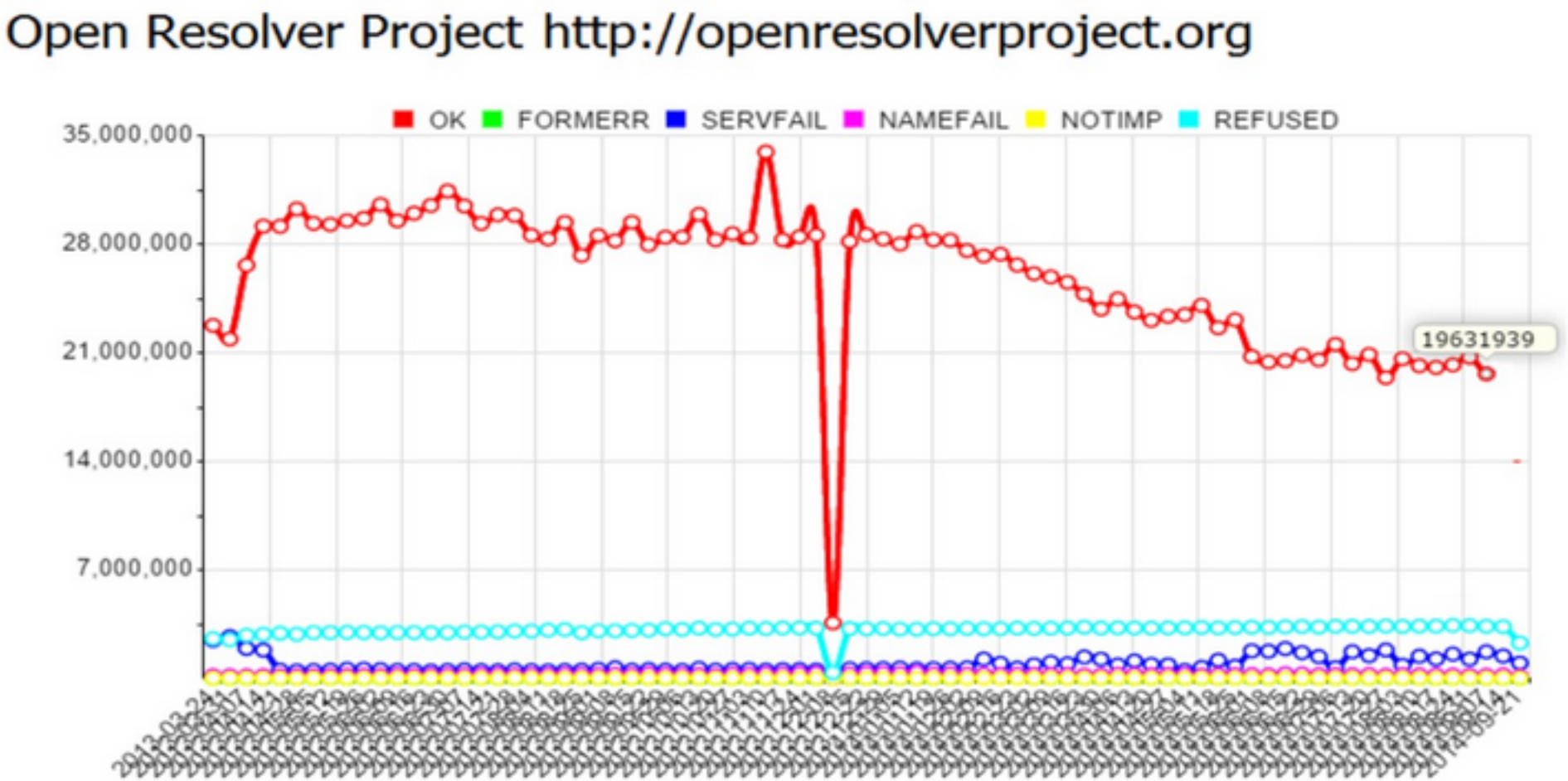
ПРИМЕР УСИЛЕНИЯ

```
[melkin@zabbix ~]$ dig +dnssec gov.ua. ANY
;; ANSWER SECTION:
gov.ua.                 86400   IN      SOA     ho1.ns.gov.ua. admin.nic.gov.ua. 2008036880 28800 7200 604800 86400
gov.ua.                 47734   IN      NS      ho1.ns.gov.ua.
gov.ua.                 47734   IN      NS      ba1.ns.ua.
gov.ua.                 47734   IN      NS      sns-pb.isc.org.
gov.ua.                 47734   IN      NS      ua.cctld.authdns.ripe.net.
gov.ua.                 47734   IN      NS      nix.ns.ua.
;; AUTHORITY SECTION:
gov.ua.                 47734   IN      NS      nix.ns.ua.
gov.ua.                 47734   IN      NS      ba1.ns.ua.
gov.ua.                 47734   IN      NS      ua.cctld.authdns.ripe.net.
gov.ua.                 47734   IN      NS      sns-pb.isc.org.
gov.ua.                 47734   IN      NS      ho1.ns.gov.ua.
;; ADDITIONAL SECTION:
ba1.ns.ua.              35186   IN      A       74.123.224.37
ba1.ns.ua.              6132    IN      AAAA    2604:ee00:0:101::37
ho1.ns.gov.ua.          32046   IN      A       195.47.253.4
ho1.ns.gov.ua.          32046   IN      AAAA    2001:67c:258::4
nix.ns.ua.              42605   IN      A       62.149.7.77
nix.ns.ua.              30187   IN      AAAA    2a03:6300:1:102::3
...
...
...
;; Query time: 2 msec
;; SERVER: 212.111.192.35#53(212.111.192.35)
;; WHEN: Sat Sep 27 16:12:58 2014
;; MSG SIZE  rcvd: 1436
```

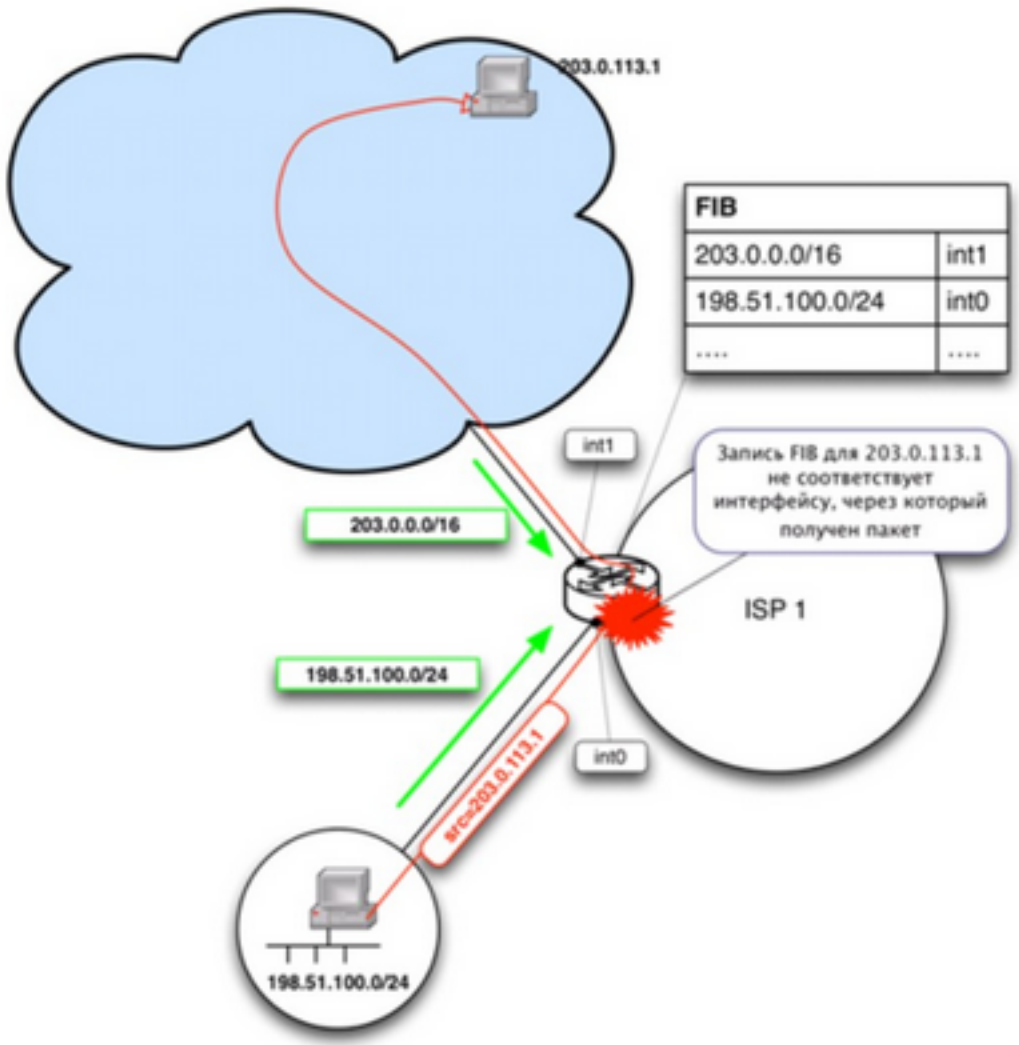
СХЕМА РЕФЛЕКТОРНОЙ АТАКИ



ОТКРЫТЫЕ РЕЗОЛВЕРЫ



ПРОФИЛАКТИКА СПУФИНГА. uRPF



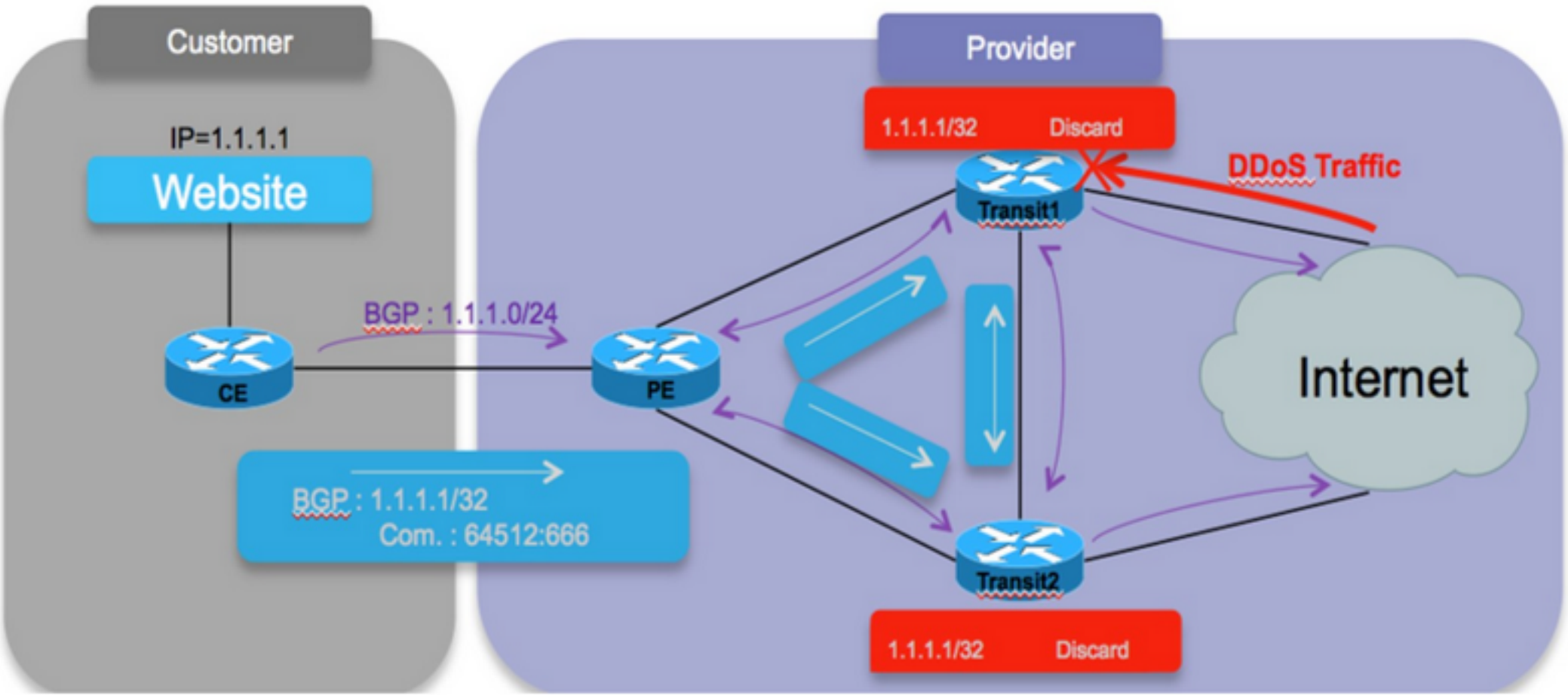
ПРОФИЛАКТИКА СПУФИНГА. BIND RESPONSE RATE LIMIT

- RRL присутствует в версиях ISC BIND начиная с версии 9.9.4
- Параметр SLIP как много UDP запросов могут быть отвечены с установленным флагом TI(truncate indicator)
- Параметр WINDOW определяет интервал для расчета порога идентичных ответов
- Параметр Response-per-second определяет допустимое колл-во идентичных запросов из одной подсети.

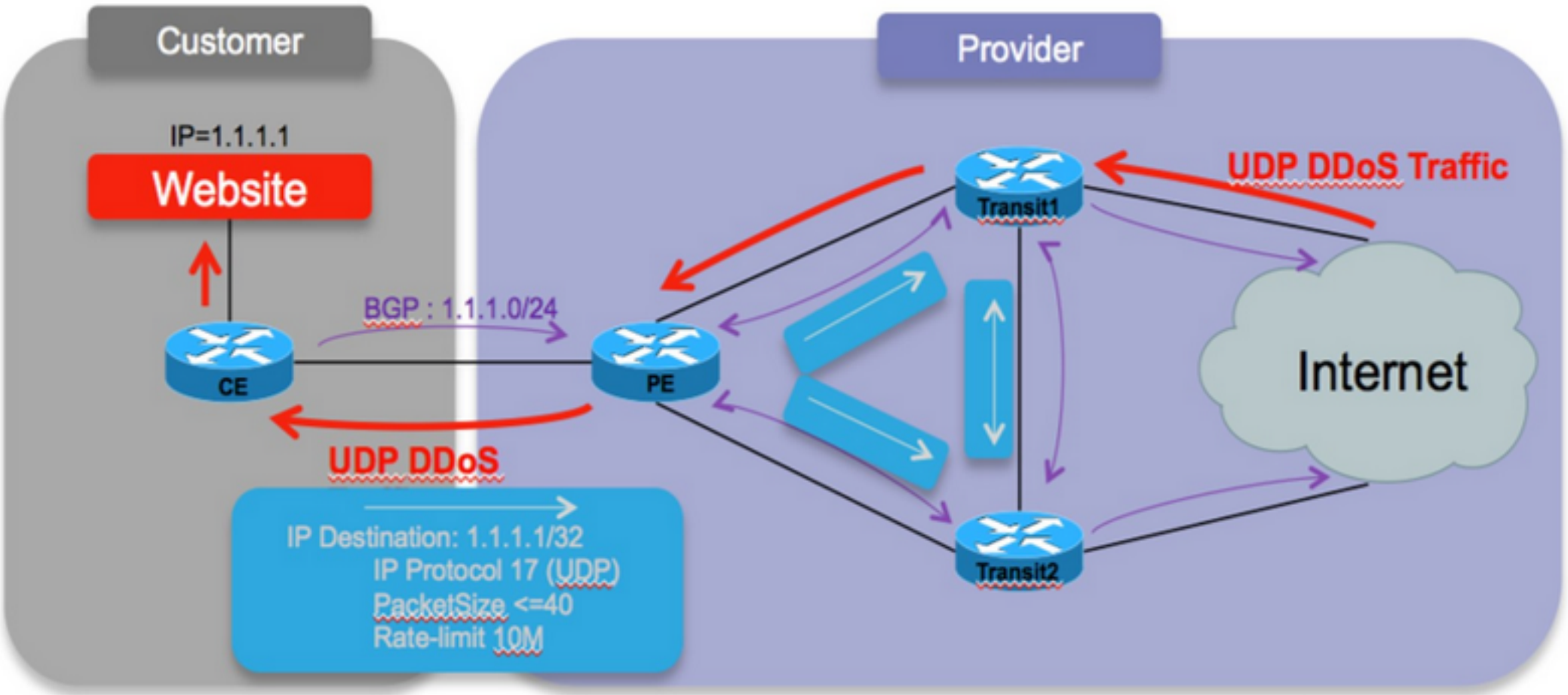
```
rate-limit {
        slip 2;                         // Every other response truncated
        window 15;                      // Seconds to bucket
        responses-per-second 5;// # of good responses per prefix-
length/sec
```

МЕТОДЫ ЗАЩИТЫ

REMOTELY TRIGGERED BLACK HOLE(RTBH)



КОНЦЕПЦИЯ FLOWSPEC



RFC5575 FLOW SPECIFICATION RULES

1. Source Prefix (unique)
2. Destination Prefix (unique)
3. IP Protocol (multiple)
4. Port (multiple)
5. Destination Port (multiple)
6. Source Port (multiple)
7. ICMP Type
8. ICMP code
9. TCP Flags
10. Packet length
11. DSCP
12. Fragment

RFC5575 – TRAFFIC FILTERING ACTIONS

Type	Description	Encoding
0x8006	traffic-rate	2 bytes ASN ; 4 Bytes as float
0x8007	traffic-action	bitmask
0x8008	redirect	6 bytes Route Target
0x8009	traffic-marking	DSCP Value

ВЫВОДЫ

Какие типы атак наиболее разрушительны и трудно устранимы на магистральном, провайдеровском уровне?

Какими инструментами и методами можно детектировать атаки и противостоять им?

1. Понимание механизма атаки
2. Использование OpenSource IDS SURICATA
3. Использование модуля ответной реакции SNORTSAM
4. Профилактика спуфинга – uRPF, BIND RRL
5. Защита от рефлекторной атаки методом REMOTELY TRIGGERED BLACK HOLE
6. Возможность рекурсивного применения метода RTBH
7. Перспективное направление – BGP FLOWSPEC
8. Перспективное направление – SBID (например обработка NETFLOW)

ВОПРОСЫ?

Евгений Преображенский

Sub: IT Arena Lviv

eugene.melkin@gmail.com