ANTI DDOS

ANGARA
Professional Assistance

Защита от DDoS и
комплексная защита DDoS
+ WAF

WWW.ANGARAPRO.RU

WAF

ОСНОВНЫЕ ТИПЫ УГРОЗ РАБОТОСПОСОБНОСТИ САЙТОВ

Существуют два основных типа угроз работоспособности сайтов:

- угрозы, направленные на доступность сайта (DDoS);
- угрозы конфиденциальности данных сайта (использующие уязвимости Web-приложения).

ЧТО ТАКОЕ DDOS-АТАКА

DDoS (сокращение английского выражения Distributed Denial of Service, что переводится на русский язык как «Распределенный отказ от обслуживания») – означает отказ от обслуживания сетевого ресурса в результате многочисленных распределенных (то есть происходящих с разных точек интернет-доступа) запросов.

Цель DDoS-атаки – вывести из строя сайт путем постоянного потока запросов, поступающих на него с десятков и сотен тысяч зараженных компьютеров, разбросанных по всему миру. Какой бы мощной ни была информационная инфраструктура, обслуживающая приложения, она не выдержит нагрузки, превышающей норму на несколько порядков и выйдет из строя.

ЧТО ТАКОЕ АТАКА НА WEB-ПРИЛОЖЕНИЕ?

В любом коде приложения возможны ошибки. Хакеры используют их, чтобы получить несанкционированный доступ к данным владельцев и пользователей сайта. Традиционные средства защиты не в состоянии защитить от большинства угроз, направленных на Web-ресурсы. Причина в том, что атаки на такие ресурсы чаще всего происходят на прикладном уровне, в виде HTTP/HTTPS-запросов к сайту, где у традиционных межсетевых экранов крайне ограниченные возможности для анализа и, как результат, обнаружения атак.

ПРОБЛЕМАТИКА

Обеспечение беспрерывного и бесперебойного предоставления сервисов своим клиентам для многих компаний является наиболее важной и приоритетной задачей, обеспечивающей гармоничный рост и развитие. По этой причине защита от атак типа DDoS, а также атак на Web-сервисы является для данных компаний всегда актуальной, что обусловлено следующими причинами:

1. Тенденция к значительному снижению стоимости проведения DDoS-атаки с появлением у злоумышленников «сервисов» для осуществления атак по модели SaaS (заплати – получи доступ к «админке», укажи жертву, получи результат).

2. Постоянный рост количества атак на компании и организации вне зависимости от их размера и отрасли экономики, в которой они работают. Согласно статистическим исследованиям годовой рост количества DDoSатак составляет 18-20% в мире и 25% в России. Рост количества атак на уязвимости приложений составил более 38%.

3. Очень высокая стоимость владения собственной системой защиты от DDoS-атак при неэффективном соотношении издержки / эффективность, так как, кроме эксплуатации самой системы, необходимо обеспечить защиту на уровне провайдера услуг доступа в Интернет или высокую избыточность пропускной способности каналов связи.

4. Множество ограничений и низкая эффективность при использовании услуг защиты от атак, предоставляемых хостинг-провайдером. При наличии серьезной атаки на ресурсы одного клиента, с целью не допустить влияния на других, хостинг-провайдер, как правило, приостанавливает работу атакуемым сервисов данного клиента или сбрасывает весь трафик, идущий к нему, от чего страдают легитимные пользователи.

5. Отсутствие решений по комплексной защите внешних ресурсов компании, включая защиту от DDoS-атак и защиту Web-приложений.

6. Наличие «ручного режима активации защиты» (по звонку) и высокого количества ложноположительных срабатываний систем защиты. Когда совершается атака – необходимо участие людей, когда атаки нет – регулярно производится блокировка легитимных пользователей.

7. Непрозрачная или отсутствующая система гарантий качества и показателей эффективности системы защиты, не предусмотрена компенсация в случаях, если система защиты не работает.

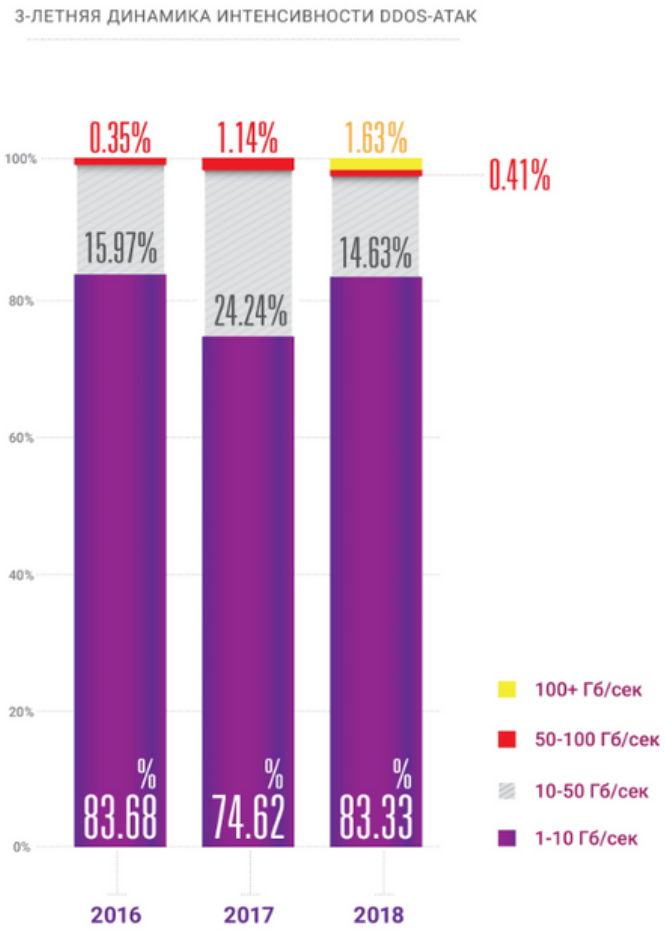
Все перечисленное приводит к недовольству пользователей защищаемого ресурса компании, повышению репутационных рисков, снижению выручки, в том числе при использовании неэффективной системы защиты.

КРАТКОЕ ОПИСАНИЕ УСЛУГИ

Защита от **DDoS**-атак (распределенная атака «отказ в обслуживании») – самостоятельная услуга фильтрации нелегитимного трафика на опубликованные в сеть Интернет ресурсы компании.

В дополнение к защите от **DDoS**-атак может предоставляться услуга **WAF** - защита от взлома с использованием уязвимостей на опубликованные в сеть Интернет ресурсы. Услуга защиты требует постоянного анализа трафика между пользователями и защищаемым ресурсом.

Компания **Angara Professional Assistance** (AA) является сервис-провайдером по предоставлению данной услуги.



ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ ПО

ИСПОЛЬЗУЮТСЯ ДВА СПОСОБА ПОДКЛЮЧЕНИЯ УСЛУГИ:

· **Простой**. Представители компании потребителя вносят изменения в записи DNS, направляющие пользовательский трафик на узлы фильтрации. Эти узлы используют технологию BGP anycast для анонсирования своих адресов.
· **Сложный**. В случае необходимости защиты подсетей компании (или если защищаемый ресурс не имеет FQDN-имени) к BGP anycast могут быть добавлены и соответствующие клиентские префиксы. Реализация данного способа требует участия технических специалистов компании потребителя услуги для настройки активного сетевого оборудования на периметре защищаемого ресурса заказчика.

После подключения трафик компании постоянно, вне зависимости от наличия атаки, поступает в сеть очистки, анализируется ей и «чистый трафик» перенаправляется на защищаемый ресурс. Такая схема работы позволяет узлам фильтрации «понимать», какой профиль трафика является нормой для каждого сайта в отдельности (происходит обучение сети фильтрации), и в случае любых отклонений реагировать на это. Все узлы сети очистки Anti.DDoS&WAF работают независимо, и в случае выхода из строя одного из них трафик защищаемого

РЕЗУЛЬТАТ ДЛЯ КОМПАНИИ

В ПРОЦЕССЕ ИСПОЛЬЗОВАНИЯ УСЛУГИ ОРГАНИЗАЦИЯ ПОЛУЧАЕТ:

1. Круглосуточную техническую поддержку. В случае обнаружения проблем с доступностью защищаемых ресурсов, необходимости внесения изменений в технические параметры услуги, инженеры круглосуточной технической поддержки связываются с представителями компании и уведомляют их о фактах зарегистрированных атак и влиянии на стоимость в случае превышения лимитов, установленных тарифным планом.

2. Личный кабинет. Является основным инструментом контроля KPI услуги. Для каждой созданной учетной записи назначается роль с соответствующими правами доступа.

3. **Гарантированную защиту от всех видов DDoS-атак** на всех уровнях модели OSI или комплексную защиту, снижающую большинство рисков доступности, подкрепленную финансовой ответственностью: при несоблюдении уровня SLA, услуга может не оплачиваться в течение месяца.

4. Полностью автоматизированную защиту, не требующую участия собственного персонала компании, с высокой скоростью реакции на атаки.

5. Наглядную и понятную отчетность об эффективности услуги защиты.

6. Наиболее сбалансированное решение по соотношению эффективность / стоимость.

7. Гибкую систему тарификации и возможность управлять затратами на систему защиты в зависимости от изменяющихся потребностей бизнеса.

8. Отсутствие негативной реакции на результаты применения защитных мер от пользователей и собственного персонала, так как компания узнает об отраженной атаке в отчете, а не от своих недовольных пользователей.

В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ WAF ОСУЩЕСТВЛЯЮТСЯ

1. Уведомления об уязвимостях приложения сайта и принятие мер по выявлению и блокированию вредоносного трафика, направленного на эксплуатацию данных уязвимостей.

2. Предоставление отчетов об обнаруженных проблемах с рекомендациями по устранению, специфичными для платформы разработки конкретного приложения. Поддерживаются приложения: Ruby, PHP, .NET, Perl, Python и другие.

СТОИМОСТЬ УСЛУГИ

Параметрами, влияющими на цену услуги, являются (необходимы для точной оценки стоимости услуги):

1. Тип услуги: только защита от **DDoS** / комплексная защита от **DDoS+WAF**.
2. Гарантированная доступность, измеряемая в процентах.
3. Максимальная полоса фильтрации в Гбит/сек.
4. Легитимный трафик, очищенный от **DDoS** с шагом в 1 Мбит/сек.
5. Легитимный трафик, защищенный **WAF** с шагом в 1 Мбит/сек.
6. Фильтрация **HTTPS**: отключена / с раскрытием / без раскрытия сертификата.
7. Обнаружение уязвимостей, специфичных для конкретного приложения: да / нет.
8. Блокирование эксплуатации выявленных уязвимостей «на лету»: да / нет.

Бюджетная оценка стоимости возможна при определении следующих параметров:

1. Тип услуги: только защита от **DDoS** / комплексная защита от **DDoS+WAF**.
2. Полоса легитимного трафика с шагом в 1 Мбит/сек.

АЛГОРИТМ ОКАЗАНИЯ УСЛУГИ

Простой. Вы вносите изменения в записи **DNS**, направляющие пользовательский трафик на узлы фильтрации. Эти узлы используют технологию **BGP anycast** для анонсирования своих адресов.

Сложный. В случае необходимости защиты подсетей компании к **BGP anycast** могут быть добавлены и соответствующие префиксы Заказчика.

* требует участия технических специалистов Заказчика для настройки активного сетевого оборудования на периметре защищаемого ресурса заказчика.

После подключения трафик компании постоянно, вне зависимости от наличия атаки, поступает в сеть очистки, анализируется ей и «чистый трафик» перенаправляется на защищаемый ресурс.

ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ

СЕТЬ ОЧИСТКИ ОБЛАДАЕТ СЛЕДУЮЩИМИ ОСНОВНЫМИ ХАРАКТЕРИСТИКАМИ:

- Около 1000 Гбит/с пассивной полосы пропускания – детерминированная обработка IP-пакетов без установления TCP-соединения.

- Более 300 Гбит/с активной полосы пропускания – каждое входящее

- TCPсоединение обрабатывается и анализируется.

- <5% ложных срабатываний в процессе отражения DDoS-атаки.

- Время обучения сети от момента подключения нового клиента - менее 2 часов:

  в 33% случаев - до 4 минут;
  в 60% случаев - от 5 минут до 1 часа.

- Добавленное время задержки при проксировании трафика – от 0 до 100 мс. В случае проксирования HTTP-трафика, в силу использования persistent HTTP-соединений с защищаемым сервисом, возможен прирост скорости работы защищаемого сервиса.

- Количество защищаемых ЦОД и сервисов – не ограничено.

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ ЗАЩИТЫ ОТ DDOS:

- «Умная» фильтрация трафика HTTPS без дешифрования.

- Сеть Angara Anti DDoS «прозрачна» для легитимных пользователей.

- Не используются CAPTCHA и прочие раздражающие пользователей сайта проверки.

- Защита в автоматическом режиме, включая L7 OSI.

- Легкость подключения – необходимо изменить A-запись своего сайта, и он – защищен.

- Наглядная **online**-отчетность в Личном кабинете.

- Вы можете увидеть в **online**-режиме анализ трафика своего сайта за любой период оказания услуги. Данный инструмент может быть использован для мониторинга производительности веб-приложений. Используя **API**, вы можете подключить свою систему мониторинга (**Nagios**, **Zabbix** и т.п.) и получать оповещения об инцидентах в удобном для вас формате.

- Минимальное количество ложных срабатываний. **0%** – без атаки. Не более **5%** – под атакой.

- Время реакции на атаку **DDoS** - от **30** секунд до **3** минут.

- По статистике, при превентивном подключении в **97%** случаев атака на ваш сайт будет подавлена в автоматическом режиме не позднее чем через **2,5** минуты.

3-ЛЕТНЯЯ ДИНАМИКА МАКСИМАЛЬНОЙ ИНТЕНСИВНОСТИ DDOS-АТАК

ANGARA

Professional Assistance

Контакты

121096, г. Москва, ул. Василисы Кожиной, д.1, к.1.
БЦ «Парк Победы»
Телефон/факс: +7 (495) 269 26 06
E-mail: info@angarapro.ru