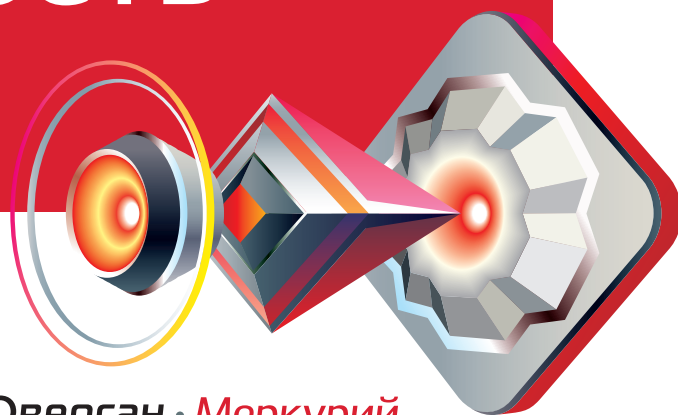
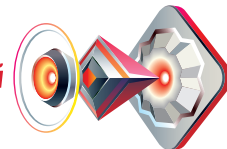


Информационная безопасность



дата-центр **Оверсан** • Меркурий



Информационная безопасность

Anti-DDoS

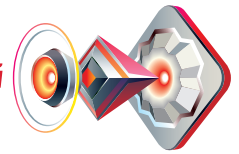
Услуга защиты от распространившихся в последнее время распределенных атак типа отказа в обслуживании (Denial of Service, DoS). Целью подобных атак является блокирование сетевых сервисов за счет создания массы обращений на сервер-жертву (victim). Такие атаки легко распознаются, и сам хакер обнаруживается и блокируется достаточно просто, поэтому новое поколение таких атак носит распределенный характер (Distributed DoS, DDoS). Суть DDoS в том, что хакер использует для атаки зараженные компьютеры (zombie), расположенные по всему миру, чтобы одновременно скрыть свое присутствие и сделать атаку более мощной и результативной.

Меры защиты от атак, предоставляемые дата-центром «Оверсан-Меркурий» основываются на многофакторном анализе трафика, поступающего на каждый защищаемый сервер. Во время нормальной работы система защиты может самообучаться или настраиваться, а после обнаружения атаки либо автоматически, либо по требованию, активно противодействует нелегитимному трафику.

Эффективность защиты от DDoS-атак обычно описывается тремя основными параметрами: мощностью атаки в Мбит/с, которую способна выдержать система, точностью действий системы при обнаружении и отражении атаки и вероятностью и количеством ложных срабатываний.

В зависимости от сочетания этих параметров формируются цена и качество услуг по защите от DDoS атак. Дата-центр «Оверсан-Меркурий» обладает собственными аппаратными системами защиты, способными выдержать DDoS-атаку масштаба нескольких гигабит в секунду с минимумом ложных срабатываний и предлагает клиентам несколько вариантов предоставления услуги:

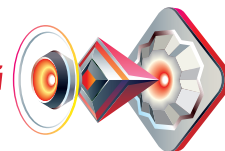
- **«Выделенная зона защиты».** Параметры оптимизированы для использования с услугами Colocation одной и более стоек.
- **«Защита сегмента».** Вариант для хостинговых компаний и клиентов, нуждающихся в незначительном количестве защищенных серверов.
- **«Защита по требованию».** Возможность активировать защиту от DDoS только на время атаки. Важнейший параметр защиты от DDoS-атак – отсутствие ограничений уровня защиты клиента пороговыми значениями производительности. Для того, чтобы отбить внезапную и мощную атаку, в любой момент времени может быть востребована вся мощь системы защиты.



Принцип защиты от DDoS-атак, используемый в дата-центре «Оверсан-Меркурий».

Защищаемой единицей является IP-сегмент, размещаемый в произвольной зоне безопасности. Зона безопасности – это объединение IP-сегментов, для которых в автоматическом или ручном режиме устанавливаются пороги для разных типов трафика (thresholds). Если трафик, поступающий на защищаемый сервер, значительно превышает порог, то, в зависимости от уровня превышения, применяется действие, способное как ограничить скорость атакующего Интернет-узла, так и полностью его заблокировать. Зоны, находящиеся в режиме самообучения, способны автоматически подстраивать пороги трафика в режиме реального времени, чтобы избежать ложных срабатываний, способных привести к деградации некоторых сервисов.

Структура систем Anti-DDoS достаточно проста. Она состоит из модулей, отвечающих за определение аномалий (Traffic Anomaly Detector) и модулей, отвечающих за предотвращение аномалий (Traffic Anomaly Guard). Детекторы (ADM) располагаются как можно ближе к серверам и следят за поступающим на серверы трафиком. Когда детектор замечает аномалию, он сообщает об этом модулю защиты (AGM). Модуль защиты активирует зону и направляет весь трафик зоны на себя, выполняя ряд сложных вычислений, распознавая и удаляя из сети вредоносный трафик. Сервер получает уже очищенный от мусорных данных трафик и продолжает нормально функционировать. По завершению атаки модуль защиты исключает себя из пути трафика и информирует об этом детектор.



Безопасная передача трафика — IPSec/VPN

Технология IPSec/VPN обеспечивает надежную и безопасную передачу информации по сети с помощью шифрования и мощной системы аутентификации. Опасность перехвата важной информации при ее использовании стремится к нулю. Передача данных ведется с шифрованием пакетов и подтверждением их подлинности, используются протоколы для защищенного обмена ключами.

Обнаружение и предотвращение атак — IDS/IPS

В последнее время разнообразные атаки на информационные системы все чаще служат способом кражи информации или создании ситуации отказа в доступе. Сервис IDS/IPS выявляет и устраняет атаки на клиентские системы. Система постоянно обновляется и способна обнаруживать новые, неизвестные ранее типы атак.

Межсетевой экран — Firewall

Аппаратный межсетевой экран осуществляет контроль и фильтрацию проходящего через него трафика в соответствии с заданными правилами, не допуская потенциально вредоносные данные к оборудованию и приложениям. Таким образом уменьшается объем используемых вычислительных мощностей, снижается нагрузка на оборудование и приложения. Клиенты, использующие данную услугу, получают надежный высокопроизводительный инструмент контроля и фильтрации трафика.

Виртуальная сеть — IP/MPLS

Технология MPLS предоставляет широкие возможности для построения частных сетей по передаче данных. Сотрудники клиента могут располагаться в любой точке планеты, при этом пользовательские данные будут храниться и обрабатываться в защищенном дата-центре. На базе сетей оператора и дата-центра создается виртуальная сеть для передачи клиентского трафика. В этом случае данные передаются по закрытой сети, изолированной от других каналов. Механизм передачи данных эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов. В протоколе MPLS переадресация пакетов управляется исключительно на основе меток. Это имеет много преимуществ перед традиционной маршрутизацией на сетевом уровне.