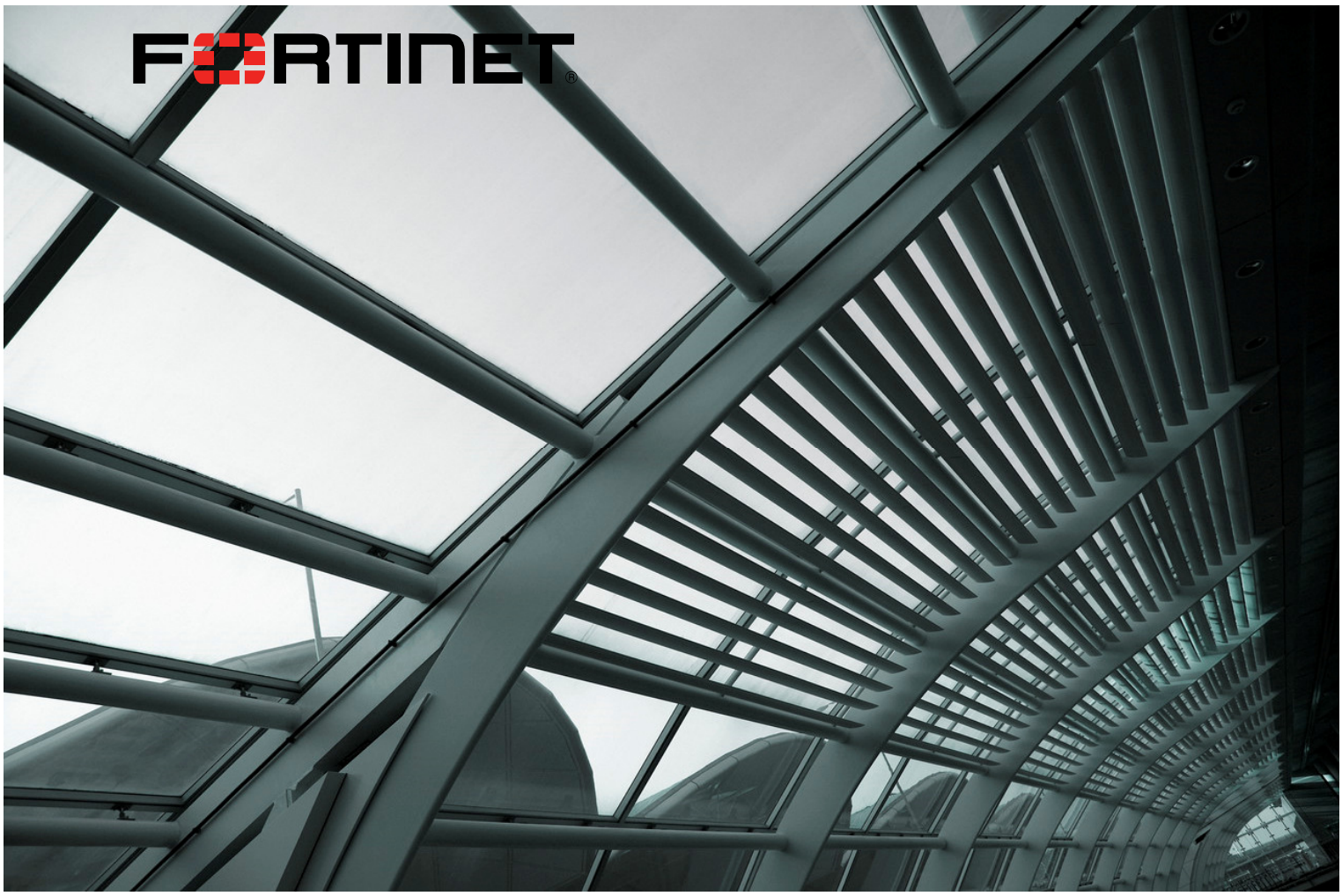


Решения компании FORTINET

Представление Fortinet

СОДЕРЖАНИЕ

1. ПРЕДСТАВЛЕНИЕ КОМПАНИИ

Компания Fortinet является мировым лидером в области высокопроизводительных сетей безопасности. Fortinet создана в 2000 году. Основатель компании Кен Кси (Ken Xie) исходил из своего стратегического видения будущего систем сетевой безопасности: межсетевые экраны и VPN в разрозненном виде не способны препятствовать угрозам нового поколения из сети Интернет, включая целевое управление контентом и приложениями.

Fortinet непрерывно разрабатывает и расширяет свое портфолио продуктов и сервисов, чтобы предоставлять наиболее инновационные и высокопроизводительные платформы сетевой безопасности, которые позволяют компаниям безопасно строить и расширять ИТ инфраструктуру, одновременно упрощая ее.

Технологические достижения помогают продвигать инновации в бизнес и делают существующую инфраструктуру предприятия более сложной, подталкивая традиционную сетевую безопасность к пределам ее возможностей. Технологии моментального подключения, Bring Your Own Device (BYOD), мобильность пользователей и облачные вычисления подводят предприятие к возрастающим угрозам безопасности на следующих уровнях: инфраструктура, пользователи, приложения.

Решения безопасности Fortinet (Fortinet Security Solution) нацелены на эти три уровня и совмещают в себе быстродействие, защиту и развитие. Мы обеспечиваем усиленный контроль и безопасность от конечных устройств до ЦОД и от периметра до приложений, что увеличивает гибкость ИТ инфраструктуры предприятия.

В то же время, наша экспертиза в технологии ASIC в сочетании с глубокой интеграцией безопасности в сетевую фабрику и минимизацией задержек и влияния на быстродействие сети препятствует превращению безопасности в узкое место в бизнесе.

Fortinet на 100% сфокусирован на безопасности и инновационных технологиях. Наша сильная и опытная команда имеет глубокую экспертизу в сетевых технологиях и безопасности. Около половины наших сотрудников - инженеры. Компания проводит полный контроль разработки и производства своих продуктов, не допуская компромиссов по качеству, быстродействию или надежности. Fortinet является единственным производителем продуктов сетевой безопасности, у которого есть собственный интеллектуальный центр мирового поиска и обработки угроз, управляемый командой FortiGuard®. Это обеспечивает нам лидерство в отрасли по скорости ответа на новые и развивающиеся ИТ угрозы.

Профиль компании FORTINET
NASDAQ: FTNT **Год основания:** Октябрь 2000 **Fortinet IPO:** Ноябрь 2009
Штаб-квартира Солнечная долина, Калифорния 30+ офисов по всему миру
Сотрудники более 2,700, включая 50% инженеров
Финансовые преимущества FY13 доход: $615M Q3 2014 доход: $193M $964M+ наличные и без долгов Прибыльность
Выпуск первого продукта Май 2002
Поставлено оборудования на текущий момент Более 1,700,000 единиц
Клиенты Более 210,000 клиентов
Лидерство на рынке UTM лидер 3-е место в мире среди производителей решений по сетевой безопасности
Патенты 177 патентов зарегистрировано 146 патентов в процессе регистрации 120 патентов в процессе регистрации

Компания Fortinet является настоящим мировым лидером в сетевой безопасности. С момента создания в 2003 году нашего первого флагманского продукта, платформы сетевой безопасности FortiGate®, Fortinet отгрузил более 1.7 миллиона единиц устройств для более чем 210 000 предприятий, сервис-провайдеров и государственных структур по всему миру, включая большинство компаний из списка 2013 «Fortune Global 100».

Fortinet имеет более 30 офисов, прямое присутствие в 61 стране и глобальные сервисы и центры поддержки клиентов в Северной и Южной Америке, странах APAC и EMEA. Наши продукты доставляются через мировую сеть дистрибуторов и реселлеров, количество которых составляет около 20 тысяч. Fortinet гордится своей финансовой стабильностью: доход за 2013 году превысил $615 миллионов, текущий баланс составляет $964 миллионов в наличности, задолженностей нет. В настоящий момент IDC признает нас в качестве производителя № 3 в области сетевой безопасности. Наша цель - стать безоговорочным лидером на рынке.

2. FORTINET—ВАШ БИЗНЕС-ПАРТНЕР В СФЕРЕ ИТ БЕЗОПАСНОСТИ

2.1 Фундаментальные проблемы в сетевой безопасности

Информационный технологии стали основным инструментом продвижения бизнес-процессов, предназначенных для увеличения продуктивности и прибыли. Технологические достижения помогают продвигать инновации в бизнесе, но в то же время они усложняют задачи по безопасности и контролю сетевой инфраструктуры предприятия:

- **Многообразие сетей**: бизнес использует различные типы сетей, включая публичные/приватные, беспроводные и 3G/4G сети. Ускоряется использование SDN и инфраструктур виртуализации.
- **Управление ресурсами извне сети**: приложения и данные должны быть доступны из большого количества локаций, таких как удаленные офисы, филиалы, транспорт, или через облака.
- **Мобильность:** пользователи получают доступ к корпоративным ресурсам изнутри и снаружи корпоративной сети, количество корпоративных и персональных устройств постоянно увеличивается.
- **Потребность в постоянном увеличении пропускной способности**: чтобы поддерживать развитие бизнеса, организации строят ЦОД, головные офисы и сети для филиалов, способные работать с высокоскоростным Ethernet.
- **Доступ к приложениям**: расширение использования облачных вычислений, социальных сетей и других онлайн приложений создает новые сложности для идентификации и контроля данных, входящих и исходящих из сети.
- **Соответствие нормативам**: организации должны соблюдать сложные отраслевые и государственные нормативы и внутренние политики для обеспечения приватности и защиты данных своих клиентов.
- **Расширенные угрозы проникают в бизнес:** количество кибератак продолжает увеличиваться, и они становятся все более сложными, подвергая компании воздействию тысяч новых вариантов вредоносных программ, которые обнаруживаются каждый день, новым углубленным целенаправленным атакам (ATA) и постоянным расширенным угрозам (APT).

В ходе этой эволюции сети передачи данных становятся все более и более сложными для управления и администрирования – и безопасность не исключение. ИТ департаменты должны успевать сделать больше работы, затратив меньше ресурсов, как бюджетных, так и кадровых.

Fortinet предлагает исчерпывающий, масштабируемый, многоуровневый подход к сетевой безопасности, предоставляющий вам прозрачность и управляемость всей вашей сети, пользователей и данных в удобной для управления форме.

2.2 Решения Fortinet в сфере безопасности

Решения Fortinet в сфере безопасности строятся на трех основополагающих принципах: Защита, Быстродействие, Развитие.

Защита

Fortinet обеспечивает интеллектуальный, многоуровневый подход к безопасности, предоставляя за межсетевым экраном расширенную защиту от угроз (ATP). Операционная система FortiOS® обеспечивает расширенное обнаружение вредоносных программ, которое вместе с превосходными антивирусными сигнатурами предоставляет надежную защиту от самых изощренных современных угроз.

В дополнение к возможностям ATP Fortinet, наше широкое портфолио распределенных решений безопасности помогает надежно защитить и контролировать сети предприятия на различных уровнях и коммуникациях.

И, наконец, собственная команда исследования угроз и ответных мер Fortinet FortiGuard предоставляет сервисы для обеспечения унифицированной защиты от новых и внезапных целенаправленных атак на сеть, контент и устройства. Эти сервисы безопасности постоянно обновляются и передаются через глобальную распределенную сеть FortiGuard, гарантируя клиентам компании постоянную динамическую защиту.

Быстродействие

Неповторимое быстродействие Fortinet базируется на проприетарной технологической платформе, состоящей из собственных процессоров FortiASIC™ и операционной системы FortiOS. Наши процессоры специальным образом ускоряют обработку задач, необходимых для обеспечения безопасности сетей, приложений и контента, предоставляя постоянное сканирование, инспекцию и защиту при постоянно возрастающей скорости передачи данных и степени использования полосы пропускания.

Процессоры FortiASIC ускоряют обработку функций сетевой передачи данных и безопасности, таких как обработка контента, IPv6, маршрутизация многоадресного трафика, предотвращение вторжений (IPS), контроль приложений и антивирусная инспекция. Эти процессоры работают совместно с другими основными процессорами и модулями ускоренных интерфейсов для увеличения общего быстродействия всех функций безопасности и обеспечения большей масштабируемости.

Обладающие уникальной архитектурой решения безопасности Fortinet разработаны для обнаружения опасного контента на высоких гигабитных скоростях. Технологии безопасности других производителей не могут защищать корпоративную сеть от столь же широкого спектра современных угроз в контенте и угроз на основе подключений, поскольку они используют обычные процессоры, предназначенные для общих задач, что приводит к значительному отставанию по производительности.

Развитие

С помощью решений Fortinet организации могут безопасно строить и наращивать свою инфраструктуру ИТ безопасности, соответствуя изменяющимся требованиям бизнеса. Функции безопасности, доступные в наших решениях, могут быть использованы индивидуально, дополняя наследуемые решения, либо могут быть скомбинированы для создания всеохватывающего решения по управлению угрозами. Развернутое решение Fortinet может изменяться и развиваться со временем – от проводных/беспроводных сетей, устройств и систем доставки сообщений до веб-приложений и баз данных, - обеспечивая безопасность в новых областях вашей ИТ инфраструктуры. Наши возможности в области виртуализации позволяют перенести решения Fortinet для защиты данных на виртуальные инфраструктуры, а наша модель лицензирования, привязанная к устройству, упрощает масштабируемость внедряемого решения Fortinet.

Наши решения интегрируются в любую существующую сетевую архитектуру. Развернутое у вас решение Fortinet растет вместе с ростом вашей сетевой инфраструктуры, при этом мы предлагаем централизованное управление безопасностью на всех узлах сети, мониторинг и отчетность для полноценного контроля и полное отображение состояния вашей безопасности в режиме реального времени.

3. ЛИДЕРСТВО FORTINET

3.1 Отраслевое лидерство

Рыночное лидерство Fortinet подтверждается ведущими компаниями по исследованию индустрии:

Место	Компания	Доля рынка (%)
1	Cisco/SourceFire	18.4
2	Check Point	12.9
3	**Fortinet**	**7.3**
4	Palo Alto Networks	7.1
5	McAfee	5.3

Источник: IDC Worldwide Security Appliances Tracker, Q2 2014 (доля рынка по доходу от производства)

- 3й в мире крупнейший производитель решений по безопасности, согласно IDC (по доходу от производства).
- Награжден званием «Европейский производитель информационной безопасности года» и званием «Производитель сетевой безопасности года» в 2013 году.
  Fortinet назван лидером рынка UTM компанией Frost & Sullivan.
- Лидер квадранта Gartner по UTM решениям; находится в числе претендентов на лидерство в магическом квадранте Gartner по корпоративным МЭ.

Источник: Gartner, магический квадрант для UTM, август 2014

Источник: Gartner, магический квадрант для МСЭ корпоративного класса, апрель 2014

Более 200 отраслевых наград присуждено компании Fortinet и ее продуктам:

Компания Fortinet имеет больше сертифицированных технологий безопасности, чем другие производители, и инвестирует значительные средства для соответствия независимым стандартам тестирования. Качество нашего функционала безопасности сертифицировано независимыми организациями, такими как ICSA Labs, NSS Labs и Virus Bulletin 100. Мы также соответствуем многочисленным государственным стандартам, таким как FIPS 140-2, Common Criteria EAL2 и EAL4+, и другим остальным важным сертификациям для IPv6 и ISO 9001.

■ CERTIFIED/RECOMMENDED ■ CAUTION/NOT RECOMMENDED

Certification	Fortinet	Check Point	Cisco	Juniper SRX	Palo Alto	FireEye
NSS Labs FW	■	■	X	■	■	X
NSS Labs Data Center Firewall	■	X	X	■	X	X
NSS Labs NGFW	■	■	■	■	■	X
NSS Labs IPS	■	■	■	■	X	X
NSS Labs Data Center IPS	■	X	■	■	X	X
NSS Labs Breach Detection System	■	X	■	■	X	■
ICSA NGFW Evaluation	■	X	X	X	X	X
BreakingPoint Resiliency Score	■	X	X	X	■	X
ICSA Firewall	■	■	X	■	■	X
ICSA IPSec	■	■	X	■	X	X
ICSA SSL VPN	■	X	X	X	X	X
ICSA IPS	■	■	X	X	X	X
ICSA Antivirus	■	X	X	X	X	X
ICSA WAF	■	X	X	X	X	X
Common Criteria	■	■	■	■	■	■
FIPS 140	■	■	■	■	■	■
DoD UC APL	■	X	■	■	■	X
JITC IPv6	■	■	X	■	X	■
IPv6 Ready	■	■	X	■	X	X
VB100 Virus	■	■	X	X	X	X
AV Comparative	■	X	X	X	X	X
VB Verified Spam	■	X	X	X	X	X

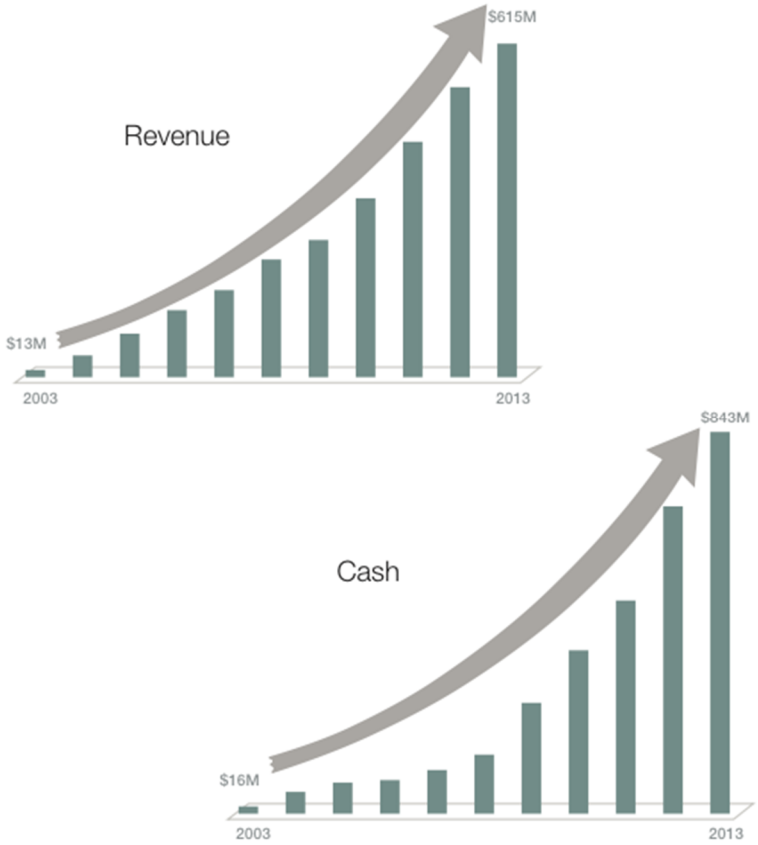
Более подробная информация доступна на нашем сайте:
http://www.fortinet.com/aboutus/fortinet_advantages/certifications.html

3.2 Команда исполнителей

Компания Fortinet была основан и возглавляется Кеном Кси, пионером индустрии ИТ безопасности, который до этого был основателем, президентом и CEO компании Netscreen. Команда исполнителей состоит из опытных людей, каждый из которых имеет большой опыт в сфере ИТ и/или сетевой безопасности.

3.3 Финансовые преимущества

Fortinet имеет серьезную финансовую стабильность, что позволяет компании быть долгосрочным игроком в индустрии ИТ безопасности.
Fortinet получил $615M дохода и 15% годовой рост в 2013 году, темп роста почти в три раза превышает среднерыночный.



Год	2011	2012	2013
Доход	*$434m*	*$534m*	*$615m*
Годовой прирост	*+34%*	*+23%*	*+15%*
Наличные и инвестиции	*$539m*	*$740m*	*$843m*

Компания обладает стабильной прибыльностью (более $964 миллионов наличности) и имеет положительное движение денежных средств уже более семи лет.

3.4 Экосистема партнерства

Компания Fortinet взаимодействует с ведущими поставщиками технологий по всему миру, чтобы обеспечить гарантии совместимости и интеграции с решениями от сторонних производителей в корпоративную ИТ инфраструктуру.

Fortinet поддерживает прочное технологическое партнерство в различных областях.

Программно-определяемые сети (SDN)	Система управления ИБ и событиями (SIEM)	МСЭ и управление рисками	Мониторинг* угроз
VMware Partner Technology Alliance	LogRhythm	FIREMON	stop badware
Citrix	HP ArcSight	ManageEngine Powering IT ahead	CVE Compatible cve.mitre.org
big switch networks	1Labs Total Security Intelligence | An IBM Company	tufin	FIRST Improving Security Together
Arista		algosec	Microsoft
Extreme networks		Bradford Networks the smart edge	
NEC		skybox security	Adobe
		ISS	

* Только сотрудничество

Fortinet также поддерживает партнерство с ведущими системными интеграторами (SI), предоставляя специализированные услуги и консультации по своим решениям безопасности. У нас есть официальные глобальные альянсы со следующими компаниями:

Alcatel·Lucent · dimension data · ERICSSON TAKING YOU FORWARD · ProCurve Networking by HP Solutions Alliance · Business Partner IBM Ready for Security Intelligence · orange Business Services · UNISYS

4. ПРЕИМУЩЕСТВА FORTINET

4.1 Превосходная технология

Компания Fortinet на 100% сфокусирована на безопасности, и технология – это сердце нашей стратегии.

Технология Fortinet разрабатывалась собственными силами компании с первого дня ее существования, компания полностью контролирует разработку своих продуктов и не приемлет компромиссов по качеству, быстродействию или надежности. Наши решения постоянно обогащаются с учетом новейших технологических достижений, чтобы оставаться в авангарде отрасли по функциональности и быстродействия по лучшей цене.

Компания Fortinet зарегистрировала 149 патентов (еще 108 патентов находятся в процессе регистрации) и имеет больше сертифицированных продуктов, чем любой другой производитель устройств безопасности.

В основе инноваций Fortinet находится FortiOS – специализированная операционная система с усиленной безопасностью, которая привносит интеллект и управляемость в сетевую безопасность. Текущая версия, FortiOS 5, имеет богатый набор функций, которые помогают бороться против самого широкого спектра угроз, упрощают настройку и внедрение, расширяют возможности по управлению безопасностью и формированию отчетности. Такие интеллектуальные функции, как оценка репутации пользователя, контекстная проверка трафика и расширенные возможности обнаружения вредоносных программ, делают FortiOS уникальной.

FortiOS дополняется процессорами Fortinet FortiASIC, чтобы помочь заказчикам обеспечить усиленную сетевую безопасности при экстремально высоком быстродействии (до 160 Гбит/с на одном устройстве и до 500 Гбит/с в блейд-системе) и исключительно низких уровнях задержки (до 2-3 микросекунд).

Специализированное аппаратное и программное обеспечение Fortinet позволяет выполнять обнаружение вредоносного контента на высокой скорости. Все функции безопасности операционной системы FortiOS разработаны на едином исходном коде, что позволяет оптимизировать быстродействие и исключить избыточные операции, относящиеся к пакетной или поточной обработке. Другие продукты безопасности на рынке не могут делать этого, поскольку их функции безопасности построены на разных, зачастую несочетаемых исходных кодах.

Платформы безопасности Fortinet комплектуются тремя типами процессоров FortiASIC:

- Сетевой процессор (Network Processor, NP) имеет высокое быстродействие, минимальную задержку и одинаково высокую производительность для IPv4 и IPv6;
- Контентный процессор (Content Processor, CP) ускоряет обработку задач по сканированию контента;
- Процессор безопасности (Security Processor, SP) ускоряет обработку специализированных функций безопасности, таких как IPv6, маршрутизация протокола многоадресной рассылки, предотвращение вторжений (IPS), контроль приложений и антивирусная проверка.

Совместная работа сопроцессоров FortiASIC с процессорами общего назначения ускоряет выполнение всех функций FortiOS по передаче данных и безопасности, что позволяет наращивать быстродействие и оптимально встраивать системы безопасности Fortinet в структуру сети.

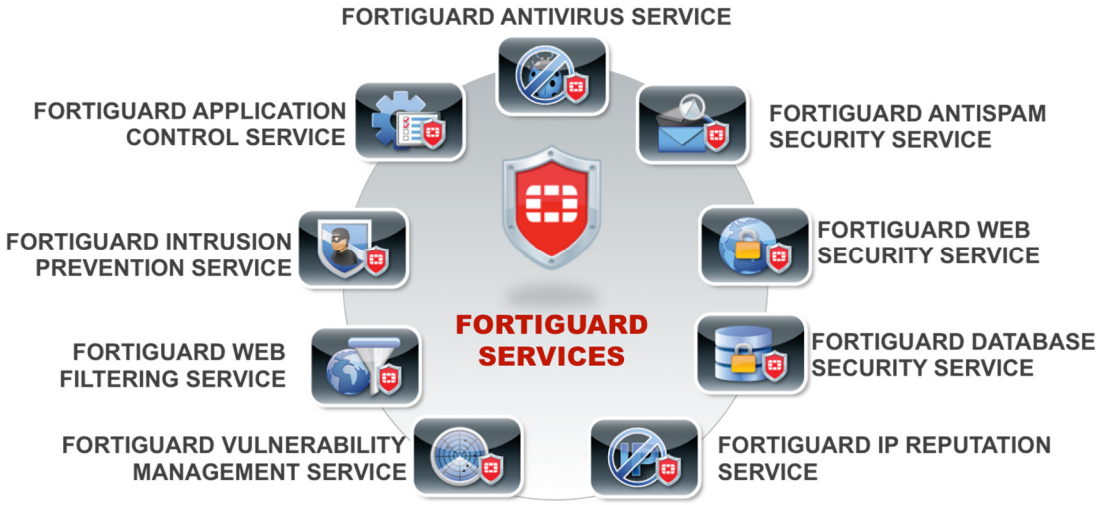
4.2 Собственные исследования и сервисы безопасности

Компания Fortinet - единственный производитель решений сетевой безопасности, у которого есть собственная команда специалистов, занимающаяся исследованием глобальных угроз и выработкой ответных мер, постоянно отслеживающая актуальные угрозы и предоставляющая заказчикам постоянную защиту в реальном времени.

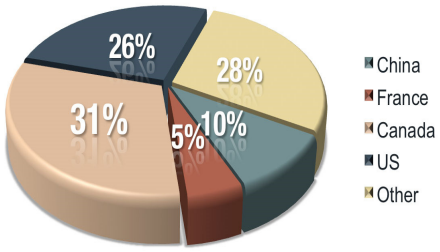
В составе команды экспертов FortiGuard более 180 аналитиков, инженеров и криминалистов, находящихся в разных странах по всему миру и создающих обновления для систем безопасности в режиме 24/7, с лучшим в отрасли временем ответа на новые и критичные угрозы, направленные на сети клиентов, контент и мобильные устройства. Наши эксперты сотрудничают с ведущими мировыми организациями по мониторингу угроз для консультации и обучения при появлении новых и критичных угроз. Своей работой они способствуют развитию всей индустрии безопасности, идентифицируя и своевременно предоставляя отчеты об уязвимостях напрямую производителям оборудования, операционных систем и приложений.

Сервисы подписки FortiGuard предоставляют унифицированную защиту от усиленных целенаправленных атак и смешанных угроз. На основе сигнатур создаются динамично развивающиеся и изменяющиеся защитные средства, такие как «облачная песочница» FortiGuard (механизм обеспечения безопасности, предусматривающий изоляцию загружаемого кода путем помещения его на время выполнения в ограниченную среду – «песочницу») и сервисы анализа репутации IP-адресов, специально разработанные для помощи в защите против целенаправленных атак.

Сервисы FortiGuard's были разработаны с нуля для оптимизации быстродействия и максимальной защиты на всем спектре платформ безопасности Fortinet. Они постоянно обновляются командой FortiGuard и доставляются через глобальную сеть распространения.



4.3 Всемирное присутствие и поддержка



Размещение сотрудников FORTINET по миру

Являясь глобальным производителем, Fortinet стремится присутствовать и активно действовать на местах. Fortinet имеет представительства в 61 стране, а через свою сеть из более чем 20,000 дистрибуторов и реселлеров покрывает в сумме 192 страны, тем самым обеспечивая тесное взаимодействие со своими заказчиками.

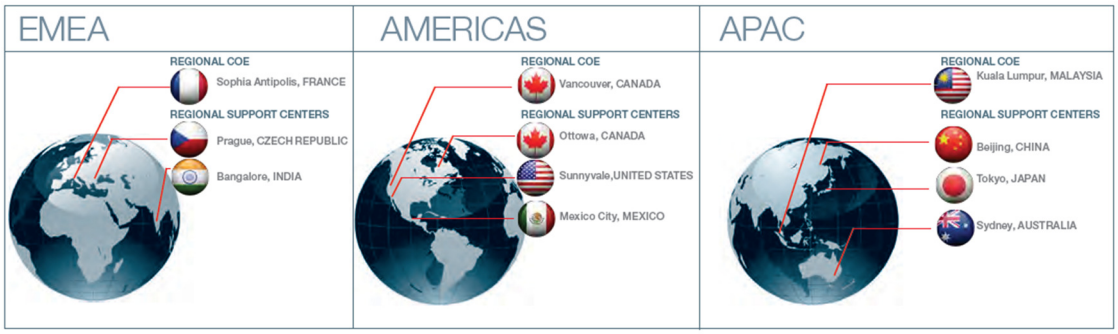
Компания Fortinet вместе со своими партнерами по каналам продаж стремится поддерживать своих клиентов на протяжении всего жизненного цикла их проектов безопасности. Компания может адаптировать свои предложения к любым специфическим требованиям бизнеса, от деловых и технических консультаций до профессиональных сервисов и поддержки продуктов.

Компания Fortinet продает свои решения в основном через двухуровневые дистрибуторские каналы по всему миру. Стратегия канала Fortinet включает интернет-сервис-провайдеров, предоставляющих услуги по управлению безопасностью (MSSP), которые предлагают широкий спектр сервисов, базирующихся на продуктовой линейке Fortinet. В некоторых случаях компания проводит прямые продажи поставщикам, работающим на госзаказчиков, очень крупным сервис-провайдерам и основным системным интеграторам, т.е. компаниям, потребности которых уникальны и/или гарантируют большие объемы закупок.

Компания Fortinet обеспечивает своим канальным партнерам поддержку команды опытных аккаунт-менеджеров, менеджеров по продажам и пресейл-инженеров для бизнес-планирования, рахзработки стратегией совместного маркетинга, предпродажной поддержки и поддержки операционных продаж.

В структуру Fortinet также входит специальная группа продаж для управления и поддержки прямых продаж крупным предприятиям и сервис-провайдерам. Эта команда работает в тесном взаимодействии с партнерами по каналу Fortinet и напрямую общается с конечными заказчиками для решения их задач с уникальными требованиями по безопасности.

Для предоставления безупречного технического сервиса Fortinet использует свою глобальную команду поддержки и сервиса для клиентов (GCSS), распределенную между тремя региональными центрами экспертизы (COE). Каждый центр экспертизы дополняется региональными центрами поддержки для обеспечения более широкого языкового и географического покрытия.



Для поддержки ваших самых ответственных проектов Fortinet может предложить следующее:

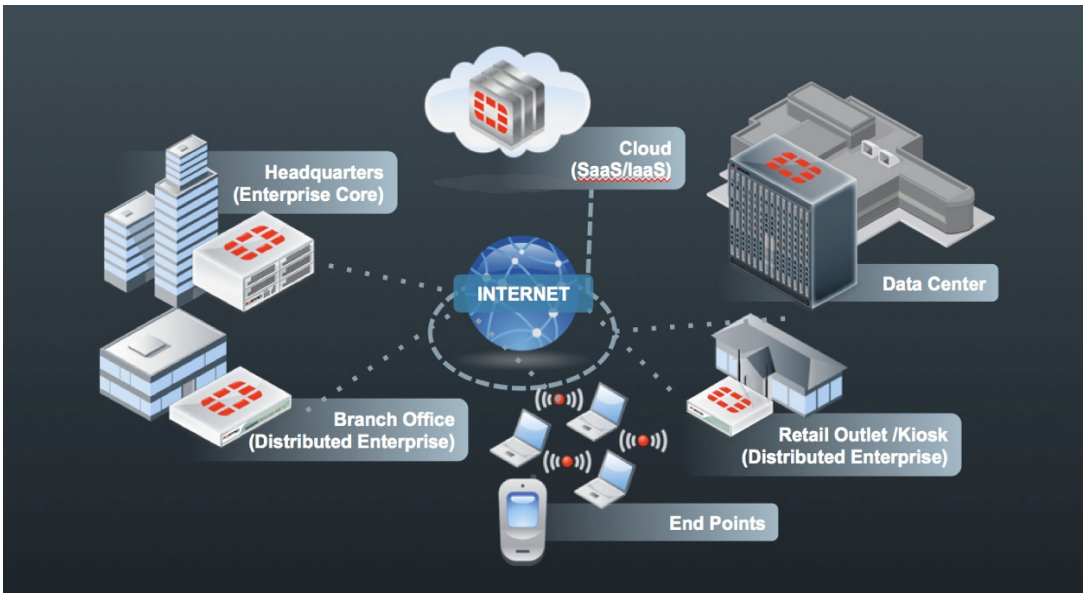
- Расширенная поддержка - включает поддержку в режиме 24x7, поддержку по телефону и расширенный сервис по замене оборудования с доставкой на следующий рабочий день;
- Премиум сервисы - могут включать быстрый доступ к нашим инженерам поддержки; предоставление выделенного технического аккаунт-менеджера (TAM); расширенные SLA; пожизненную поддержку развернутого ПО Fortinet; расширенные опции RMA, например, доставка на следующий день в режиме 24x7, выезд курьера к Заказчику в течение 4 часов, выезд инженера на площадку Заказчика в течение 4 часов.

В штате Fortinet также есть опытные консультанты, предназначенные для плотной работы с нашими клиентами в любой стране по всему набору задач, планированию сроков, ресурсов и качества проекта. Профессиональные сервисы Fortinet FortiCare могут поддерживать ваши проекты на всех фазах жизненного цикла: архитектура и разработка; внедрение и развертывание; переход и миграция.

5. ОБЗОР РЕШЕНИЙ БЕЗОПАСНОСТИ FORTINET

Портфолио решений Fortinet позволяет обеспечить защиту широчайшего спектра видов корпоративной информационной инфраструктуры - от проводных/беспроводных сетей и систем передачи сообщений до веб-приложений, баз данных и так далее, - позволяя заказчикам гарантировать защиту и контроль своих сетей, пользователей и данных.

В то же время решения централизованного управления и отчетности Fortinet позволяют заказчикам эффективно управлять и наблюдать за любым внедренным решением Fortinet, от нескольких устройств до тысяч. С нашими решениями клиенты получают выгоду от упрощенного управления, расширенного контроля и полного обзора состояния их безопасности в реальном времени.



5.1 Платформа сетевой безопасности FortiGate

Платформа сетевой безопасности FortiGate обеспечивает наилучший уровень быстродействия и защиты, упрощая структуру и управление сетью. Модельный ряд устройств Fortinet удовлетворяет любым требованиям к развертыванию систем, от десктоп-серии FortiGate-20 для малых офисов и розничных сетей до шассийной серии FortiGate-5000 для крупных предприятий, сервис-провайдеров, центров обработки данных и операторов связи.

Платформы сетевой безопасности Fortinet отвечают всем требованиям по обеспечению сетевой безопасности.

- **Высокопроизводительные межсетевые экраны для ЦОД**
- Шасси и серверы-лезвия серии FortiGate-5000 предназначены для высокоскоростных сетей сервис-провайдеров, ЦОД и сетей телеком-операторов. Поддержка 10-GbE и гибкая архитектура AdvancedTCA™ (ATCA) позволяет серии FortiGate-5000 обеспечивать защиту комплексных, многопользовательских, облачных сред класса «инфраструктура как сервис» и «безопасность как сервис».
- Серия устройств FortiGate-3000 обеспечивает интегрированную безопасность сети с высоким быстродействием для крупных предприятий и провайдеров, предоставляющих услуги по управлению сервисами. Устройства FortiGate-3000 предлагают высокую пропускную способность за счет процессоров ускоренной обработки FortiASIC, высокую плотность портов и гибкость при развертывании.

- **NGFW (МСЭ следующего поколения)**

Модели МСЭ FortiGate для предприятий предоставляют функциональность межсетевых экранов следующего поколения (NGFW) с исключительной пропускной способностью, ультранизкой задержкой и многовекторной защитой от угроз. NGFW платформы FortiGate обеспечивают функционал системы предотвращения вторжений (IPS) с глубоким сканированием пакетов (DPI), возможность идентифицировать и контролировать работающие через сеть приложения, а также возможность верификации пользователей и соблюдения политик доступа. Возможности Fortinet по расширенной защите от угроз (ATP) можно использовать для борьбы и смягчение эффекта от расширенных целенаправленных атак.

- **UTM (Unified Threat Management)**

Семейство UTM платформ FortiGate предоставляет вам возможность найти правильное сочетание быстродействия и цены, подходящее именно для ваших специфических требований. Компания Fortinet предлагает больше моделей и опций технологии безопасности, чем любой другой производитель на рынке, делая наши UTM решения идеальными для организаций с ограниченными ИТ-ресурсами. Каждое устройство FortiGate соединяет в себе технологии безопасности ядра, такие как межсетевой экран, IPS, контроль приложений, фильтрация веб-контента, VPN, противодействие шпионскому ПО, оптимизация WAN, анти-спам и т.д. и т.п.

5.2 Решения Fortinet для безопасной WLAN

Решения по безопасности для беспроводной ЛВС от Fortinet основаны на предположении, что существует единая сеть, независимо от того, каким способом к ней подключаются пользователи - через проводной, беспроводной, либо удаленный доступ. Сетевая инфраструктура интегрируется, представляя собой единую комплексную инфраструктуру безопасности с общим набором правил и политик, которые определяют разрешенный уровень доступа для пользователей, основываясь на их потребностях, а не на их способа доступа.

Решение для безопасности беспроводной сети Fortinet's включает три компонента.

- **1. Беспроводной контроллер – FortiGate**

Платформа сетевой безопасности FortiGate служит в качестве беспроводного контроллера для тонких точек доступа FortiAP™, позволяя интегрировать защиту WLAN, управляемую из единой консоли. Эта стандартная функция FortiGate не требует никаких дополнительных лицензий. Необходимо единожды выбрать подходящую модель FortiGate для сети, дополнительные издержки – это затраты на то количество и тип точек доступа FortiAP, которые необходимы для создания сети.

- **2. «Тонкая» точка доступа – FortiAP**

Точка доступа FortiAP - это рентабельная 802.11n/ac «тонкая» точка доступа, которая обеспечивает интегрированную безопасность и доступ клиентам Wi-Fi сети. Диапазон FortiAP включает модели и для малых филиальных офисов, и для штаб-квартир с высокой плотностью пользователей, а также модели для наружного размещения или для размещения в условиях промышленного производства. В серии FortiAP используется лидирующая в отрасли технология беспроводного чипа, которая обеспечивает до 1,300 Мбит/с пропускной способности беспроводной сети на канал в обоих спектрах 2.4 ГГц и 5 ГГц.

- **3. «Толстая» точка доступа – FortiWifi**

FortiWiFi™ представляет собой единое устройство, в котором возможности беспроводной точки доступа интегрированы в платформу FortiGate. Это решение «все в одном» идеально подходит для малого и среднего бизнеса, корпоративных филиальных офисов, либо ритейла. Каждый FortiWiFi обеспечивает безопасный доступ для проводной и беспроводной ЛВС, так же, как и для различных WAN подключений, в едином рентабельном устройстве.

5.3 Безопасность почтовой системы FortiMail

Решение FortiMail™ является мощной платформой безопасного обмена сообщениями, которая предотвращает превращение систем доставки сообщений в системы доставки угроз. FortiMail – это решении «все в одном», которое обладает таким функционалом как анти-спам, антивирус, анти-фишинг, защита от вредоносных программ, предотвращение утечки данных, шифрование по идентификации (IBE), архивация сообщений, защита от занесения в черный список.

Механизм входящей фильтрации блокирует спам и вредоносные программы до того, как они заразят сеть и затронут пользователей. Технология проверки исходящей корреспонденции предотвращает генерацию исходящего спама или вредоносных программ (включая мобильный трафик 3G), исключая возможность добавления вашего сервера в черный список другими анти-спам шлюзами.

Система FortiMail постоянно выигрывает награду VBSpam Platinum за обладание одним из лучших показателей срабатывания в распознавании и наименьшей частотой ложных

срабатываний. Механизм защиты FortiMail от вредоносных программ получил многочисленные награды VB100.

Доступны различные модели для соответствия потребностям в быстродействии организации любого размера, от малого бизнеса до телеком-операторов, сервис-провайдеров и крупных корпораций. Система FortiMail может быть развернута в «облаке» или в серверной, в любом шлюзе, сети, и/или на различных моделях серверов. Система FortiMail доступна в устройствах различного форм-фактора или в виде виртуальных машин.

5.4 МСЭ для веб приложений FortiWeb

Межсетевой экран для веб приложений FortiWeb™ защищает веб-приложения и данные, открытые для доступа через Интернет, от атак и утечки данных.

Решение FortiWeb выходит за рамки традиционных МСЭ для веб-приложений, обеспечивая усиление безопасности XML, ускорение приложений и балансировку нагрузки на серверы. Решение FortiWeb использует усовершенствованные технологии, предоставляя двунаправленную защиту против вредоносных источников, атак на отказ сервиса (DoS) на уровне приложений и сложных угроз, таких как внедрение SQL-кода и межсайтовый скриптинг. Платформы FortiWeb помогают предотвращать кражу личных данных, финансовое мошенничество, и атаки на отказ сервиса. Они обеспечивают мониторинг и реализацию требований регулирующих органов, лучших отраслевых практик и внутренних политик.

Модельный ряд FortiWeb, включающий платформы для средних и крупных предприятий, сервисов приложений и провайдеров SaaS, позволяет кардинально уменьшить время развертывания и сложность внедрения и защиты веб-приложений.

5.5 Защита от распределенных атак FortiDDoS

Семейство специализированных устройств FortiDDoS™ обеспечивает обнаружение и предотвращение распределенных атак на отказ сервиса (DDoS), используя возможность мониторинга сетевого трафика в реальном времени.

Решение FortiDDoS помогает защитить от угроз и сбоев в обслуживании инфраструктуру, открытую для доступа из сети Интернет, путем хирургически точного отсечения DDoS-атак сетевого уровня и уровня приложений. Эти масштабируемые высокопроизводительные устройства предоставляют реальную защиту от DDoS и полностью совместимы с существующими технологиями безопасности и сетевой инфраструктурой.

Ключевые функции и достоинства:

- Детализированное отображение и управление сетью.
- Автоматическое обнаружение и минимизация трафика атаки.
- Встроенное прозрачное подавление угроз упрощает настройку и управление защитой от DDoS целенаправленных атак, очагов червей, DDoS/Botnet атак и прочего.
- Разделение и виртуализация устройств FortiDDoS позволяет назначать свою политику безопасности для каждого сегмента сети в многопользовательских средах.
- Централизованное оповещение, ролевая модельдоступа и порталы самообслуживания обеспечивают гибкость управления и интеграции.

5.6 Расширенная защита от угроз FortiSandbox

Решение FortiSandbox™ - это усовершенствованное устройство защиты от угроз, предназначенное для идентификации и помощи в пресечении расширенных целенаправленных атак (APT), которые все чаще обходят традиционные системы защиты сетей.

Решение FortiSandbox сочетает в едином устройстве уникальную двухуровневую «песочницу» (изолированная среда, куда помещается загружаемый извне код на время его выполнения), механизм динамического распознавания угроз, панель отображения состояния сетевой безопасности в режиме реального времени и богатый функционал отчетности. Это устройство может работать самостоятельно либо в связке с МСЭ нового поколения FortiGate и шлюзом электронной почты FortiMail для обеспечения углубленной проверки подозрительных или высокорисковых файлов в изолированной среде и подготовки соответствующих обновлений системы защиты на основе анализа полного жизненного цикла раскрытых атак.

Ключевые особенности и преимущества:

- Эмуляция программного кода для оперативной проверки в независимой среде в режиме реального времени.
- Безопасная виртуальная среда для развертывания вновь обнаруженных угроз и исследования их полного жизненного цикла.
- Встроенные анализаторы вредоносного кода, URL и ботнетов, предназначенные для предварительной фильтрации и последующего анализа угроз.
- Развитая система отчетности с категоризацией рисков, обеспечивающая быструю корректировку и обновление защиты.
- Проверка трафика всех уровней в одном устройстве, обеспечивающая простоту развертывания и снижение издержек.
- Возможность обращения в FortiGuard для получения обновлений и рекомендаций по исправлению недостатков.

5.7 Виртуальные решения от Fortinet

Виртуальные устройства Fortinet и виртуальные домены обеспечивают такой же уровень защиты и набор функций для виртуальной инфраструктуры, как и аппаратные решения Fortinet. Компания Fortinet разработала виртуальные версии следующих продуктов: FortiGate, FortiManager, FortiMail, FortiAnalyzer, FortiWeb, FortiCache и FortiScan, предоставляя заказчикам возможность получить все преимущества сервисов сетевой безопасности и передачи данных, доступных на аппаратных устройствах Fortinet. Виртуальные устройства Fortinet поддерживаются на виртуальных средах VMware, Xen, Microsoft Windows Server Hyper-V и Kernel-based Virtual Machine (KVM).

Виртуальные и физические устройства Fortinet позволяют использовать сегментацию сети в многопользовательских средах. На виртуальных или физических устройствах Fortinet возможно создавать виртуальные домены (VDOM) и виртуальные домены администрирования, чтобы разделить сеть на отдельные домены для разных абонентов или бизнес-подразделений.

Виртуализация системы сетевой безопасности с помощью функций Fortinet VDOM обеспечивает изоляцию виртуальных доменов, предоставляя администраторам возможность гибкой настройки и управления трафиком. Эта уникальная возможность обеспечивает прозрачность и контроль безопасности между зонами, сохраняя при этом все преимущества виртуализации.

5.8 Платформа Ethernet коммутации FortiSwitch

Семейство коммутаторов FortiSwitch™ включает модели Gigabit Ethernet (GbE), 10 Gigabit и Power over Ethernet (PoE) - коммутационные платформы для сетей высокоскоростной проводной передачи данных, характеризующиеся ультранизкой задержкой, высокой плотностью портов и максимальной масштабируемостью.

Коммутаторы Fortinet разработаны для построения высокопроизводительной сетевой инфраструктуры, предназначенной, например, для суперкомпьютерных вычислителей, для высокоскоростных взаимосвязанных приложений серверной виртуализации, для консолидации центров обработки данных или для облачных вычислений.

Технология vScale, реализованная в коммутаторах FortiSwitch, позволяет в реальном времени отслеживать и динамически перераспределять потоки трафика по наименее загруженным маршрутам в коммутируемой сети, что помогает избегать заторов, и при этом сохраняет полную совместимость со стандартами Ethernet.

Линейка продуктов FortiSwitch:

- **Защищенные коммутаторы уровня доступа**

Интеграция коммутаторов уровня доступа с устройствами FortiGate обеспечивает возможность администрирования коммутатора и управление безопасностью портов доступа через интерфейсы FortiGate либо FortiManager. Такие коммутаторы идеально подходят организациям любого размера и обеспечивают полный контроль и управление сетевой безопасностью и доступом.

- **Коммутаторы уровня доступа**

Идеально подходящие для малого и среднего бизнеса, филиалов и офисов, эти коммутаторы обеспечивают максимальную гибкость, простоту и полезность. Поддержка PoE позволяет реализовать интеграцию с беспроводными точками доступа, IP-телефонами и другим оборудованием PoE.

- **Коммутаторы для ЦОД**

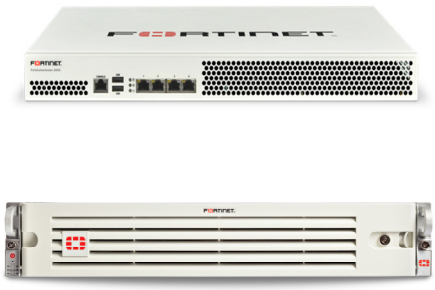
Соответствуют требованиям к плотности портов для высокоскоростных Ethernet-сетей в центрах обработки данных, обеспечивая высокую производительность 10-гигабитной коммутационной платформы в сочетании с низкой стоимостью владения. Эти специализированные коммутаторы идеально подходят для применения в качестве стоечных «top of rack» коммутаторов, для выполнения функций коммутаторов уровня ядра крупной сети или граничных коммутаторов.

5.9 Управление и отчетность Fortinet

Решения Fortinet для централизованного управления и формирования отчетности позволяют заказчикам эффективно управлять и осуществлять мониторинг любых сетей на базе оборудования Fortinet, от нескольких устройств до тысяч виртуальных и аппаратных устройств и агентов безопасности. Наши решения обеспечивают многообразие типов инфраструктуры, гибкость, подстройку под потребности заказчика через API, а также простую схему лицензирования.

Устройства **FortiManager™** обеспечивают простую централизованную настройку, сквозной мониторинг сети, предоставление доступа и сервисов на основе политик и управление обновлениями для инсталляций Fortinet.

Сетевые администраторы получают возможность более эффективно управлять сетью с помощью логического группирования устройств в виртуальные домены администрирования (ADOMs), применения политик и распространения обновлений прошивки.



Устройства **FortiAnalyzer™** собирают, анализируют и строят отчеты по журналам событий от продуктов Fortinet и других устройств, поддерживающих протокол syslog. Это централизованное решение отчетности имеет полный набор индивидуализируемых отчетов, позволяя пользователям фильтровать и просматривать записи для быстрого анализа и визуализации сетевых угроз, потерь производительности и степени загруженности. Предустановленные и персонализированные диаграммы помогают распознавать модели атак, контролировать соответствие установленным политикам.

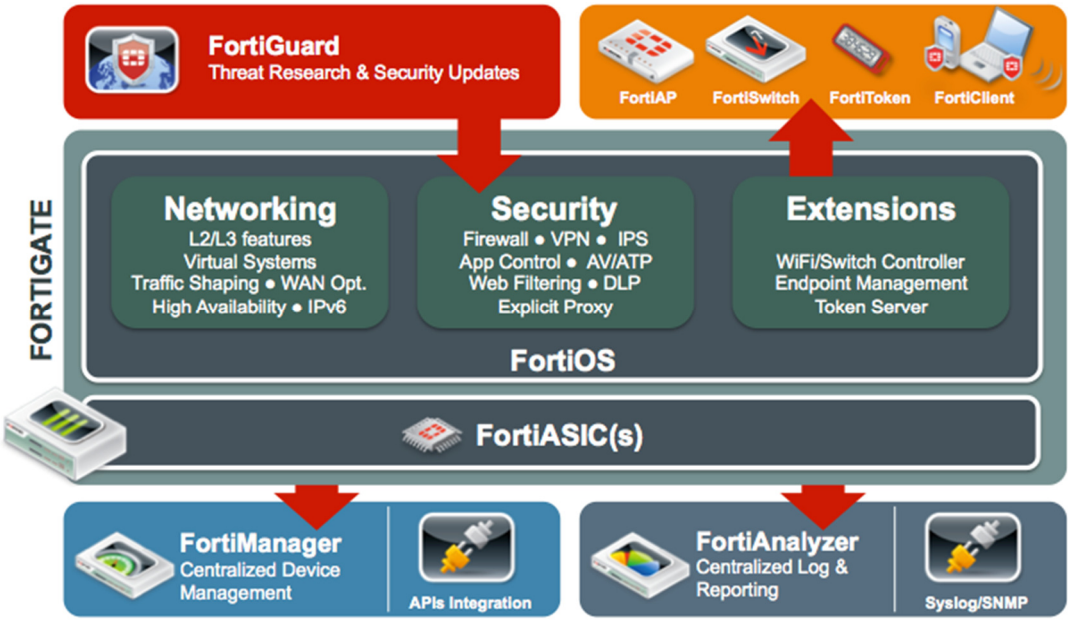
Решение FortiAnalyzer также предоставляет расширенные функции управления безопасностью, такие как архивирование файлов, находящихся в карантине, корреляция событий, оценка уязвимостей, анализ трафика, а также архивация электронной почты, данных о веб-доступе, мгновенных сообщений и содержания передаваемых файлов.

Для организаций, которым требуется максимальная гибкость решения и масштабируемость, оба решения FortiManager и FortiAnalyzer доступны в виде виртуальных устройств. Совместно они предоставляют функции наблюдения и управления, необходимые для обеспечения безопасности физической и виртуальной инфраструктуры организации.

6. ОБЗОР ФУНКЦИЙ FORTIOS

6.1 Обзор

Операционная система FortiOS – это фундамент для всех платформ сетевой безопасности Fortinet FortiGate. Она обеспечивает гибкую интеграцию и безопасность для всех типов сетевой инфраструктуры и для любого уровня требований. FortiOS характеризуется простотой управления через интуитивно понятный веб-интерфейс и предлагает множество функций мониторинга и оповещения, которые важны для реагирования на сетевые угрозы. Операционная система FortiOS помогает расширить безопасную зону через управление рядом дополнительных продуктов Fortinet.



ПРИМЕЧАНИЕ: на различных моделях и версиях прошивки реализованы различные наборы функций, не все указанные выше функции доступны для любой модели или прошивки. Для получения полной, детальной и актуальной информации следует ознакомиться с другими

официальные документами Fortinet.

6.2 Сетевой функционал

Операционная система FortiOS предлагает надежные сетевые возможности, которые являются непревзойденными в отрасли. Эти функции необходимы для поддержки различных сетевых топологий, которые могут потребоваться организациям для создания инфраструктур с высокой устойчивостью, с особыми требованиями к сетевой среде, либо для облегчения интеграции в существующую инфраструктуру.

Операционная система FortiOS поддерживает следующие сетевые технологии:

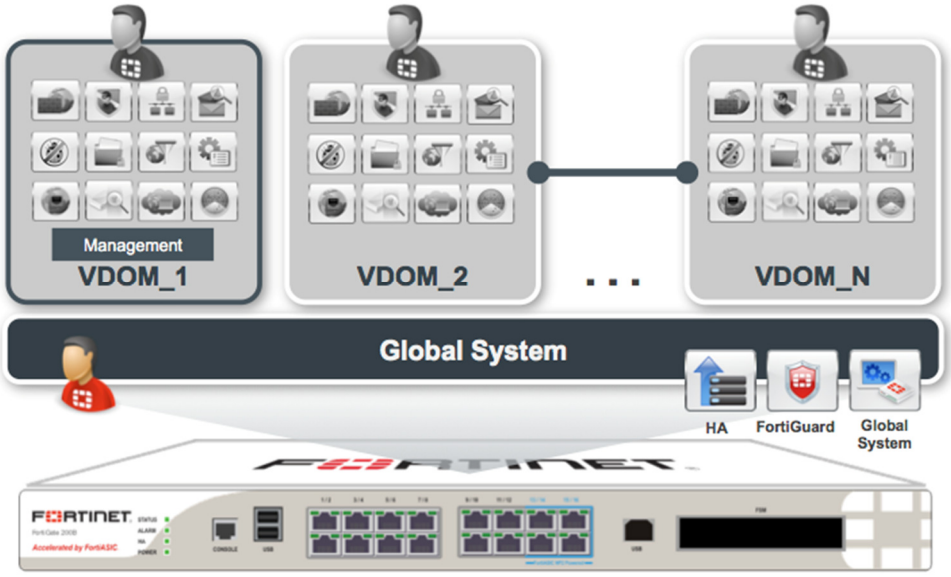
- Сетевые сервисы - NTP, DNS и DHCP;
- Взаимодействие с WAN технологиями PPPoE и DDNS;
- Протоколы динамической маршрутизации - RIPv1 и v2, OSPF v2 и v3, ISIS, BGP4;
- Многоадресный трафик: рассеянный и плотный режимы, поддержка PIM;
- Статическая маршрутизация и маршрутизации на основе политик;
- Балансировка нагрузки WAN по алгоритму маршрутизации множественных путей ECMP (Equal Cost Multi-Path) и резервирование;
- Контекстно-зависимая маршрутизация: WCCP & ICAP;
- Поддержка IPv6: управление через IPv6, протоколы маршрутизации IPv6, туннелирование IPv6, МСЭ и UTM для IPv6 трафика, NAT46, NAT64, IPv6 IPSEC VPN;
- Различные режимы работы интерфейса: sniffer, агрегирование портов, loopback, VLAN (802.1Q и Trucking), аппаратный и программный коммутатор (доступно на большинстве моделей).

Требование высокой доступности зачастую является обязательным для современных сетей, так как ИТ инфраструктура тесно связана с работоспособностью бизнеса и сервисов. Операционная система FortiOS обеспечивает полный набор настроек для кластера высокой доступности (HA), в том числе:

- Резервный интерфейс heartbeat;
- Резервный интерфейс управления HA;
- Обнаружение отказа:мониторинг портов, локальных и удаленных соединений;
- Функции аварийного переключения: с учетом состояния (stateful), subsecond;
- Информирование об обнаружении отказа через журнал событий и SNMP;
- Различные режимы: Active-Passive, Active-Active, виртуальные кластеры, VRRP, кластеризации серий FG-5000.

Кроме контроля сетевого трафика FortiOS также позволяет повысить доступность и удобство доступа пользователей к критичным приложениям с помощью WAN оптимизации и технологии ограничения пропускной способности каналов для разных видов трафика (traffic shaping). Для обеспечения чувствительных сетевых транзакций FortiOS может использовать веб-кэширование или другие технологии оптимизации WAN. Администраторы могут назначать ширину канала или приоритеты для определенных потоков трафика или даже для приложений.

Компания Fortinet была пионером в создании виртуальных систем. Операционная система FortiOS предлагает функциональность виртуальных систем, называемую VDOM. Виртуальные домены (VDOM) разделяют шлюз безопасности FortiGate на два или более (до 250) виртуальных устройства FortiGate, каждое из которых работает как независимый шлюз безопасности FortiGate. Каждый VDOM может обеспечить полностью раздельное межсетевое экранирование, маршрутизацию, UTM, VPN и сервисы МСЭ следующего поколения. Весь входящий и исходящий трафик каждого VDOM полностью независим от трафика других VDOM.



6.3 Функционал безопасности

Технологии безопасности FortiOS предоставляют интегрированную высокопроизводительную защиту против современных расширенных и целенаправленных угроз широкого спектра для приложений, данных и пользователей. Для защиты сетей против вновь появляющихся угроз FortiOS включает разнообразные компоненты интегрированной безопасности, которые позволяют организациям применять защиту, соответствующую их меняющимся потребностям, без усложнения либо добавления дополнительного оборудования.

Ключевые компоненты безопасности

МСЭ

Основная функция МСЭ на FortiOS - контроль входящего и исходящего сетевого трафика путем анализа пакеты данных и разрешения либо запрета на их пропуск в соответствии с набором заранее установленных правил, при этом другие функции, такие как журналирование и аутентификация, опциональны. Используя свои политики, устройство FortiGate разрешает или запрещает пакеты и информацию, входящие или исходящие из сети, решает, кто получит приоритет (ширину канала) перед другими пользователями и когда пакеты могут проходить. В сочетании с чипами FortiACIS устройство FortiGate предлагает чрезвычайно привлекательное сочетание цена/быстродействие.

VPN

Технология Fortinet VPN позволяет организациям устанавливать защищенные соединения и обеспечивать конфиденциальность передачи данных между множеством сетей и хостов, используя протоколы IPsec и SSL VPN, при этом поддерживаются и другие VPN технологии. Возможности обоих VPN сервисов усиливаются применением специализированных сетевых процессоров FortiASIC™ для ускорения операций по шифрованию и дешифрованию сетевого трафика. После дешифрации трафика для всего контента, проходящего через VPN туннель, может применяться множество средств проверки на наличие угроз, включая антивирусы, системы предотвращения вторжений, контроль приложений, средства фильтрации сообщений электронной почты и веб-фильтрации.

Система предотвращения вторжений (IPS)

Система предотвращения вторжений IPS на FortiOS предлагает широкий спектр функций, которые могут быть использованы для мониторинга и блокирования нежелательной сетевой активности, в том числе: предустановленные и персонализированные сигнатуры, декодирование протокола, режим управления по вспомогательному каналу out-of-band (или режим однорукого IPS), журналирование пакетов и IPS сенсоры. IPS сенсоры обеспечивают централизованный набор инструментов с удобной настройкой. Технология IPS поддерживается автоматической доставкой в режиме реального времени обновлений от сервисов FortiGuard, имеющих базу данных с тысячами уникальных сигнатур атак, в том числе уязвимостей «нулевого дня».

Контроль приложений

Контроль приложений необходим для управления огромным количеством новых Интернет-технологий, бомбардирующих современные сети. Контроль приложений от Fortinet расширен и усилен благодаря наличию одной из самых крупных в мире базы данных сигнатур приложений - базы данных контроля приложений FortiGuard. Это позволяет вам контролировать более 3 000 различных веб-приложений, программных продуктов, сетевых сервисов и протоколов. Администраторы также могут визуально контролировать загруженность сети через встроенный виджет, отображающий очереди в режиме реального времени и отчеты.

Антивирус

Антивирусная технология Fortinet сочетает метод обнаружения вирусов на основе сигнатур и эвристический метод, что обеспечивает многоуровневую защиту в режиме реального времени от вновь появившихся и эвролюционирующих вирусов, шпионского ПО и другие видов вредоносных атак через веб-трафик, электронную почту и файловый трафик. Процессоры обработки контента FortiASIC™ ускоряют работу антивирусной защиты как в режиме прокси, так и режиме обработки потока. Обнаружение неизвестных и целенаправленных постоянных атак становится возможным с помощью передачи подозрительных файлов в облачные либо аппаратные системы проверки sandbox.

Веб фильтрация

Кроме традиционных списков блокирования URL, возможности FortiOS по фильтрации веб-трафика предлагают широкий набор процедур по детализированному контролю веб-трафика периметра, таких как мониторинг, предупреждение пользователя или переопределение пользователя. Используя технологию FortiOS по фильтрации веб-контента, FortiGate может классифицировать и фильтровать веб-трафик по различным предустановленным и настраиваемым правилам, предоставляемых сервисом облачной базы данных FortiGuard. FortiOS имеет и более продвинутые возможности, такие как «принуждение к безопасному поиску» и «предотвращение уклонения от прокси».

DLP

Решение FortiOS по предотвращению утечки данных использует техники сопоставления с образцом на базе сложных шаблонов и идентификацию пользователей для обнаружения и предотвращения неавторизованной передач конфиденциальной информации и файлов через периметр сети. Функции Fortinet DLP включают технологию сравнения «цифровых отпечатков» файлов документов и исходного файла документа, расширенный шаблоны сопоставления и архивацию данных.

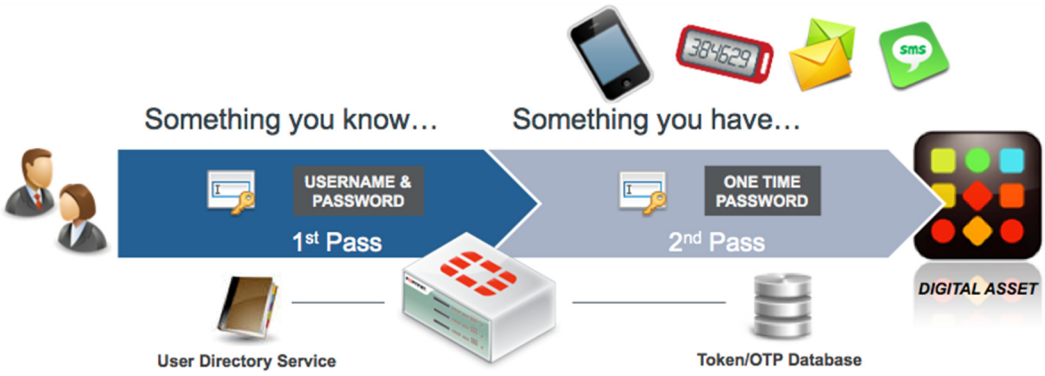
6.4 Дополнительные возможности

Операционная система FortiOS позволяет администраторам расширить сферу сетевой защиты, предоставляя контроль над дополнительными интерфейсами и периферийными устройствами безопасности. Это предоставляет полезные преимущества, такие как упрощение внедрения систем безопасности и снижение стоимости владения.

Устройства FortiGate могут расширять свой функционал и число интерфейсов, используя возможности коммутатора и беспроводного контроллера. Операционная система FortiOS может работать как контроллер доступа для тонких точек доступа Fortinet и коммутаторов, обеспечивая следующие возможности:

- Управление и распространение настроек для локальных и удаленных тонких точек доступа или коммутаторов;
- Настройка доступа и метода аутентификации для SSID или VLAN (поддерживает технологию captive portal);
- Усиление безопасности WiFi - подавление незарегистрированных точек доступа и поддержка технологии предотвращения вторжений Wireless IDS;
- Поддержка различных беспроводных технологий: быстрый роуминг, балансировка точек доступа, wireless mesh, wireless bridging.

Операционная система FortiOS облегчает развертывание системы безопасности для мобильных пользователей. Специальное ПО FortiClient Endpoint Security обеспечивает усиленную защиту клиентских устройств, работающих под управлением MAC OS X, Windows, Android и iOS, и может загружать настройки безопасности в приложения клиента, включая настройки для антивируса, веб-фильтрации, межсетевого экранирования и VPN.



Метод двухфакторной аутентификации улучшает безопасность и снижает риск компрометации, свойственный методам однофакторной аутентификации, таким как постоянный пароль. FortiOS предлагает интегрированный сервер ключей Token, который предоставляет и управляет физическими и программными ключами FortiToken. Этот сервер также способен доставлять коды через SMS и электронную почту.