

# Next Generation Firewall

Корпоративная SD-WAN - главное требование на сегодня для сетевой безопасности

## Ключевые преимущества

### Постоянное подключение к SD-WAN для предприятий

Современные предприятия требуют полностью отказоустойчивых решений сетевой безопасности. Forcepoint Next Generation Firewall (NGFW) обеспечивает высокую масштабируемость и доступность на всех уровнях:

- › **Активно-активная смешанная кластеризация.**  
До 16 узлов разных моделей, работающих под управлением различных версий, могут быть объединены в кластер. Это обеспечивает высокую производительность и отказоустойчивость сети, а также безопасность, такую как глубокая проверка пакетов и VPN.
- › **Бесперебойное обновление политик и программного обеспечения.**  
Лучшая в отрасли доступность Forcepoint позволяет беспрепятственно передавать обновления политик (и даже программного обеспечения) в кластер без прерывания работы.
- › **Кластеризация сети SD-WAN.**  
Расширяет зону высокой доступности на сетевые и VPN-соединения. Сочетание безостановочной безопасности с возможностью использования преимуществ локальных широкополосных соединений для дополнения или замены дорогостоящих выделенных линий, таких как MPLS.

Forcepoint NGFW объединяет быстрые, гибкие сетевые технологии (SD-WAN и LAN) с лучшей в отрасли системой безопасности для подключения и защиты людей и данных, которые они используют в разнообразных, развивающихся корпоративных сетях. Forcepoint NGFW обеспечивает постоянную безопасность, производительность и работу в физических, виртуальных и облачных системах. Он разработан с нуля для обеспечения высокой доступности и масштабируемости, а также централизованного управления с полным обзором на 360°.

**Клиенты, перешедшие на Forcepoint NGFW, сообщают о снижении числа кибератак на 86%, уменьшении нагрузки на ИТ-отдел на 53% и сокращении времени на обслуживание на 70%.\***

## Не отставайте от меняющихся потребностей в области безопасности

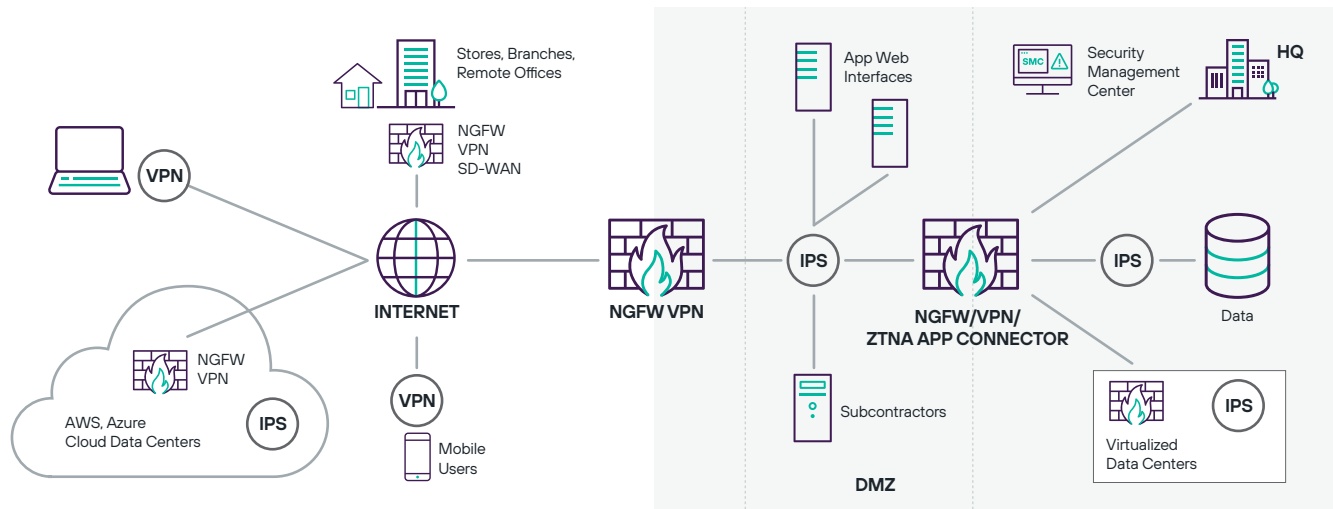
Унифицированное программное ядро позволяет Forcepoint NGFW выполнять множество функций безопасности, от межсетевого экрана/VPN и коннектора приложений ZTNA до IPS и межсетевого экрана второго уровня в динамичных бизнес-средах. Forcepoint NGFW могут быть развернуты различными способами (например, физические, виртуальные, облачные устройства), и все они управляются с единой консоли.

Forcepoint уникально подстраивает контроль доступа и глубокую проверку под каждое соединение, обеспечивая высокую производительность и безопасность. Он сочетает в себе гранулярный контроль приложений, защиту от вторжений (IPS), встроенный контроль виртуальных частных сетей (VPN) и прокси-серверы критически важных приложений в эффективной, расширяемой и масштабируемой конструкции. Мощные технологии защиты от вторжений декодируют и нормализуют сетевой трафик перед проверкой и на всех уровнях протокола, чтобы выявить и блокировать самые современные методы атак.

## Блокирование хитроумных атак, связанных с утечкой данных

Крупные утечки данных продолжают беспокоить предприятия и организации всех отраслей. Теперь вы можете дать им отпор с помощью защиты от эксфильтрации на уровне приложений. Forcepoint NGFW избирательно и автоматически разрешает или блокирует сетевой трафик, исходящий от определенных приложений на ПК, ноутбуках, серверах, файлообменниках и других конечных устройствах, основываясь на высоко детализированных контекстных данных конечных устройств. Он выходит за рамки обычных межсетевых экранов и предотвращает попытки утечки конфиденциальных данных с конечных устройств через несанкционированные программы, веб-приложения, пользователей и каналы связи.

## Одна платформа с множеством вариантов развертывания — все управляется с единой консоли



### Непревзойденная защита

Злоумышленники стали экспертами по проникновению в корпоративные сети, приложения, центры обработки данных и конечные точки. Проникнув внутрь, они крадут интеллектуальную собственность, информацию о клиентах и другие конфиденциальные данные, нанося непоправимый ущерб предприятиям и их репутации.

Новые методы атак позволяют уклоняться от обнаружения традиционными сетевыми устройствами безопасности, включая многие брандмауэры известных брендов, выходя за рамки простой передачи уязвимостей.

Уклонения работают на нескольких уровнях для маскировки эксплойтов и вредоносных программ, делая их невидимыми для традиционной проверки пакетов на основе сигнатур. Благодаря уклонениям даже старые атаки, которые блокировались в течение многих лет, могут быть переупакованы для компрометации внутренних систем.

Forcepoint NGFW использует другой подход. Ведущий в отрасли механизм безопасности предназначен для всех трех этапов защиты сети: для преодоления уклонений, обнаружения уязвимостей и остановки вредоносного ПО. Он может быть развернут незаметно за существующими брандмауэрами, чтобы добавить защиту без сбоев, или как полнофункциональный NGFW для обеспечения безопасности "все-в-одном".

Кроме того, Forcepoint NGFW обеспечивает быструю дешифровку зашифрованного трафика, включая веб-соединения HTTPS, в сочетании с детализированным контролем конфиденциальности, что позволяет сохранить безопасность вашего бизнеса и пользователей в быстро меняющемся мире. Он даже может ограничивать доступ из определенных приложений конечных точек, чтобы заблокировать устройства или предотвратить использование зловещего программного обеспечения.

### Бизнес-результаты

- Более быстрое развертывание филиалов, облаков или центров обработки данных
- Меньше простоев
- Повышение безопасности без сбоев
- Меньше нарушений
- Меньше подверженности новым уязвимостям, пока ИТ-команды готовятся к развертыванию новых исправлений
- Снижение совокупной стоимости владения сетевой инфраструктурой и безопасности

### Ключевые особенности

- Возможность подключения SD-WAN в масштабах предприятия
- Интеграция SASE/SSE для обеспечения безопасности веб-сайтов, облаков и частных приложений
- Встроенная IPS с защитой от вторжений
- Кластеризация устройств и сетей с высокой степенью готовности
- Автоматизированные обновления с нулевым временем простоя
- Централизованное управление на основе политик
- Действенная интерактивная видимость 360°
- Прокси-серверы безопасности Sidewinder для критически важных приложений
- Контекст пользователя и конечного устройства
- Высокопроизводительная расшифровка с гранулированным контролем конфиденциальности
- Разрешение/блокировка по клиентскому приложению и версии
- Мониторинг работоспособности приложений
- Интеграция CASB и Web Security
- Антивирусная песочница
- Унифицированное программное обеспечение для физических, AWS, Azure, VMware развертываний

## Технические характеристики Forcepoint Next Generation Firewall (NGFW)

ПЛАТФОРМЫ	
Физическое оборудование	Множество вариантов оборудования, начиная от установки в филиалах и заканчивая установкой в центрах обработки данных
Облачная инфраструктура	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Виртуальное оборудование	64-разрядные системы на базе x86; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM и Nutanix AHV
Конечная точка	Endpoint Context Agent (ECA), VPN Client
Виртуальные контексты	До 250
Централизованное управление	Централизованная система управления корпоративного уровня с возможностями анализа журналов, мониторинга и отчетности. Подробности см. в техническом описании Forcepoint Security Management Center
ВОЗМОЖНОСТИ БРАНДМАУЭРА	
Глубокая инспекция пакетов	Многоуровневая нормализация трафика/глубокая проверка всего потока, защита от вторжений, динамическое обнаружение контекста, обработка/инспекция трафика по протоколу, тщательная расшифровка трафика SSL/TLS (TLS 1.2 и 1.3), обнаружение уязвимостей, индивидуальная дактилоскопия, разведка, анти-ботнет, корреляция, запись трафика, защита от DoS/DDoS, методы блокирования, автоматические обновления
Идентификация пользователей	Внутренняя база данных пользователей, нативная LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, сертификат клиента
Высокая доступность	<ul style="list-style-type: none"> <li>&gt; Кластеризация активно-активных/активно-резервных межсетевых экранов до 16 узлов</li> <li>&gt; SD-WAN</li> <li>&gt; Обход отказа по состоянию (включая VPN-соединения)</li> <li>&gt; Балансировка нагрузки сервера</li> <li>&gt; Агрегация каналов (802.3ad)</li> <li>&gt; Обнаружение отказов каналов</li> </ul>
Назначение IP-адресов	<ul style="list-style-type: none"> <li>&gt; IPv4 статический, DHCP, PPPoA, PPPoE, IPv6 статический, SLAAC, DHCPv6</li> <li>&gt; Услуги: DHCP Server для IPv4 и DHCP relay для IPv4 и IPv6</li> </ul>
Маршрутизация	<ul style="list-style-type: none"> <li>&gt; Статические маршруты IPv4 и IPv6, маршрутизация на основе политики, статическая многоадресная маршрутизация</li> <li>&gt; Динамическая маршрутизация:: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy</li> <li>&gt; Маршрутизация, ориентированная на приложения</li> </ul>
IPv6	Двойной стек IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, полные функции NGFW
Перенаправление прокси	Перенаправление протоколов HTTP, HTTPS, FTP, SMTP на Forcepoint или сторонние службы проверки содержимого (CIS) в локальной и облачной среде
Геозащита	Динамически обновляемая страна или континент источника/назначения
Список IP-адресов	Предопределенные категории IP-адресов или использование пользовательских или импортированных списков IP-адресов
Фильтрация URL (отдельная подписка)	Пользовательские или импортированные списки URL; поддерживает QUIC и HTTP/3
Приложения конечной точки	Имя и версия приложения
Сетевые приложения	7400+ сетевых и облачных приложений
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

## ИНТЕГРАЦИЯ SASE

<b>Переадресация веб-трафика</b>	Туннелирование GRE и IPsec на платформы Security Service Edge (SSE), такие как Forcepoint ONE
<b>ZTNA Application Коннектор</b>	Позволяет частным приложениям во внутренних центрах данных подключаться к службе Zero Trust Network Access от Forcepoint ONE, чтобы пользователи могли получить к ним доступ без VPN

## SD-WAN

<b>Протоколы</b>	IPsec и TLS
<b>Межсайтовая VPN</b>	<ul style="list-style-type: none"><li>› VPN на основе политик и маршрутов</li><li>› Hub and spoke, full mesh, partial mesh, гибридные топологии</li><li>› Динамический выбор нескольких каналов провайдера</li><li>› Распределение нагрузки, активный/резервный, агрегация каналов</li><li>› Мониторинг и отчетность о качестве соединения с провайдером в реальном времени (задержка, джиттер, потеря пакетов)</li></ul>
<b>Удаленный доступ</b>	<ul style="list-style-type: none"><li>› VPN-клиент Forcepoint для Microsoft Windows, Android и Mac OS</li><li>› Любой стандартный IPsec-клиент</li><li>› Высокая доступность с автоматическим обходом отказа</li><li>› Проверки безопасности клиента</li><li>› Доступ к порталу TLS VPN</li></ul>

## РАСШИРЕННОЕ ОБНАРУЖЕНИЕ ВРЕДНОСНЫХ ПРОГРАММ И КОНТРОЛЬ ФАЙЛОВ

<b>Протоколы</b>	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
<b>Фильтрация файлов</b>	Фильтрация файлов на основе политик с эффективным процессом отбора. Более 200 поддерживаемых типов файлов в 19 категориях файлов
<b>Репутация файлов</b>	Высокоскоростная проверка репутации и блокировка вредоносных программ на основе облачных технологий
<b>Антивирус</b>	Локальный механизм антивирусного сканирования*
<b>Zero-Day Sandboxing</b>	Forcepoint Advanced Malware Detection доступен как в виде облачной, так и локальной службы

\* Локальная проверка на наличие вредоносных программ недоступна для устройств 110/115.

