efficient iP™
DEFINING SMART DDI

Защитите Ваш бизнес
Защитите Ваш DNS

Повышенная безопасность с 360° DNS Security

360° DNS Security

- DNS Guardian – адаптивная защита для непрерывности бизнеса
- Защита от атак нулевого дня при помощи Hybrid DNS
- Обработка большого количества запросов с встроенными возможностями балансировки с DNS Blast
- Защита от вредоносных программ и фишинга с DNS Firewall (RPZ)
- Смягчение возможных последствий amplification и reflection атак при помощи DNS RRL
- Аутентичность и целостность данных DNS: DNNSEC
- Ослабление DNS DDoS атак из интернета с помощью DNS Cloud

DNS-сервисы являются критически важными для любой компании, как для доступности интернета, так и для доступа к сетевым приложениям, таким как электронная почта, CRM, VoIP, сервисы, работающие в облаке. В силу своей фундаментальной роли в ИТ-инфраструктуре, DNS-серверы уязвимы в связи со своей открытостью. Они играют двойную роль в модели направленной атаки «Cyber-Kill Chain»: как вектор угрозы и как лучшая цель. Атаки, направленные на DNS-серверы, становятся все более и более изощренными, объединяя в себе несколько векторов одновременно.

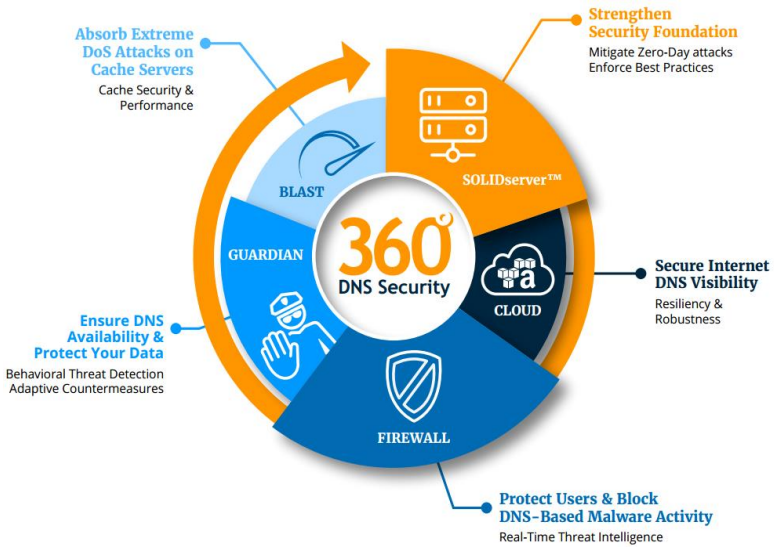
Существуют различные типы DNS-атак:

- объемные атаки - обычно DDoS, Amplification и Reflection атаки;
- скрытые или Меделенные DoS атаки – такие как фантомные домены, SLOTH атаки;
- эксплойты для служб DNS или операционной системы (например уязвимости нулевого дня, отравления кэша DNS, аномалии в протоколе DNS).

Опрос IDC DNS Security, проведенный в июне 2014 года, показал, что 72% респондентов были подвержены атакам на DNS-серверы в течение последних 12 месяцев. Их результатом стали: у 45% был простой, 36% сообщили о потере бизнеса, а у 40% была украдена интеллектуальная собственность. IDC пришел к выводу что «достаточно мало осуществляется для обеспечения безопасности DNS, и компании считают, что базовой защиты, предлагаемой файерволами, достаточно. Это реальный случай неправильной реакции на существующую проблему. В файерволах нет технологий для борьбы с уязвимостями нулевого дня на DNS-серверах или когда они находятся под атакой DNS DDoS, поскольку они не будут иметь никакого эффекта».

Обнаружение и защита от DNS-Атак с решением - 360° DNS Security

Efficient IP предлагает мощное решение - DNS Security, помогающее предотвратить вредоносную активность на уровне протокола DNS, которую сложно отразить при помощи традиционных решений ИТ-безопасности. DNS Security включает в себя: DNS Guardian, DNS Blast, SOLIDserver Hybrid DNS Engine, DNS Cloud и DNS Firewall.



DNS Guardian

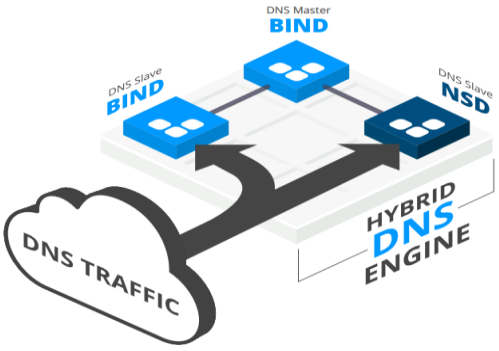
Для идентификации и реагирования на более сложные DNS атаки предлагается использовать модуль DNS Guardian, который включает механизмы поведенческого анализа. DNS Guardian обеспечивает более точный анализ DNS запросов, в случае выявления атаки предлагает меры, которые не нарушают целостность легитимного трафика. DNS Guardian контролирует загрузку DNS сервера и в случае высокой загрузки активирует инновационную технологию Rescue Mode, при которой сервер продолжает отвечать на запросы, используя кэш, что позволяет поддерживать работоспособность даже под DDOS или DNS Flood атакой.

DNS Blast

Решение DNS Blast предлагается в виде программно-аппаратного комплекса, который обеспечивает высокую производительность. В случае массированной DDoS DNS атаки DNS Blast нивелирует влияние атаки за счет высокой производительности сервера. Мощность ПАК Efficient IP SDS-5500 достигает 17 000 000 запросов в секунду.

SOLIDserver Hybrid DNS Engine

Hybrid DNS Engine обеспечивает защиту от уязвимостей класса «Zero-Day». В случае получения алерта от системы безопасности или детектирования кибератаки, которые могут затрагивать DNS-сервер, Hybrid DNS Engine предоставляет альтернативный DNS-сервер, на который сервисы DNS можно переключиться одним щелчком мыши. Возвращение на основной DNS-сервер происходит только после исправления, тестирования и проверки его на уязвимости. Hybrid DNS Engine обеспечивает большую безопасность, меньший риск, лучшую производительность и простоту администрирования.



DNS Cloud

Для повышения безопасности можно развернуть гибридную облачную структуру. Это даст возможность централизованно управлять внутренним DNS-сервером и облачным решением на базе Amazon Web Services. DNS Cloud от Efficient IP - единственное решение, которое позволяет интегрироваться с сервисом Amazon Route 53, обеспечивая возможность управлять логической и облачной инфраструктурой DNS из единой консоли управления. DNS Cloud включает все стандартные функции сервиса Amazone Route 53.

DNS Firewall

Вредоносные программы, использующие уязвимости сервиса (протокола) DNS особенно опасны, поскольку они используются для кражи важных данных. DNS Firewall от Efficient IP активно помогает защищать пользователей, обнаруживая и блокируя вредоносную активность, идентифицируя зараженные устройства и предотвращая новые атаки. DNS Firewall защищает SOLIDserver™ и DNS-инфраструктуру под управлением Linux.