ARBOR NETWORKS

Эволюция DDoS глазами оператора связи

Кирилл Касавченко
Инженер-консультант
kkasavchenko@arbor.net

Содержание

1. Анализ DDoS атак в мире и их особенностей в 2011 году
2. Правильные и неправильные методы защиты от DDoS атак
3. Рекомендации по организации безопасности сетевой инфраструктуры оператора

DDoS атаки – норма в глобальной сети

- Происходят круглосуточно: 24x7x365
- Разнообразная мотивация
  - Финансовая мотивация, криминальная деятельность, идеологические причины... или отсутствие мотивации
- Могут затронуть любого оператора
- Обычно операторов не интересуют исходящие атаки
  - Исключение – сети мобильной связи
- Могут сопровождаться значительным дополнительным ущербом для оператора связи

DDoS и ботнеты – внешняя угроза

- Применения ботнетов:
  - DDoS
  - Спам
  - Мошенничество
  - Шпионаж
  - Воровство

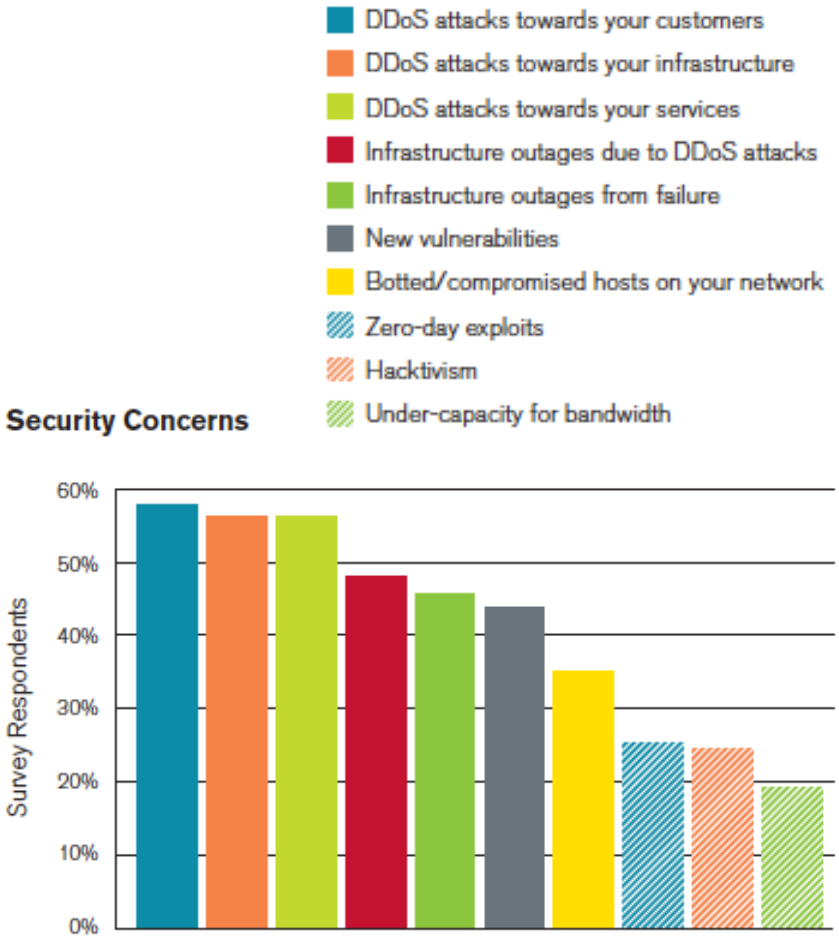


Figure 9 *Source: Arbor Networks, Inc.*

DDoS атаки в 2011 году

- Сильный рост атак с идеологической мотивацией
- 10 Гбит/с – вполне обычный объем для flood атаки
- Все больше атак уровня приложения и мультивекторных атак
- Первые атаки на IPv6 (но пока простые и редкие)

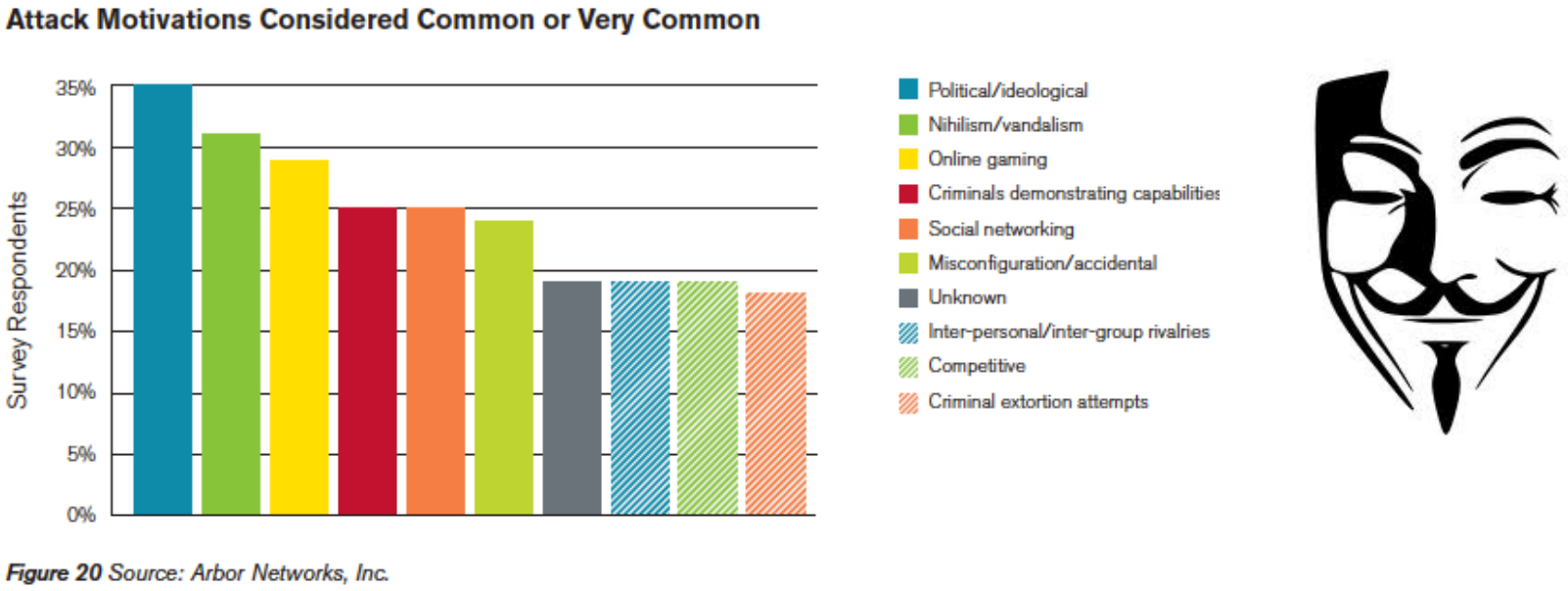


Figure 20 Source: Arbor Networks, Inc.

ARBOR NETWORKS

DDoS в СНГ и Восточной Европе

	2010		2011	
Страна	**В среднем**	**MAX**	**В среднем**	**MAX**
Украина	158.20Mbps / **334.35Kpps**	1.57Gbps / 4.573Mpps	349Mbps / 1Mpps	970Mbps / 2.82Mpps
Россия	339.63Mbps / 258.42Kpps	29.89Gbps / **6.86Mpps**	1.07Gbps / **1.596Mpps**	14.4Gbps/ **33.749Mpps**
Польша	220.43Mbps / **513.20Kpps**	5.73Gbps / **14.86Mpps**	339.89Mbps / 522.78Kpps	1.28Gbps / 1.56Mpps
Чехия	136.74Mbps / 314.69Kpps	912.44Mbps / 1.9Mpps	745.2Mbps / **2.36Mpps**	3.07Gbps / **8.91Mpps**
Венгрия	123.32Mbps / 252.39Kpps	1.81Gbps / 1.96Mpps	334.74Mbps / 676.88Kpps	1.57Gbps / 3.92Mpps
Румыния	113.00Mbps / 267.39Kpps	2.76Gbps / 5.94Mpps	602.69Mbps / 734.71Kpps	17.78Gbps / 6.40Mpps
Македония	341.58Mbps / 150.75Kpps	1.73Gbps / 275.1Kpps	1.762Gbps / 489.89Kpps	3.204Gbps / 1.08Mpps

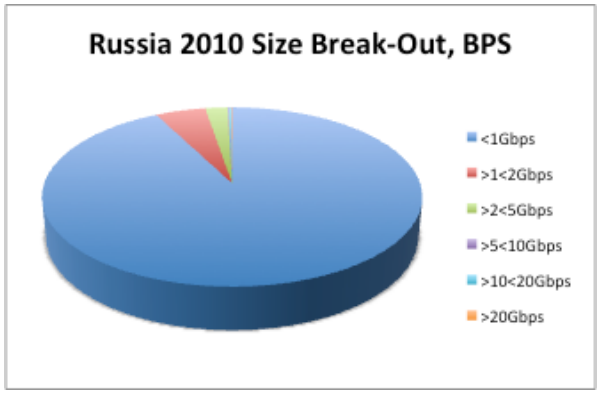
Статистика по РФ в 2011 году: Новая реальность «маленьких» атак

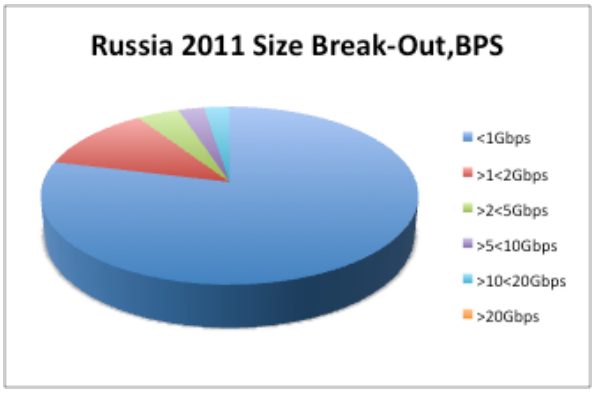
Доля атак > 1 Гбит/с:

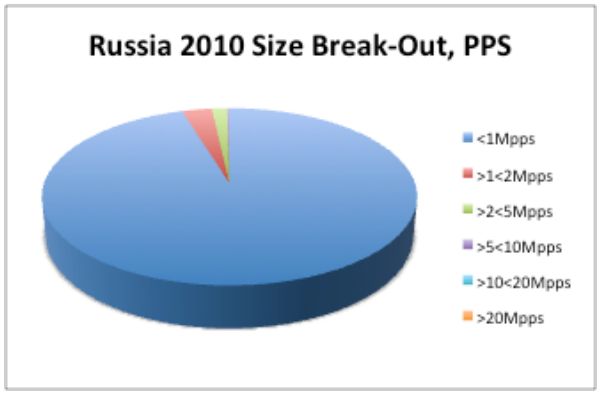
- 7.59% в 2010
- **21.19%** в 2011

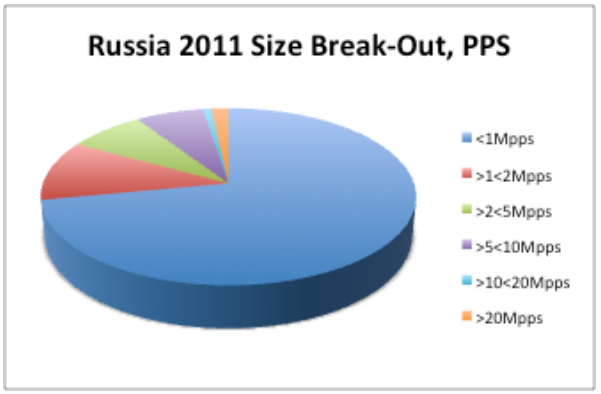
Доля атак > 1Мп/с

- 4.73% в 2010
- **27.97%** в 2011









ARBOR NETWORKS

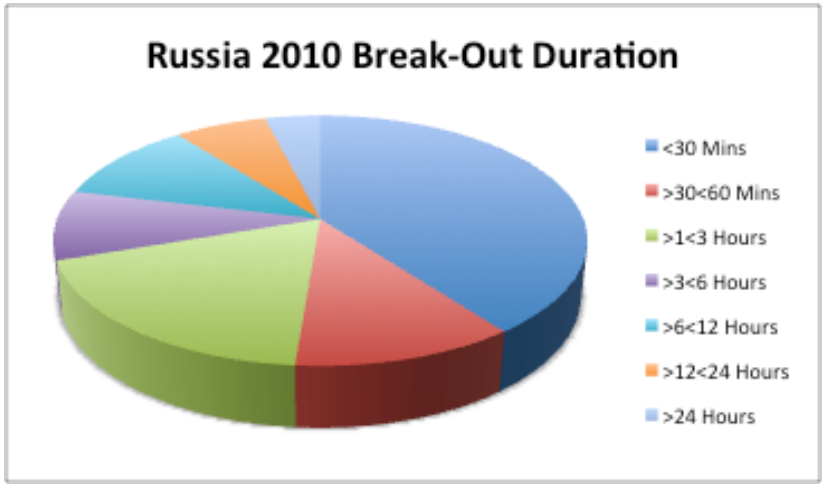
Статистика по РФ в 2011 году: Длительность атак больше средней в мире

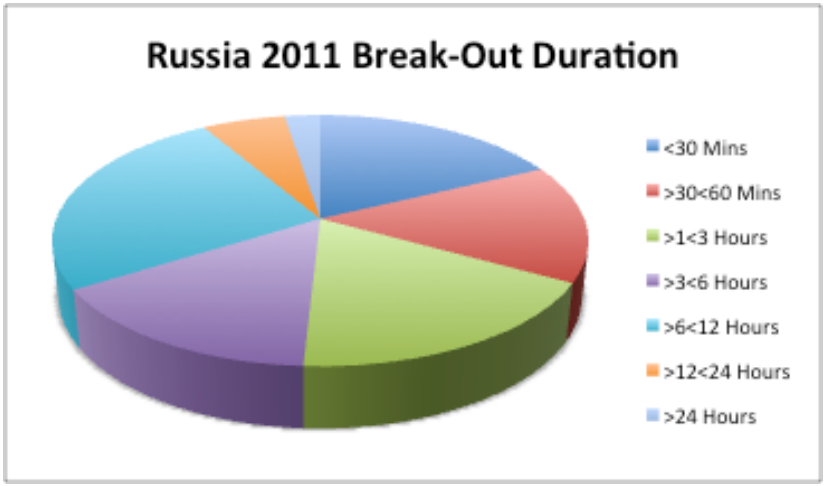
Средняя длительность в 2011:

- В мире:
  - 3 часа 27 минут
- В РФ:
  - 6 часов 17 минут

Доля атак > 12 часов почти не изменилась:

- 8.47% (2011)
- 10.56% (2010)
- Больше, чем в среднем в мире





ARBOR NETWORKS

Flood DDoS в 2011 году

- “We were a primary target of the WikiLeaks/Anonymous incident, experiencing ~100 attacks over 10 days and covering more or less the full gamut of DDoS attack types. Unrelated 6.5 Gbps attack was IP fragments, 1500-byte packets, highly distributed.”
- “DDoS against UDP/80, 29 Mpps. Do I need to say more?”
- “Mostly invalid packets that were stopped at our border routers via ACLs. Sources were mostly from Europe, target was a Russian Webcam recruitment site. The observed size of the attack was 30 Gbps, but the overall attack was larger than 50 Gbps and hitting capacity restraints within our providers’ networks.”

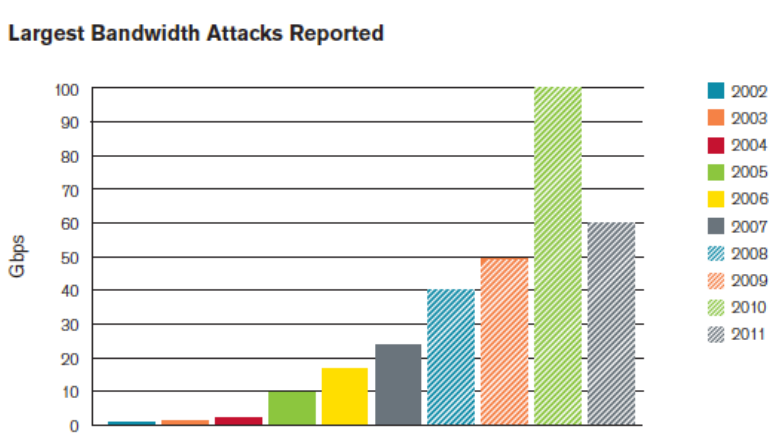


Figure 15 Source: Arbor Networks, Inc.

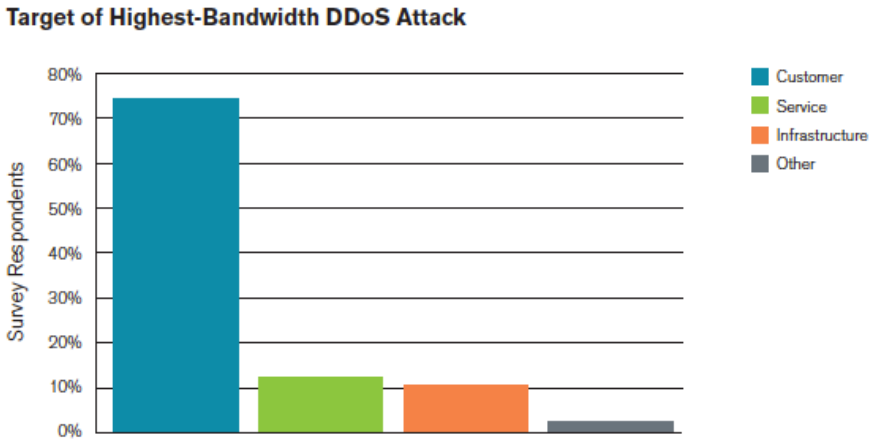


Figure 16 Source: Arbor Networks, Inc.

ARBOR NETWORKS

DDoS на приложения в 2011 году

- “4.4 Mpps attack was an attack using malformed DNS queries toward our DNS resolvers—payloads included either a bunch of NULL characters or the string ‘0123456789ABCDE.’
- “Automated system made malformed HTTP requests. It moved with the DNS, but couldn’t handle HTTP/S, so we moved the site to HTTP/S-only for a month”
- “We faced a side-effect of a spam botnet which tried to resolve nonexistent domain names, causing high loads of NXDOMAIN answers.”

Цели L7 атак:

- HTTP/S
- DNS
- VoIP
- SMTP
- POP

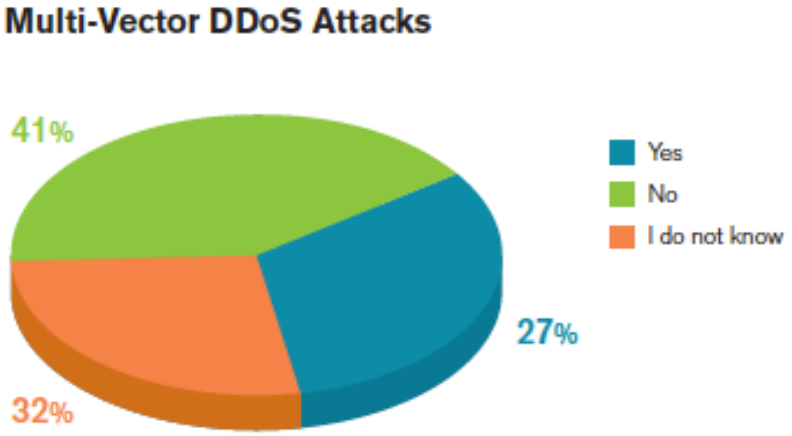


Figure 19 Source: Arbor Networks, Inc.

ARBOR NETWORKS

DNS атаки в 2011: атака isc.org/ANY

- Старая разновидность DNS Amplification атаки получила новое развитие в 2011…
- Атакующий нанимает бот с полосой 10 Мбит/с
- Бот использует вместо своего адреса адрес жертвы
- Бот посылает на публичный resolver 36-байтный ANY запрос, вызывая ~ 50x ответ на IP жертвы:
  - Бот → DNS: 10 pps / 2880 bps
  - DNS → жертва: 10 pps / 144 Kbps
- А если это многопоточная атака на сотни resolver-ов…
  - Бот → DNS: 60 kpps / 8.6 Mbps
  - DNS → жертва: 60 kpps / 432 Mbps
- … с 10 ботами вместо одного:
  - Бот → DNS: 600 kpps / 86 Mbps
  - DNS → жертва: 600 kpps / 4+ Gbps

На основе презентации Eric Zeigast “ISC.ORG/ANY (DNS Amplification Attacks)”

DNS атаки в 2011: эффект DNSSEC

```
dhcp-26-175:~ kirillkasavchenko$ dig @ns2.ukrtelecom.ua isc.org ANY | grep SIZE
;; MSG SIZE  rcvd: 25

dhcp-26-175:~ kirillkasavchenko$ dig @ns.kyivstar.net isc.org ANY | grep SIZE
;; MSG SIZE  rcvd: 492

dhcp-26-175:~ kirillkasavchenko$ dig @8.8.4.4 isc.org ANY | grep SIZE
;; MSG SIZE  rcvd: 1169

dhcp-26-175:~ kirillkasavchenko$ dig @ns2.ok.cox.net  isc.org ANY | grep SIZE
;; MSG SIZE  rcvd: 3466
```


На основе презентации Eric Zeigast “ISC.ORG/ANY (DNS Amplification Attacks)”

Работающие методы защиты? Практика!

- Наладьте контакт с вашими пирами/апстримами! Узнайте заранее чем они могут вам помочь и с кем связываться в случае трудностей
- Не игнорируйте BCP. Они работают.
- Отработайте методы мониторинга трафика в вашей сети. При выборе сетевого оборудования учитывайте нюансы телеметрии.
- S/RTBH и FlowSpec – эффективные методы быстрой блокировки
- Использование собственных операторских систем защиты
- Определите ответственных за политику безопасности. Эти люди должны обладать необходимым сетевым опытом.

Что не работает против сетевых угроз...

- Неподготовленность и игнорирование (*зачем кому-либо атаковать меня/моих клиентов?*)
- Отсутствие отработанных контактов
- Отсутствие необходимой инфраструктуры
- Отсутствие/неготовность средств телеметрии
- Неподготовленность архитектуры BGP, отсутствие специализированных инструментов
- Межсетевые экраны, IDS/IPS, балансировщики нагрузки и прочие средства с сохранением состояний сессий (stateful)
- Отсутствие специалистов, неосведомленность о современных угрозах

Знайте свое оборудование и приложения

- Производительность, функциональность оборудования и его ограничения
- Производительность, функциональность приложений и их ограничения
- Продумайте и поддерживайте списки доступа на внешних интерфейсах. Типовая ошибка – предположение что кроме TCP/UDP/ICMP других протоколов не бывает.
- BGP – хрупкий протокол. Укрепите его.

Защита инфраструктуры: управление и control plane

- В идеале для управления должна существовать отдельная независимая сеть управления (DCN)
- Отключите неиспользуемые сервисы и протоколы control-plane
- Оставшиеся в живых сервисы должны быть защищены: rACL, CoPP, GTSM, авторизация MD5
- SNMPv3, SNMP view, SNMP Community ACL, SNMP RO
- service tcp-keepalives-in
- SSH вместо TELNET
- QoS для приоритета management и control-plane трафика
- AAA: не забудьте авторизацию и учет
- Уберите ненужный функционал на интерфейсах
- Следите за изменениями конфигураций (RANCID)

Защита инфраструктуры: BGP

- Почти все и в одном месте: draft-jdurand-bgp-security-00
  - MD5
  - GTSM (проверка TTL)
  - Как правильно фильтровать префиксы и AS-PATH
  - BGP Dampening (вернее, его отсутствие ☺)

Защита инфраструктуры: iACL

- Разработайте целостную схему адресации ваших интерфейсов
- Какие именно пакеты могут быть нужны вашим маршрутизаторам?
- Не забывайте про анти-спуфинг (собственные адресное пространство, RFC1918, 224/4, RFC3330)
- Используйте NetFlow для изучения трафика на ваше оборудование – увидите ошибки конфигурации
- Не забудьте закончить iACL через permit ip any any
- Не пропускайте протоколы которые вы не знаете

Пример iACL

```
access-list 101 deny ip our_CIDR_block any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any

access-list 101 permit tcp host peerA host peerB eq 179
access-list 101 permit tcp host peerA eq 179 host peerB
access-list 101 deny ip any ControlPlaneAddressBlock

access-list 101 permit ip any any
```

Телеметрия и инструменты для работы

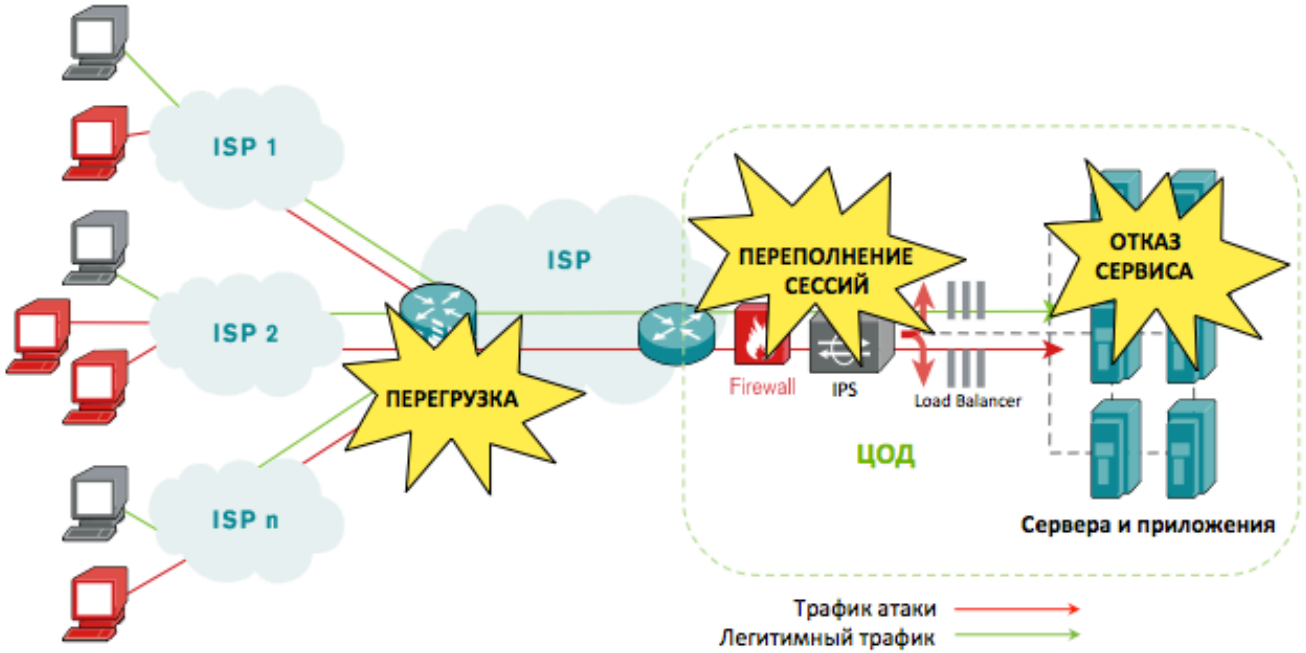
- *«Интернет не работает»*
- Синхронизация времени необходима для корреляции событий
- Требуется отдельная сеть управления или приоритезация трафика телеметрии
- SNMP – загрузка CPU, памяти, интерфейсов, счетчики HQoS/QPPB/ SCU/DCU – CLI, MRTG, rrdtool
- RMON – ntop, nGenius, OptiView Pro
- IP Flow – масштабируемое решение для детектирование аномалий
  - CLI, nfdump, nfsen, Stager, PeakFlow SP, PeakFlow X
- DNS – dnstop, dnslogger, rrdtool, PeakFlow TMS
- BGP – Zebra, Quagga, PeakFlow SP
- Пакетные анализаторы – TCPdump, WireShark
- Syslog – Simple Event Correlator, Sawmill

Противодействие атакам

- Подготовьте инфраструктуру для централизованного управления S/RTBH/FlowSpec
- Не используйте stateful межсетевые экраны для борьбы с DDoS! Используйте stateless списки доступа на маршрутизаторах и коммутаторах
- BCP84 – фильтрация входящего трафика: iACL, uRPF
  - Anti-Spoofing, Anti-Bogon, iACL, отбрасывание определенного трафика L3/L4, фильтры инцидентов, пропуск определенного трафика L3/L4, отбрасывание всего остального
  - uRPF: в случае ассиметрии loose, по возможности strict
- Rate-limit ACL на границе сети
- Взаимодействие с вышестоящими операторами

Защита клиента от DDoS

- При защите клиента надо понимать:
  - Никто не знает свое приложение лучше клиента, но…
  - Клиент не в состоянии остановить Flood DDoS, переполняющий канал связи к оператору.
    - Никто, кроме оператора, не сможет помочь!



ARBOR NETWORKS

Самый важный компонент системы безопасности – люди!

- В идеале специалист по безопасности в операторе связи должен знать:
  - Все что знает инженер развития опорной сети;
  - Все что знает инженер развития сети доступа;
  - Все что знает инженер эксплуатации;
  - Все что знает IT-администратор и web-мастер;
  - Все что знает специалист по электронной почте;
  - Все что знает специалист по пиринговой политике;
  - Все что знает специалист по шифрованию;
  - Все что знает специалист по безопасности в корпоративных сетях.

ARBOR NETWORKS

Спасибо!

kkasavchenko@arbor.net

Содержание

Дополнительные слайды

Полезные ссылки

Best current practices:

- http://tools.ietf.org/html/draft-jdurand-bgp-security-00
- https://datatracker.ietf.org/doc/rfc3704/
- https://datatracker.ietf.org/doc/rfc3013/
- https://datatracker.ietf.org/doc/rfc5358/
- http://www.first.org/resources/guides/
- http://www.sans.org/reading_room/whitepapers/networkdevs/http://www.ietf.org/html.charters/opsec-charter.html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Полезная информация:

- http://ddos.arbornetworks.com
- http://www.arbornetworks.com/report

ARBOR NETWORKS

Услуги по защите от DDoS от крупных операторов

- http://rtcomm.ru/services/anti-DDos/
- http://www.synterra.ru/services/antiddos/
- http://ttk.ru/rus/msk/business/service/servicepage59894.phtml
- http://www.akado-telecom.ru/page.html?id=149
- http://westcall.spb.ru/corporate/services/network/ddos_ataka/
- http://www.verisigninternetdefensenetwork.com/
- http://www.business.att.com/enterprise/Service/business-continuity-enterprise/threat-management-enterprise/ddos-defense-enterprise/
- http://www.globalservices.bt.com/LeafAction.do/param/Record/assure_denial_of_service_mitigation_products_uk_en-gb/fromPage/Search/chapterKey/1
- http://www.rackspace.com/managed_hosting/services/security/ddosmitigation.php
- http://www.verizonbusiness.com/terms/us/products/security/dosdefense/
- http://www.tatacommunications.com/downloads/enterprise/Data%20Sheet%20-%20%20Internet-clean-pipe%20-%20DDOS%20Protection.pdf