



FORCEPOINT Next Generation Firewall (NGFW)

**ЗАЩИТА ВАШИХ СОТРУДНИКОВ И ИХ ДАННЫХ
В ВАШЕЙ КОРПОРАТИВНОЙ СЕТИ**



Protecting the human point.

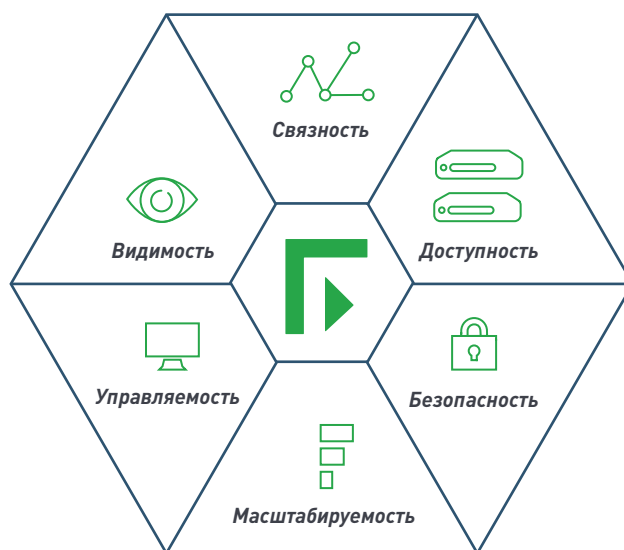


Forcepoint NGFW

САМЫЙ БЕЗОПАСНЫЙ И ЭФФЕКТИВНЫЙ КОРПОРАТИВНЫЙ FIREWALL — С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ, РАБОТАЮЩИЙ БЕЗ ПЕРЕРЫВОВ И СБОЕВ

[Forcepoint Next Generation Firewall \(NGFW\)](#) обеспечивает связь и защиту сотрудникам, а также данным в корпоративной сети, с высочайшим уровнем эффективности, доступности и безопасности. Заслужившие доверие тысяч заказчиков по всему миру, решения по обеспечению сетевой безопасности Forcepoint позволяют предприятиям, правительственным учреждениям и прочим организациям эффективно и без лишних затрат решать важнейшие вопросы.

Решения в сфере сетевой безопасности Forcepoint управляются плавно и автоматически независимо от того, где они используются — в физической, виртуальной или облачной среде. Они позволяют администраторам с одной панели и за считанные минуты разворачивать, контролировать и обновлять тысячи Firewall, VPN и IPS, сокращая затраты на обслуживание сети на целых 50%. Расширенная кластеризация для Firewall и сетей исключает возможность возникновения периодов простоя и позволяет администраторам быстро сопоставить бизнес-процессы с надежными и точными средствами управления для блокирования наиболее современных атак, предотвращения кражи данных и обеспечения правильного управления зашифрованным трафиком — и все это без ущерба для производительности.



Firewall и IPS в одном продукте

▶ Forcepoint NGFW не только получил в 2017 году высшую оценку лаборатории NSS Labs при тестировании Firewall нового поколения, он также содержит в себе одну из лучших систем предотвращения вторжения (IPS). Теперь отсутствует необходимость в дополнительных лицензиях или использовании отдельных инструментов для реализации мощных политик защиты от вторжений.

Предотвращение взломов и краж

- ▶ Forcepoint — «провидец» с наивысшей оценкой способности реализации в «магическом квадранте» Gartner 2017 года для корпоративных Firewall. Firewall предоставляет широкий спектр продвинутых средств контроля доступа и возможностей глубокой проверки трафика для создания защиты от угроз, которые приводят к взломам и краже критически важных данных или интеллектуальной собственности.
- ▶ Являясь пионером в области обнаружения усовершенствованных методов обхода, которые часто предшествуют проведению современных атак, Forcepoint NGFW срывает попытки злоумышленников внедрить вредоносный код, выявляет аномалии и предотвращает попытки использования уязвимых мест в сети.



«Мы увидели возможность объединить функциональность маршрутизатора и расширенного Firewall, чтобы повысить уровень безопасности на каждом предприятии и увеличить пропускную способность сети. Нам нужно было решение с централизованным управлением, которое можно легко продублировать каждый раз, когда мы добавляем новую мобильную площадку, — решение, которое снизило бы нагрузку на деятельность нашего ИТ-отдела».

— Кристоф Хейзман, руководитель отдела информационных технологий, компания Carglass





Эффективность управления при снижении затрат

Forcepoint NGFW специально разработан для того, чтобы уменьшить сложность операций и время, необходимое для обеспечения бесперебойной и надежной работы вашей сети. Аналитики считают, что 80% общих затрат на информационные технологии (TCO) возникают после первоначальной покупки¹. Перегруженным подразделениям, которые занимаются обслуживанием сетей, постоянно приходится иметь дело с развертыванием новых Firewall, мониторингом сетевой активности, обновлением политик и программного обеспечения, а также реагированием на различные инциденты.

Forcepoint NGFW построен на основе единого программного ядра, которое обеспечивает одинаковые возможности, ускорение развертывания и централизованное управление при любом варианте применения. Центр управления безопасностью (SMC) Forcepoint NGFW позволяет настраивать, контролировать и обновлять до 2 000 устройств Forcepoint NGFW — физических, виртуальных, облачных — с одной панели.

Ускорение
развертывания
Firewall на

70%²

Уменьшение
нагрузки на
ИТ-персонал на

53%²

Повышение
скорости
реагирования на
инциденты на

73%²

Автоматическое развертывание

Экономьте время и средства за счет развертывания Forcepoint NGFW в удаленных офисах и филиалах без необходимости присутствия в них технического специалиста. Устройства могут автоматически загружать свою начальную конфигурацию из облака для установки Forcepoint, что устраняет необходимость в ручной настройке.

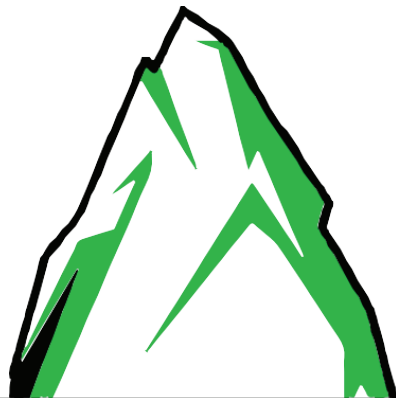
Интеллектуальные политики, обновление в одно действие

Интеллектуальные политики Forcepoint позволяют интерпретировать ваши бизнес-процессы в привычных терминах, таких как пользователи, приложения, местоположения и т. д. Простая группировка пришла на смену жестко заданным значениям, позволяя динамически повторно использовать политики в различных участках вашей сети. Forcepoint NGFW дает администраторам возможность быстро обновлять и вводить в действие политики на всех нужных Firewall, глобально и одним щелчком мыши.

Повышение скорости реагирования на инциденты

Центр управления безопасностью Forcepoint упрощает процесс виртуализации и анализа событий в вашей сети. Сетевые администраторы могут в интерактивном режиме получать соответствующие данные, чтобы быстро исследовать закономерности и аномалии, чтобы затем переходить от догадок к немедленным действиям.

Forcepoint NGFW разработан специально для уменьшения ИТ-затрат



- ▶ Аппаратное обеспечение
- ▶ Подписка и лицензии
- ▶ Поддержка

КАК FORCEPOINT УМЕНЬШАЕТ СКРЫТЫЕ ЗАТРАТЫ:

- ▶ Единое решение для физической, виртуальной и облачной сред
- ▶ Встроенные IPS, VPN, NGFW, прокси-службы
- ▶ Автоматическое развертывание
- ▶ Высокая доступность на всех уровнях
- ▶ Управление сетью SD-WAN с недорогим широкополосным соединением
- ▶ Центральное управление, развертывание в одно действие
- ▶ Обновление ПО
- ▶ Повторное использование средств
- ▶ Управление доступом по названию и версии приложения



Высокая доступность, устраняющая простои в работе сети

Forcepoint NGFW специально разработан для того, чтобы не прерывать работу ни на миг, даже когда возникают проблемы. Устойчивость (способность сохранять работоспособность при отключении машин от сети или краже кабеля на линиях) соблюдается на всех уровнях: устойчивость Firewall, непрерывность работы сети и неизменная эффективность управления. Forcepoint NGFW устраняет вероятность простоев, чтобы обеспечить бесперебойную работу вашей компании.

Продвинутая кластеризация Firewall, которая исключает простои

Разверните Firewall Forcepoint NGFW группами (а не только парами), которые называются кластерами, чтобы поддерживать работу сети, даже если потребуются перерыв на обслуживание любого из отдельных устройств. Вы можете даже объединять в кластер разные модели, чтобы продлить срок службы ваших текущих устройств.

Обновления, не требующие остановки работы

Используя Forcepoint NGFW, можно обновлять политики обеспечения безопасности Firewall, не выходя в автономный режим, незамедлительно реагировать на инциденты в сфере безопасности без ущерба для возможностей подключения и без проблем обновлять программное обеспечение устройства — для этого не нужно ждать предусмотренной паузы на проведение обслуживания, при этом вы не потеряете ни одного пакета данных.



Кластеризация защищенной многопровайдерной сети SD-WAN

Forcepoint — один из пионеров в кластеризации различных сетевых каналов. Технология многоканальной VPN позволяет совместно использовать коммерческие широкополосные линии связи и выделенные линии для устранения точек отказа, снижения сетевых затрат, увеличения пропускной способности и повышения качества обслуживания.

Отказоустойчивое управление

Центр управления безопасностью (SMC) Forcepoint NGFW дает возможность одновременно применять сразу несколько серверов, чтобы вы могли продолжать процесс управления сетью и анализа внештатных ситуаций, даже когда пропадает связь с основным сервером.



«Мы работаем с мощной сетью, обладающей чрезвычайно высокой пропускной способностью, поэтому производительность была основным фактором при выборе Firewall для нашего нового оборудования. Forcepoint NGFW — идеальный выбор, поскольку он объединяет в себе самые современные функции безопасности и высокую степень надежности».

— сетевой архитектор, компания Cegedim



Forcepoint NGFW получил в 2017 году высшую оценку лаборатории NSS Labs при тестировании Firewall нового поколения

Непревзойденная система безопасности, снижающая число краж данных, а не параметры производительности

Forcepoint NGFW получил в 2017 году высшую оценку лаборатории NSS Labs при тестировании Firewall нового поколения. Он поставляется со множеством встроенных средств обеспечения безопасности (включая VPN, IPS, NGFW и прокси-серверы), освобождая вас от необходимости манипулировать различными продуктами, распределять лицензии или выполнять обязанности администратора в самых разных местах. Вы даже можете менять роли устройств безопасности в соответствии с собственными нуждами, продлевая жизненный цикл вашей инфраструктуры.

С помощью Центра управления безопасностью Forcepoint (SMC) вы можете применять к каждому соединению различные методы контроля: по приложению, по организации, по местоположению или по множеству других факторов — и все это без ущерба для производительности сети

Контроль зашифрованного трафика с обеспечением конфиденциальности

Forcepoint NGFW дает возможность безболезненно справляться с быстрым переходом на зашифрованные методы передачи для входящего и исходящего трафика. Используя ускоренное дешифрование, Forcepoint NGFW позволяет проверять HTTPS и другие протоколы на основе SSL/TLS, чтобы запретить или разрешить определенные HTTP-команды



или сегменты URL внутри HTTPS — даже в виртуальных и облачных средах. SSH-прокси-сервер Forcepoint NGFW обеспечивает расширенный контроль над критически важными приложениями. Кроме того, использование интеллектуальных политик упрощает соблюдение новых законов и внутренних норм, регулирующих сферу обеспечения конфиденциальности, предотвращая утечку персональных данных при взаимодействии пользователей с банками, страховыми компаниями и другими организациями, где соблюдение данного требования является особенно важным.

Механизм песочницы и служба Advanced Malware Detection

Forcepoint NGFW применяет несколько методов сканирования переданных по сети файлов, включая проверку репутации, встроенное сканирование на наличие вирусов и использование службы Forcepoint Advanced Malware Detection. Эта мощная облачная система использует передовой механизм песочницы и другие аналитические методы для изучения поведения файлов и эффективного выявления и блокирования вредоносного кода. Организациям предоставляется возможность выбора между облачной и внутренней версией, в зависимости от того, какая из них лучше отвечает их потребностям.



Надежная защита от вторжений

Forcepoint является пионером в области защиты от усовершенствованных методов обхода (AET). Наша методика нормализации трафика на всех протокольных уровнях срывает попытки злоумышленников внедрить вредоносный код, обнаруживает аномалии и предотвращает попытки использования узвимых мест вашей сети.

Защита критически важных приложений

Forcepoint NGFW поставляется с возможностью обеспечения защиты на основе проксирования с полной проверкой трафика для критически важных приложений, которые обмениваются данными через зашифрованные HTTPS-соединения. Эта технология впервые начала использоваться в наших Firewall Sidewinder, от работы которых зависят многие из самых чувствительных сетей на планете. В Forcepoint NGFW уникальные возможности проксирования еще больше расширены, что дает администраторам возможность контролировать HTTPS-трафик, разрешая или блокируя определенные URL-адреса или типы HTTPS-запросов.

Встроенные средства фильтрации URL-адресов

Forcepoint NGFW предоставляет быстрый и гибкий способ соблюдения политик веб-доступа для блокирования доступа к фишинговым сайтам, а также вредоносного или нежелательного контента. Облачная служба Forcepoint ThreatSeeker Intelligence предоставляет обширную, постоянно

обновляемую классификацию URL-адресов, которая может использоваться непосредственно в политиках предоставления доступа для обеспечения динамического контроля того, какие пользователи имеют доступ к определенным сайтам.

Перенос приложений предприятия в облако

Forcepoint NGFW обеспечивает защиту рабочих нагрузок, которые реализуются в облаках AWS и Azure. Forcepoint NGFW может быть развернут прямо из магазинов облачных сервисов при управлении из существующей системы SMC. Это помогает организациям защищать свои приложения и другие рабочие нагрузки в облаке с точно таким же уровнем безопасности и связности, который они получают в своих внутренних центрах обработки данных, офисах, магазинах и филиалах, а также в других облачных средах.

Добавление конечных приложений в белый и черный списки

Агент конечного контекста (Endpoint Context Agent) обеспечивает внесение в белый и черный списки клиентских приложений, работающих на хостах и устройствах конечных пользователей. Это, например, позволяет администраторам указать браузеры и их версии, которые могут или не могут получить доступ к сети Интернет. Это предоставляет более точечные средства контроля, которые можно настроить для самых разных нужд и стратегий обеспечения безопасности организации.

Forcepoint — инвестиция, которая сразу окупается

Forcepoint внедряет новый подход к обеспечению корпоративной безопасности: останавливать плохое и пропускать хорошее. Forcepoint NGFW — это удостоенный множества наград Firewall нового поколения, который блокирует атаки злоумышленников и предотвращает кражу данных и интеллектуальной собственности одновременно с преобразованием инфраструктуры и повышением эффективности ваших операций.

Увеличение продуктивности коммерческой деятельности.

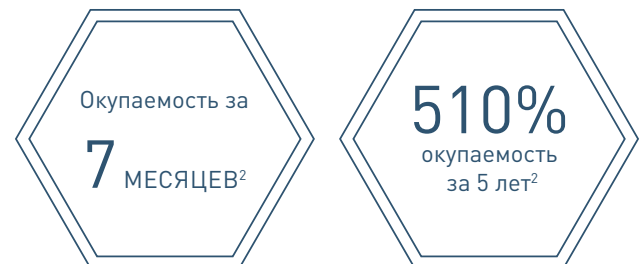
Решения в сфере сетевой безопасности Forcepoint предназначены для предприятий, которым требуется постоянная связь; они обеспечивают безопасный доступ к данным, которые нужны распределенной рабочей группе.

Снижение затрат. Уникальная архитектура высокой доступности, многофункциональная платформа и автоматизированное централизованное управление брандмауэра Forcepoint NGFW сокращают эксплуатационные расходы, обеспечивают более длительный срок службы

и требуют меньше затрат на обучение или получение специализированных навыков.

Снижение информационных рисков. Forcepoint NGFW предотвращает потенциальные угрозы, взломы и кражу данных до того, как они превратятся в финансовую катастрофу.

Упрощенные решения проблем. Forcepoint NGFW сопоставляет бизнес-процессы с элементами управления и позволяет быстро реагировать на инциденты и устранять проблемы, что является очень важным аспектом при работе с аудитором.



ССЫЛКИ:

¹ Gartner

² Forcepoint NGFW Business Value Snapshot, IDC Research, март 2017 г.



«Форспойнт удовлетворяет всем требованиям наших клиентов, включая безопасность, совместимость и стоимость. Он надежен, безопасен, превосходно масштабируется. Ни один другой Firewall не может обеспечить безопасность на том же уровне, как это делает Форспойнт».

— главный консультант по безопасности, компания Netprotocol



О КОМПАНИИ FORCEPOINT

Компания Forcepoint меняет подход к обеспечению кибернетической безопасности, сосредоточившись на том, что является наиболее важным: понимание целей людей при взаимодействии с критически важными данными и интеллектуальной собственностью, где бы они ни находились. Наши безупречные системы позволяют компаниям предоставлять своим сотрудникам беспрепятственный доступ к конфиденциальным данным, защищая интеллектуальную собственность и упрощая процесс решения проблем. Компания Forcepoint со штаб-квартирой в г. Остин, штат Техас, обеспечивает поддержку для более чем 20 000 организаций по всему миру. Чтобы узнать больше о нашей компании, посетите сайт www.forcepoint.com и следите за нашим аккаунтом @ForcepointSec в Twitter.

НАШИ КОНТАКТНЫЕ ДАННЫЕ:

www.forcepoint.com/contact

©2017 Forcepoint. Forcepoint и логотип FORCEPOINT являются торговыми марками компании Forcepoint. Raytheon является зарегистрированной торговой маркой компании Raytheon Company. Все прочие торговые марки, упомянутые в настоящем документе, являются собственностью их непосредственных владельцев.

[BROCHURE_NGFW_OVERVIEW_ENUS] 400013.101017