FORCEPOINT

Техническое описание

FORCEPOINT Next Generation Firewall (NGFW)

№ 1 на рынке сетевой безопасности корпоративных сетей SD-WAN

КЛИЕНТЫ, КОТОРЫЕ ПЕРЕШЛИ НА ИСПОЛЬЗОВАНИЕ FORCEPOINT NGFW, СООБЩАЮТ О СНИЖЕНИИ ЧИСЛА КИБЕРНЕТИЧЕСКИХ АТАК НА 86%, ЗАТРАТ НА БОРЬБУ С НИМИ НА 56% И ВРЕМЕНИ ОБСЛУЖИВАНИЯ НА 70%.*

Forcepoint Next Generation Firewall (NGFW) сочетает быструю, гибкую работу в сети (SD-WAN и LAN) с лучшим в отрасли уровнем безопасности, чтобы гарантировать связь и защиту вашим сотрудникам и их данным в разнообразных быстро развивающихся корпоративных сетях. Forcepoint NGFW обеспечивает постоянную защиту, высокую производительность и удобную эксплуатацию в физических, виртуальных и облачных системах. Он изначально был разработан для обеспечения высокой доступности, масштабируемости и возможности централизованного управления с полной видимостью на все 360°.

Постоянное SD-WAN-соединение для предприятий

Современные компании нуждаются в полностью отказоустойчивых решениях в сфере сетевой безопасности. Брандмауэр Forcepoint NGFW обеспечивает высокий уровень масштабируемости и доступности на всех уровнях:

- **«Активная-активная», смешанная кластеризация.** До 16 узлов различных моделей, на которых запущены различные версии, могут быть объединены в один кластер. Это обеспечивает превосходную производительность и устойчивость сети, а также облегчает работу таких функций безопасности, как глубокая проверка пакетов и VPN.
- **Бесшовное обновление политик и программного обеспечения.** Высочайший уровень доступности Forcepoint позволяет выполнять обновление политик (и даже программного обеспечения), не прерывая процесс обслуживания.
- **Кластеризация в сети SD-WAN.** Распространяет покрытие высокой доступности на сетевые и VPN-подключения. Объединяет непрерывное обеспечение безопасности с возможностью использования локальных широкополосных подключений, призванных дополнить или заменить дорогостоящие выделенные линии (таких как MPLS).

Своевременно отслеживайте изменения потребностей в сфере обеспечения безопасности

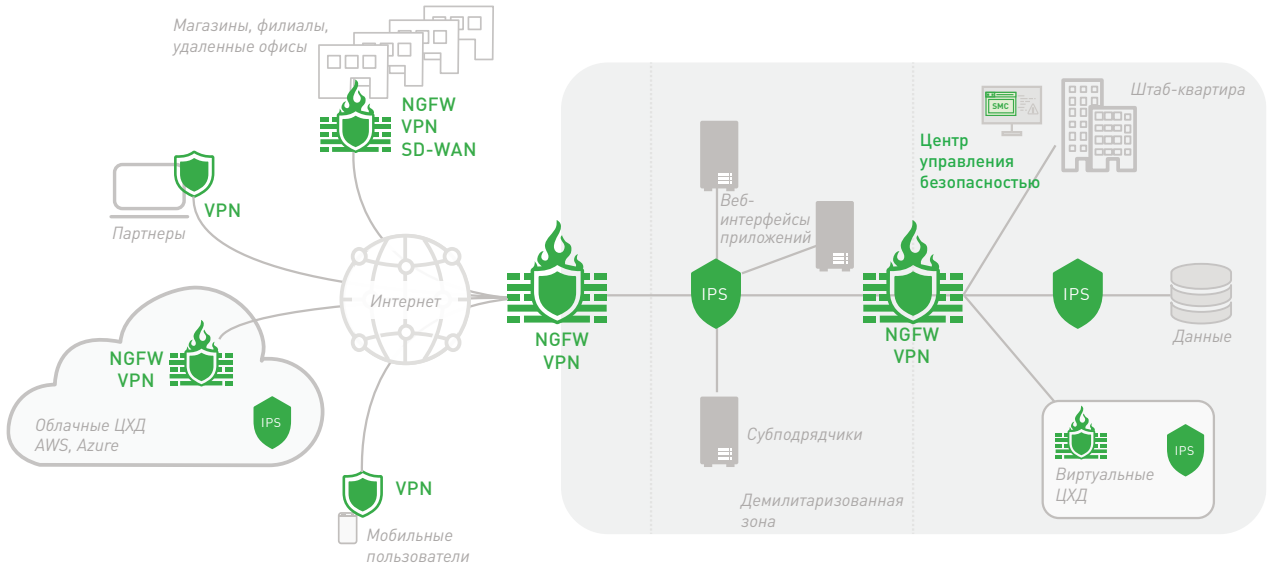
Единое программное ядро позволяет Forcepoint NGFW выполнять в динамических бизнес-средах несколько ролей безопасности: от Firewall/VPN и IPS до Firewall 2-го уровня. Forcepoint NGFW можно развернуть различными способами (в физической, виртуальной, облачной средах), каждый из которых контролируется с одной панели.

Forcepoint совершенно уникальным образом адаптирует процесс управления доступом и глубокую проверку к особенностям каждого соединения для обеспечения высокой степени производительности и безопасности. Он объединяет в эффективном, расширяемом и масштабируемом решении точечный контроль приложений, защиту от вторжений (IPS), встроенное управление виртуальной частной сетью (VPN) и использование прокси-служб для критически важных приложений. Наши мощные технологии защиты от обхода расшифровывают и нормализуют сетевой трафик перед проверкой и на всех уровнях протоколов, чтобы выявлять и блокировать самые передовые методы проведения атак.

Блокировка сложных атак с целью кражи данных

Крупные кражи данных продолжают наносить ущерб компаниям и организациям во всех отраслях. Бороться с ними теперь можно с помощью фильтрации на уровне приложений. Forcepoint NGFW выборочно и автоматически вносит в белый или черный списки сетевой трафик, исходящий от определенных приложений на ПК, ноутбуках, серверах, файловых хранилищах и других конечных устройствах, на основе точечных контекстных данных конечной точки. Он делает больше, чем обычные Firewall, чтобы предотвратить попытки извлечения конфиденциальных данных с конечных точек через несанкционированные программы, веб-приложения, пользователей и каналы связи.

* "Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, май 2017.



Единая платформа со множеством вариантов развертывания — все управляются с одной панели

Непревзойденный уровень защиты

Злоумышленники с течением времени становятся настоящими экспертами в сфере проникновения в сети предприятий, приложения, центры хранения данных и конечные точки. Проникнув внутрь, они крадут интеллектуальную собственность, данные клиентов и другие конфиденциальные данные, нанося невосполнимый ущерб компаниям и их репутации.

Новые методы атак выходят за рамки простого использования уязвимых мест, что позволяет им избегать обнаружения традиционными сетевыми устройствами безопасности, включая многие известные Firewall.

Обход выполняется на нескольких уровнях для маскировки эксплойтов и вредоносных программ, из-за чего они становятся невидимыми во время проведения традиционной проверки пакетов на основе сигнатур. С использованием методик обхода даже старые атаки, которые успешно блокируются в течение многих лет, могут быть применены для проникновения в сеть предприятия.

Forcepoint NGFW использует подход, который не применяется ни в одном другом Firewall. Наш передовой механизм обеспечения безопасности разработан для всех трех этапов сетевой защиты: для противодействия обходу, для обнаружения фактов использования уязвимых мест и для блокировки вредоносного ПО. Forcepoint NGFW может быть развернут в системе с уже имеющимися Firewall как дополнительный уровень защиты без возникновения сбоев в работе, либо в качестве полноценного Firewall, объединяющего в себе все функции безопасности.

Кроме того, Forcepoint NGFW обеспечивает быструю дешифровку зашифрованного трафика, в том числе веб-соединений по протоколу HTTPS, в сочетании со средствами контроля соблюдения конфиденциальности, которые гарантируют безопасность вашего бизнеса и пользователей в быстро меняющемся мире. Он может даже ограничить доступ от конкретных приложений конечной точки, чтобы заблокировать устройства или предотвратить использование уязвимого программного обеспечения.

Преимущества использования:

- **Ускорение развертывания филиалов, облачных ресурсов, центров обработки данных.**
- **Сокращение периодов простоя.**
- **Увеличение уровня безопасности без возникновения сбоев в работе.**
- **Уменьшение количества взломов.**
- **Снижение уровня вероятности возникновения новых уязвимых мест в то время, когда ИТ-специалисты готовятся к применению новых патчей.**
- **Снижение затрат на сетевую инфраструктуру и обеспечение безопасности.**

Основные характеристики:

- **SD-WAN-связность в масштабе предприятия.**
- **Кластеризация высокой доступности для устройств и сетей.**
- **Автоматическое обновление, не требующее остановки работы.**
- **Централизованное управление на основе применения политик.**
- **Полная интерактивная видимость на все 360°.**
- **Встроенная система IPS с защитой от обхода.**
- **Прокси-службы Sidewinder для критически важных приложений.**
- **Ориентированный на человека пользовательский и конечный контекст.**
- **Высокопроизводительное дешифрование с точечным контролем соблюдения конфиденциальности.**
- **Внесение в белый и черный список по клиентскому приложению и его версии.**
- **Интеграция CASB (брокера безопасного доступа к облаку) и средств безопасности веб-приложений.**
- **Механизм песочницы для вредоносных программ.**
- **Унифицированное программное обеспечение для развертывания в физической среде, а также средах AWS, Azure, VMware.**

Технические характеристики Forcepoint Next Generation Firewall (NGFW)

ПОДДЕРЖКА ПЛАТФОРМ	
Устройства	Несколько вариантов устройств, начиная от оборудования для филиалов и заканчивая оборудованием для дата-центров
Облачная инфраструктура	Amazon Web Services, Microsoft Azure
Виртуальная среда	ОС x86 и 64-bit; виртуальные среды VMware ESXi, VMware NSX, Microsoft Hyper-V и KVM
Конечная точка	Endpoint Context Agent (ECA)
Поддерживаемые роли	Firewall/VPN (уровень 3), IPS (уровень 2), Firewall 2-го уровня и смешанный режим 2-го и 3-го уровня
Количество виртуальных контекстов	Виртуализация с целью разделения логических контекстов (Firewall, IPS, Firewall 2-го уровня или смешанный режим 2-го/3-го уровней) с отдельными настройками интерфейса, адресации, маршрутизации и политик для каждого контекста
ФУНКЦИОНАЛЬНАЯ РОЛЬ: Firewall/VPN	
Общие функции	Фильтрация пакетов с учетом состояния и без него, прозрачная глубокая проверка пакетов, расширенные прокси-службы уровня приложения для протоколов HTTP, HTTPS и SSH, общие прокси-службы уровня приложения для TCP и UDP, а также внесение приложений в белый и черный список по названию и версии
Аутентификация пользователя	Внутренняя база данных пользователей, встроенный LDAP, Microsoft Active Directory, RADIUS, TACACS+, служба Forcepoint User ID (FUID), аутентификация на основе сертификата клиента с помощью веб-браузера или клиента IPsec
Высокая доступность	▸ «Активная-активная» или «активная-пассивная» кластеризация Firewall, до 16 узлов в кластере ▸ Автоматическое переключение при возникновении сбоев (включая VPN-соединения) ▸ Распределение нагрузки сервера ▸ Агрегирование каналов (802.3ad) ▸ Обнаружение сбоев в работе каналов
Распределенная работа в многопровайдерной сети	Многоканальная сетевая кластеризация: высокая доступность и распределение нагрузки между несколькими системами обнаружения вторжений, включая выбор VPN-соединения, агрегирование каналов VPN, выбор канала передачи данных на основе QoS
Назначение IP-адресов	▸ Кластеры Firewall: статическое назначение, IPv4, IPv6 ▸ Отдельные узлы Firewall: статическое IPv4, DHCP, PPPoA, PPPoE; статическое IPv6, SLAAC, DHCPv6 ▸ Службы: DHCP-сервер для IPv4 и DHCP-ретранслятор для IPv4
Трансляция сетевых адресов	▸ IPv4, IPv6 ▸ Статическая трансляция NAT, NAT источника с трансляцией «порт-адрес» (PAT), NAT-назначения с PAT
Маршрутизация	Статическая маршрутизация IPv4 и IPv6, маршрутизация на основе политик, статическая многоадресная маршрутизация
Динамическая маршрутизация	IGMP proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM, PIM-SSM
IPv6	Двойной стек IPv4/IPv6, ICMPv6, DNSv6
SIP	Позволяет динамически передавать медиапотоки по протоколу RTP, использовать протокол NAT Traversal, выполнять глубокую проверку и взаимодействовать с RFC3261-совместимыми устройствами SIP
Перенаправление на CIS	Перенаправление протоколов HTTP, HTTPS, FTP, SMTP на сервер проверки контента (CIS)

Технические характеристики Forcepoint Next Generation Firewall (NGFW). *Продолжение*

Географическая защита	Контроль доступа по стране или континенту источника/адресата
Список IP-адресов	Контроль доступа по заранее заданным категориям IP-адресов или через список IP-адресов
Список URL-адресов	Контроль доступа по списку URL-адресов
Списки конечных приложений	Контроль доступа по названию и версии приложения
Прокси-службы Sidewinder Security	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS
Перенаправление на службу Forcepoint Web Security	Перенаправление трафика HTTP/HTTPS на службу Forcepoint Cloud Web Security для проверки входящего и исходящего веб-контента
IPSEC VPN	
Протоколы	IKEv1, IKEv2 и IPsec с IPv4 и IPv6
Шифрование	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES
Алгоритмы хеширования	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Протокол Диффи-Хеллмана	Группы Диффи-Хеллмана 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Аутентификация	Цифровые подписи RSA, DSS, ECDSA с сертификатами X.509, аутентификация с помощью предварительно выданных ключей, гибридная аутентификация, XAUTH, EAP
Прочее	▸ Сжатие IP-данных IPCOMP ▸ NAT-T ▸ Обнаружение мертвых узлов (DPD) ▸ MOBIKE
VPN-соединение между сайтами	▸ VPN на основе политик, VPN на основе маршрутов, в том числе в пределах клиентских доменов ▸ Звездообразная, полная ячеистая и частичная ячеистая топологии ▸ Динамический выбор звеньев сети на основе системы нечеткой логики Forcepoint NGFW Multi-Link ▸ Режимы Forcepoint NGFW Multi-Link: распределение нагрузки, активный/пассивный, агрегирование каналов
Мобильная VPN	▸ VPN-клиент для Microsoft Windows ▸ Автоматическое обновление конфигурации со шлюза ▸ Автоматическое переключение в случае возникновения сбоев с помощью технологии Multi-Link ▸ Проверка безопасности клиента ▸ Безопасный вход в домен
SSL VPN	
Доступ через клиент	Платформы: Android 4.0, Mac OS X 10.7, Windows Vista SP2 (и более новые версии)
Доступ без клиента *(недоступно в моделях 110 и 115)*	Доступ с веб-портала к веб-сервисам через заранее определенные службы и URL-адреса свободного формата

Технические характеристики Forcepoint Next Generation Firewall (NGFW). *Продолжение*

ПРОВЕРКА КОНТЕНТА	
Многоуровневая нормализация трафика/глубокая проверка	▸ Реконструкция и анализ фактической полезной нагрузки для гарантии целостности потоков данных ▸ Отбрасывание дубликатов сегментов нижнего уровня, которые могут привести к неоднозначности при сборке
Защита от обхода	Блокировка передачи фрагментов вне очереди, перекрывающихся сегментов, манипуляций протоколом, обфускации, недопустимого кодирования
Динамическое определение контекста	Определение протокола, приложения, типа файла
Управление/проверка трафика на основе конкретного протокола	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, инкапсуляция IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, дейтаграммы NetBIOS, OPC Classic, OPC UA, Oracle SQL Net , POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, встроенная проверка Sidewinder Security Proxies
Точечное дешифрование трафика SSL/TLS	▸ Высокопроизводительное дешифрование потоков клиента и сервера HTTPS ▸ Контроль на основе политик для обеспечения конфиденциальности пользователей и ограничения доступа к персональным данным ▸ Проверка подлинности сертификатов TLS и список исключений сертификатов на основе доменных имен
Обнаружение факта использования уязвимых мест	▸ Регистрация данных любых TCP/UDP-протоколов с признаками обхода и аномалиями ▸ Виртуальное устранение уязвимых точек CVE как для клиента, так и для сервера ▸ Сложная методика сравнения сигнатур устраняет необходимость использования множества подписей ▸ Скоростной механизм детерминированных конечных автоматов (DFA) быстро обрабатывает новые сигнатуры ▸ Непрерывное обновление сигнатур от Forcepoint
Пользовательское создание сигнатур	▸ Независимое от протокола сравнение сигнатур ▸ Язык сигнатур на базе регулярных выражений с поддержкой пользовательских приложений
Обнаружение процесса сканирования сети	Обнаружение TCP/UDP/ICMP-сканирования, скрытого и медленного сканирования в сетях IPv4 и IPv6
Защита от бот-сетей	▸ Обнаружение на основе дешифрования и анализ последовательности длины сообщения ▸ Автоматически обновляемая категоризация URL-адресов для блокировки или предупреждения пользователей о сайтах бот-сетей
Корреляция	Локальная корреляция, серверная корреляция журнальных данных
Защита от DoS/DDoS	▸ Обнаружение SYN- и UDP-флуда с одновременным ограничением соединения, сжатие журнала ▸ Защита от медленных HTTP-запросов, ограничение полуоткрытого соединения ▸ Разделение плоскости управления и плоскости данных
Методы блокировки	Прямая блокировка, сброс соединения, добавление в черный список (локальный и распределенный), HTML-ответ, переадресация HTTP
Запись трафика	Автоматическая запись трафика, создание выборок при обнаружении нарушений
Автоматическое обновление	▸ Непрерывное динамическое обновление через Центр управления безопасностью (SMC) Forcepoint ▸ Обновление виртуальных патчей, а также обнаружение и предотвращение возникающих угроз
ФИЛЬТРАЦИЯ URL-АДРЕСОВ	
Классификация URL-адресов	Классификация URL-адресов для ресурсов HTTP и HTTPS с помощью облачной службы Forcepoint ThreatSeeker Intelligence
Пользовательские списки URL-адресов	Сравнение с локальными наборами URL-адресов

* Для получения дополнительной информации см. техническое описание системы предотвращения вторжения Forcepoint.

Технические характеристики Forcepoint Next Generation Firewall (NGFW). *Продолжение*

Протоколы	HTTP, HTTPS
Классификация URL-адресов Forcepoint	Контроль доступа с использованием фильтрации URL-адресов на основе категорий, обновляемых службой Forcepoint ThreatSeeker Intelligence
База данных	▸ Более 280 миллионов доменов верхнего уровня и подстраниц (миллиарды URL-адресов) ▸ Поддержка более 43 языков, 82 категорий
Безопасный поиск	Активация режима безопасного поиска в поисковых системах Google, Bing, Yahoo, DuckDuckGo
СЛУЖБА ADVANCED MALWARE DETECTION И КОНТРОЛЬ ФАЙЛОВ	
Протоколы	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Фильтрация файлов	Фильтрация файлов на основе политик с эффективным процессом отсеивания Поддержка более 200 типов файлов в 19 категориях
Репутация файлов	Быстрая облачная проверка репутации и блокировка вредоносных программ
Антивирус	Механизм локальной проверки на вирусы*
Механизм песочницы для борьбы с угрозами нулевого дня	Forcepoint Advanced Malware Detection доступна как в виде облачной, так и в виде локальной службы
УПРАВЛЕНИЕ И МОНИТОРИНГ	
Интерфейсы управления	▸ Централизованная система управления на уровне предприятия с функциями анализа журналов, мониторинга и создания отчетности ▸ Подробную информацию см. в документе «Техническое описание Центра управления безопасностью Forcepoint»
Мониторинг SNMP	SNMPv1, SNMPv2c и SNMPv3
Захват трафика	Консольная команда tcpdump, удаленный захват через Центр управления безопасностью Forcepoint
Защищенная передача данных системы управления	256-битное шифрование при передаче управляющих данных
Сертификаты безопасности	Профиль защиты сетевых устройств Common Criteria для Firewall с дополнительными функциями, фильтрующего трафик с хранением состояния, сертификация алгоритмов по стандарту FIPS 140-2, сертификат ANSSI CSPN, (сертификат безопасности первого уровня USGv6)

* Локальное сканирование на наличие вирусов не предусмотрено в моделях 110 и 115.

НАШИ КОНТАКТНЫЕ ДАННЫЕ:
www.forcepoint.com/contact

[DATASHEET_FP_NETSEC_APP_EN] 100080.070218