Услуги по защите от DDoS-атак

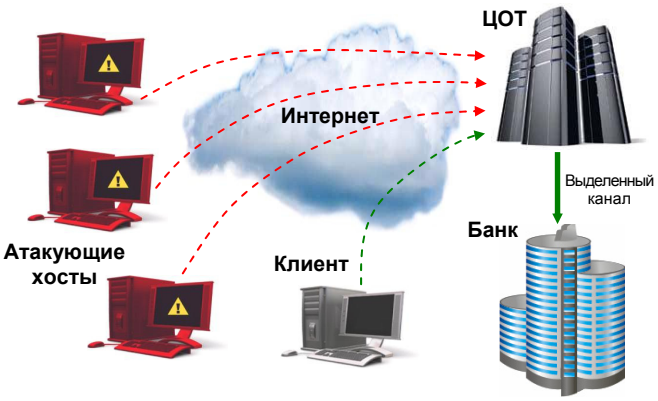
antiddos@bifit.com
+38 (044) 585-12-21

Компания «БИФИТ» предлагает банкам подключиться к Центру очистки трафика «iBank2.UA» для защиты системы электронного банкинга «iBank 2 UA» от DDoS-атак.

Услуги с **минимальным SLA** предоставляются банкам **бесплатно** в рамках технической поддержки.

Схема работы

Для защиты от DDoS-атак весь трафик клиентов системы «iBank 2 UA» направляется в Центр очистки трафика (далее «ЦОТ»), после чего очищенный легитимный трафик направляется из ЦОТа в банк по выделенному каналу.



Защита от DDoS-атак в Центре очистки трафика осуществляется для двух сервисов системы «iBank 2 UA» банка:

- Для вспомогательного HTTPS-сервера «iBank 2 UA», с которого по HTTPS клиенты загружают стартовые страницы, конфигурационные файлы и Java-апплеты
- Для Сервера Приложения «iBank 2 UA», с которым по протоколу GSL (IBTP поверх GSL) взаимодействуют клиентские Java-апплеты и PC-Банкинг

Для защиты банковского HTTPS-сервера «iBank 2 UA» от прикладных DDoS-атак необходимо анализировать HTTPS-запросы, что невозможно делать без секретного SSL-ключа. В то же время передавать в ЦОТ секретные SSL-ключи банковских HTTPS-серверов недопустимо.

Поэтому в настоящее время предлагается два варианта защиты HTTPS-серверов от прикладных DDoS-атак:

- Использование в банке HTTPS-сервера «iBank 2 UA» со встроенным механизмом автоматического управления IP-фильтрами ЦОТа (установка порогов и контроль количества HTTPS-запросов к заданному URI в единицу времени по IP-адресу отправителя)
- Использование всеми клиентами всех банков единой точки входа https://ibank2.ua (https://ibank2.com.ua) – защищенного от DDoS-атак высокопроизводительного HTTPS-сервера, расположенного в Центре очистки трафика «iBank2.UA»

Первый вариант с HTTPS-сервером банка, взаимодействующим с ЦОТом, используется для модуля «Web-Банкинг для частных клиентов» системы «iBank 2 UA».

Второй вариант с единой точкой входа https://ibank2.ua используется для обслуживания корпоративных клиентов.

При подключении к https://ibank2.ua клиент загружает единый клиентский Java-апплет, который автоматически определяет нужный банк по выбранному клиентом секретному ключу ЭЦП.

Механизм автоопределения банка использует идентификатор экземпляра системы «iBank 2 UA» (у каждого банка – свой уникальный ID), который в качестве одного из свойств хранится вместе с ключом ЭЦП клиента.

По идентификатору экземпляра системы клиентский Java-апплет определяет банк, загружает с https://ibank2.ua соответствующие конфигурационные файлы и начинает работать с банковским Сервером Приложения через Центр очистки трафика «iBank2.UA».

Размещение в ЦОТе единой точки входа https://ibank2.ua позволяет анализировать все HTTPS-запросы, выявлять и подавлять сетевые и прикладные DDoS-атаки.

Работа клиентского Java-апплета и клиентского модуля «PC-Банкинг» с банковским Сервером Приложения системы «iBank 2 UA» осуществляется через ЦОТ – все GSL-запросы приходят в ЦОТ, очищаются от DDoS-трафика и через выделенный канал направляются в банк на Сервер Приложения.

Центр очистки трафика «iBank2.UA»

Центр очистки трафика «iBank2.UA» организован компанией «БИФИТ», расположен непосредственно в дата-центре компании «Датагруп» (Киев, ул. Смоленская, 31/33), имеет каналы 1 Gbps в Интернет и 1 Gbps в UA-IX.

Для защиты от сетевых и прикладных DDoS-атак в Центре очистки трафика «iBank2.UA» в рамках первого этапа используется решение **Radware DefensePro 2016** с производительностью 2 Gbps.

В рамках второго этапа по мере прихода заказанного оборудования запланировано внедрение решения **Radware DefensePro 8412 IPS & Behavioral Protection** с производительностью 8 Gbps и 10 Mpps, организация второй площадки ЦОТа в дата-центре компании «NewTelco» (Киев, ул. Гайдара, 50), подключение к UA-IX через канал 10 Gbps и расширение каналов в Интернет.

Выделенный канал «Банк – Центр очистки трафика»

Подключение банка к Центру очистки трафика осуществляется через выделенный канал. На практике есть два типовых варианта организации выделенного канала:

1. Организация канальным провайдером банка выделенного канала типа «точка-точка» (L2 VPN) от банка до ЦОТа по существующему физическому каналу
2. Использование банком резервного Интернет-канала с организацией L3 VPN-канала от банка до ЦОТа

Для банков, имеющих физический канал к оператору «Датагруп», подключение к Центру очистки трафика «iBank2.UA» через канал L2 VPN производит компания «БИФИТ» совместно с компанией «Датагруп» после согласования с банком полосы пропускания (5..100 Mbps).

Второй вариант с резервным Интернет-каналом должен использоваться банками только как временная мера на начальном этапе, так как сохраняется угроза DDoS-атаки на резервный Интернет-канал при знании злоумышленником IP-адресов, выделенных банку для данного канала.

В то же время второй вариант является самым простым в реализации (время подключения к ЦОТу менее 30 минут) и не требует дополнительных финансовых затрат банка.

Radware DefensePro 8412 IPS & Behavioral Protection

Radware DefensePro 8412 – это специализированная платформа со встроенными высокопроизводительными сетевыми процессорами NP-3 (30 Gbps) компании EZChip Technologies, со специализированными ASIC и FPGA для аппаратного ускорения обработки сетевого трафика.

Radware DefensePro 8412 содержит встроенный IPS на базе высокопроизводительного контекстного процессора NETL7 компании NetLogic Microsystems для аппаратного ускорения сигнатурного анализа сетевых пакетов.

Обработка сетевого трафика осуществляется поэтапно, с использованием различных механизмов защиты. При этом суммарное время задержки сетевого пакета не превышает 60 микросекунд.

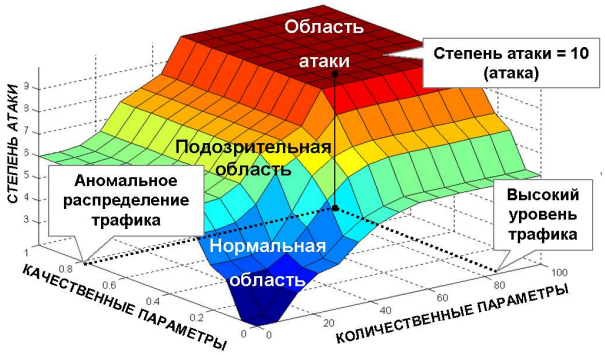
.

В Radware DefensePro 8412 реализованы следующие механизмы защиты:

- Behavioral DDoS Protection
- TCP SYN Flood Protection
- Signature Protection (IPS)
- Connection Limit
- Stateful Inspection
- HTTP Mitigator
- BandWidth Management
- Behavioral Server-Cracking Protection
- Anti-Scanning Protection
- Stateful Firewall (ACL)

Behavioral DDoS Protection. Самый действенный и самый ресурсоемкий механизм защиты от DDoS-атак.

В основе поведенческой защиты – глубокая инспекция пакетов вплоть до 7-го уровня (Deep Packet Inspection), накопление и анализ статистики, обучение и адаптивное построение многомерной модели распределения трафика для штатных условий работы защищаемых сетей и сетевых сервисов, выявление DDoS-атак на основе отклонений и аномалий, блокирование нелегитимного трафика методом динамической фильтрации сетевых пакетов с автоматической генерацией сигнатур DDoS-атаки в реальном времени.



Механизм поведенческой защиты имеет большое количество настраиваемых параметров, поддерживает периоды обучения в течение дня, недели и месяца, позволяет создавать отдельные политики для каждой защищаемой сети и для каждого сетевого сервиса.

При обнаружении признаков DDoS-атаки время на принятие решения, построение динамических фильтров и генерацию сигнатур DDoS-атаки составляет 12 секунд.

В процессе подавления DDoS-атаки механизм поведенческой защиты отслеживает количественные и качественные параметры трафика и при снижении сетевой активности ниже критических порогов снимает динамические фильтры и деактивирует сигнатуры.

Если же применение построенных динамических фильтров и сгенерированных сигнатур не привело к снижению нелегитимного трафика ниже пороговых значений, то DefensePro осуществляет анализ дополнительных параметров трафика с последующим ужесточением фильтрации и перегенерацией сигнатур.

Одно из важных преимуществ механизма поведенческой защиты DefensePro – противодействие атакам «нулевой минуты», для которых еще не созданы статические сигнатуры и не может быть применен встроенный IPS.

TCP SYN Flood Protection. Высокопроизводительный (до 10 Mpps) механизм защиты от атак TCP SYN flood с подменой IP-адреса отправителя (спуфинг). В основе – механизм SYN Cookies, поддерживаемый встроенными в DefensePro сетевыми процессорами NP-3.

Signature Protection. Классический IPS с аппаратной поддержкой статических сигнатур, разработанных и постоянно обновляемых компанией Radware, а также сигнатур пользователя (разрабатываются специалистами Центра очистки трафика «iBank2.UA»).

Высокопроизводительный аппаратный IPS является оптимальным методом противодействия известным уязвимостям в ПО и DDoS-атакам, реализуемым на базе широко распространенных утилит и конструкторов.

Connection Limit. Данный механизм для защищаемого сервиса обеспечивает контроль максимально допустимого количества сессий с IP-адреса отправителя в единицу времени и при превышении пороговых значений блокирует трафик с чрезмерно активных хостов.

Stateful Inspection. Данный механизм проверяет протоколы TCP, ICMP, HTTPS, DNS, SMTP, IMAP, POP3, FTP и SSH на полное соответствие спецификациям RFC. Механизм предотвращает атаки, основанные на нарушении последовательностей пакетов указанных протоколов.

HTTP Mitigator. Механизм поведенческой защиты Web-серверов от прикладных DDoS-атак по протоколу HTTP с функцией обучения. Анализирует все HTTP-запросы и собирает статистику индивидуально по каждому URI. На основе отклонений от типовой активности блокирует доступ с чрезмерно активных хостов к заданным URI.

BandWidth Management. Данный механизм позволяет управлять полосой пропускания для заданного протокола, защищаемой сети или сетевого сервиса. Настраиваются приоритеты обслуживания, минимально гарантированная и максимально допустимая полоса пропускания.

За информацией о решениях для защиты от DDoS-атак и услугах Центра очистки трафика «iBank2.UA» обращайтесь по тел. +38 (044) 585-12-21 и e-mail: antiddos@bifit.com