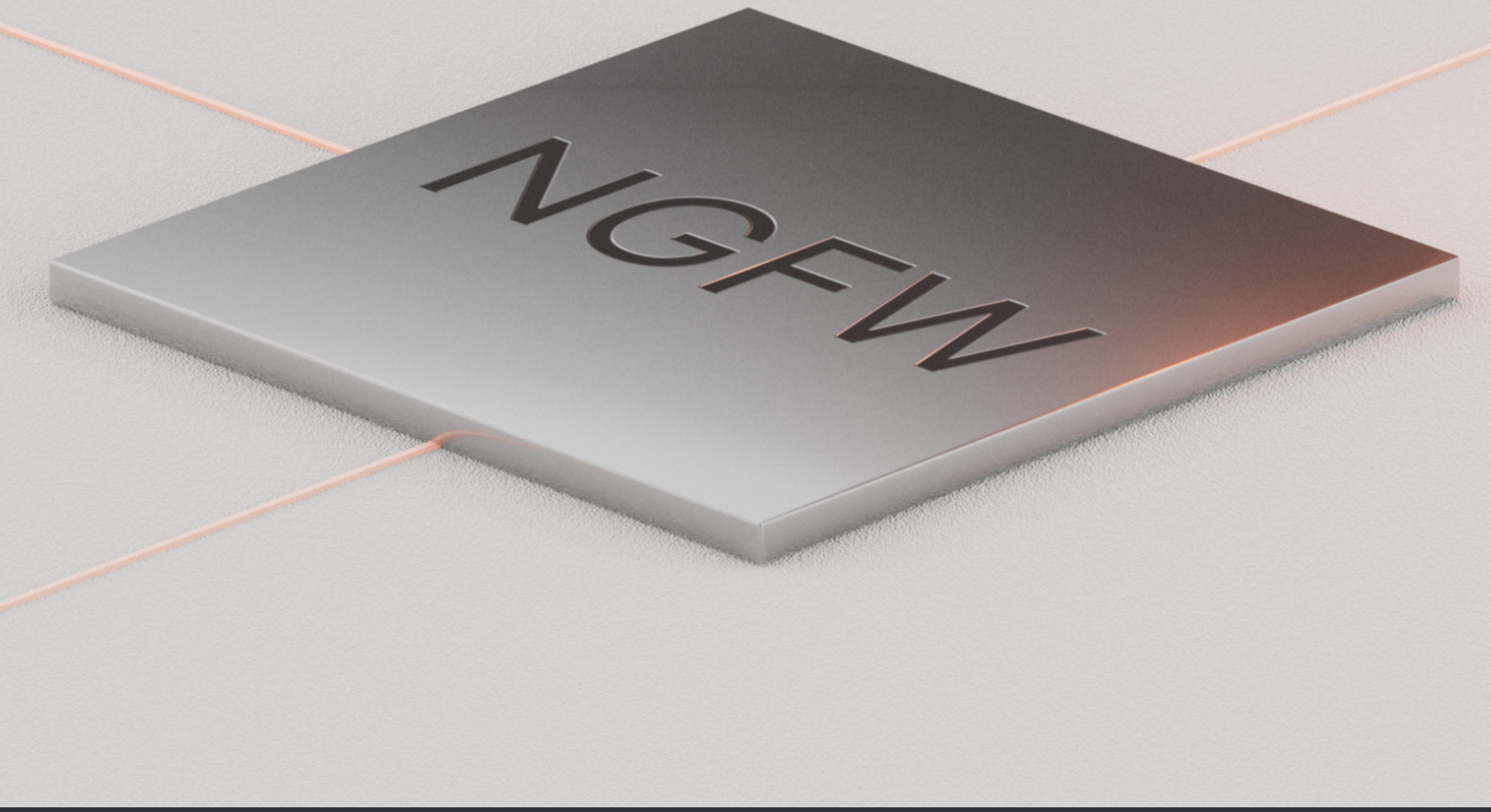
SOLAR

SOLAR NGFW



КАК ВЫБРАТЬ МЕЖСЕТЕВОЙ ЭКРАН КРУПНОМУ БИЗНЕСУ?

W: RT-SOLAR.RU

T: 8 (800) 302-85-23

Обстановка в сегменте сетевой безопасности

13 МЛН РУБ.

стоит в среднем один инцидент крупному бизнесу

1/3

от всех типов угроз составляют целевые атаки и атаки на управляющие протоколы

26 %

профессионалов из крупного бизнеса малознакомы с решениями класса NGFW

Справиться с сетевыми угрозами позволяет межсетевой экран. Вот два наиболее точных определения этого класса средств защиты:

GARTNER

- Устройство или приложение для контроля доступа к сети и мониторинга потока сетевого трафика
- Отфильтровывает попытки вторжения в частную сеть
- Предотвращает внешние попытки вторжения в частную сеть

ГОСТ

- Барьер безопасности, который размещен между различными сетевыми средами
- Состоит из специализированного устройства или совокупности нескольких компонентов и технических приемов
- Пропускает трафик из одной сетевой среды в другую исходя из политики безопасности

Важно знать

Межсетевые экраны обычно устанавливаются на пересечении контролируемых надежных внутренних сетей и потенциально небезопасных внешних сетей, таких как интернет.

Современный подход к сетевой безопасности предполагает установку межсетевых экранов не только на границах сети, но и между ее отдельными сегментами, обеспечивая таким образом дополнительный уровень защиты.

Атаки могут быть инициированы даже с внутренних узлов. Если цель атаки находится в доверенной сети, трафик не выйдет за границы сетевого периметра и межсетевой экран в этом случае будет бесполезен. Исключение составляет ситуация, когда бот обращается к управляющему серверу (C&C), который находится за периметром сети.

Какие существуют виды межсетевых экранов?

1 ПРОГРАММНЫЕ

ПО, установленное на компьютерах и серверах общего назначения, которое отслеживает и контролирует входящий и исходящий сетевой трафик.

2 ОБЛАЧНЫЕ

Межсетевые экраны, предоставляемые как услуга (Firewall as a Service, FWaaS). Они обеспечивают безопасность для сетей, доступ к которым осуществляется через интернет.

3 АППАРАТНО-ПРОГРАМНЫЕ

Межсетевые экраны, которые сочетают в себе как специальное ПО, так и подготовленные к задачам сетевой защиты аппаратные платформы.

4 ПРОМЫШЛЕННЫЕ

Межсетевые экраны, предназначенные для контроля над сетевой безопасностью АСУ ТП. Работают по специализированным промышленным сетевым протоколам, поэтому требуют специальных навыков для внедрения и обслуживания.

Какие межсетевые экраны были раньше?

КЛАССИЧЕСКИЕ

Межсетевые экраны первого поколения, которые работают по модели OSI 3-го и 4-го уровней по списку контроля доступа (ACL). Они анализируют пакеты данных на основе IP-адресов и портов отправителей и получателей, проверяя заголовок TCP-пакета или UDP-дейтаграммы.

ВТОРОГО ПОКОЛЕНИЯ

Межсетевые экраны, которые контролируют шлюзы сеансового уровня по технологии контроля состояния канала и пакетов (SPI). Они анализируют пакеты на уровне принадлежности к активным TCP-сессиям. Это обеспечивает более высокую безопасность по сравнению с классическими МЭ.

Межсетевые экраны нового поколения (NGFW) — за ними будущее, и вот почему:

01 Защищают на всех уровнях модели OSI, кроме физического, не ограничены функциями фильтрации пакетов и контроля состояния сеансов.

02 Позволяют полноценно защищать корпоративный периметр от сетевых угроз и заражений вредоносным ПО, контролировать сетевую активность приложений, ограничивать доступ к запрещенному и вредоносному контенту, защищать от утечки данных через веб-канал и сегментировать сеть.

03 С развитием процессоров и других аппаратных компонентов решается проблема нехватки вычислительных ресурсов для работы всех механизмов защиты и снижения пропускной способности корпоративной сети.

В чем отличия от предыдущих решений?

DPI

Технология анализа полезной нагрузки пакетов трафика. Позволяет выявить в общем потоке данные конкретного приложения и заблокировать либо приоритизировать их.

ПОТОКОВЫЙ АНТИВИРУС

Механизм защиты, по сигнатурам выявляющий в сетевом трафике вредоносное ПО и предотвращающий его попадание на рабочие устройства пользователей.

IDS/IPS

Система выявления в сетевом потоке вероятных атак на корпоративную инфраструктуру с помощью анализа соответствия трафика сигнатурам уже известных атак.

РАСШИФРОВАНИЕ SSL

Технология, обеспечивающая расшифровку защищенного трафика для последующего анализа остальными механизмами защиты.

URL-ФИЛЬТРАЦИЯ

Технология, которая позволяет блокировать запросы пользователей к спискам нежелательных, запрещенных и вредоносных веб-страниц.

VPN-СЕРВЕР

Компонент, который позволяет устанавливать защищенные соединения между удаленным пользователем и корпоративной сетью либо филиалами организации.

У нас сегодня то, что у других – завтра

Скорость

4 Гбит/с в режиме NGFW

Сигнатуры

IPS от Solar 4RAYS

Интерфейс

Современный

Solar NGFW

NGFW — оптимальный класс решения для защиты крупного бизнеса от киберугроз. Внедрение современного российского решения позволяет значительно уменьшить риски инцидентов, повысить комплексную защищенность, обеспечить соответствие законодательству. Это напрямую влияет на устойчивость бизнеса в условиях социальной и экономической неопределенности внешней среды.

Для консультации и получения дополнительной информации оставьте заявку на нашем сайте.

ПЕРЕЙТИ НА САЙТ