Линейки продуктов SonicWall

Обзор

Обеспечьте безопасность публичного/частного облака, приложений, пользователей и данных вашей организации, применяя глубокий уровень защиты, который не будет влиять на производительность сети. Облачная платформа SonicWall Capture тесно интегрирует безопасность, управление, аналитику и оценку угроз в режиме реального времени в портфеле решений для сети, беспроводных технологий, электронной почты, мобильной связи, веб и облачной безопасности. Этот подход позволяет предприятиям различного масштаба – от малых и средних до крупных, правительственным организациям, точкам розничной торговли, образовательным организациям, здравоохранению и сервис-провайдерам испытать нашу полную экосистему безопасности, которая использует мощность, гибкость и масштабируемость облака.

Стратегия Capture Cloud Platform и видение будущего - это постоянные инновации и разработка контейнерных приложений безопасности как услуги, которые легко программируются и предоставляются по требованию. Она состоит из 10 ключевых компонентов и функциональных возможностей:

- Сетевой безопасности;
- Безопасности беспроводных сетей;
- Безопасности веб-приложений;
- Безопасности конечных точек;
- Безопасности облачных приложений;
- Расширенных сервисов безопасности;
- Удаленного доступа;
- Безопасности электронной почты;
- Управления безопасностью и аналитики.

Сочетание этих функций обеспечивает критически важную многоуровневую киберзащиту, оценку угроз, анализ и совместную работу, а также общее управление, отчетность и аналитику, которые работают вместе и синхронно.

Продукты сетевой безопасности

SonicWall является одним из ведущих поставщиков межсетевых экранов (МСЭ) нового поколения (МСЭНП). В основе каждого МСЭНП SonicWall лежит проверенная операционная система SonicOS. SonicOS использует нашу масштабируемую, многоядерную аппаратную архитектуру, а также нашу запатентованную систему глубокой проверки памяти в реальном времени (RTDMI™) и нашу запатентованную* однопроходную глубокую проверку пакетов без их сборки (Reassembly-Free Deep Packet Inspection®, RFDPI) с малой задержкой для сканирования всего трафика независимо от порта или протокола.

Наши МСЭНП обеспечивают проверку каждого байта каждого пакета, сохраняя при этом высокую производительность и низкую задержку, необходимые для загруженных сетей. В отличие от конкурентных предложений, механизм однопроходного RFDPI обеспечивает одновременное сканирование нескольких угроз и приложений, а также анализ файлов любого размера без повторной сборки пакетов. Это позволяет масштабировать МСЭНП от SonicWall, чтобы обеспечить современную защиту для растущих и распределенных корпоративных сетей и центров обработки данных.

МСЭ SonicWall предлагают широкий спектр надежных функций, в том числе:

- Облачную «песочницу» Capture ATP с несколькими механизмами проверки;
- SD-WAN;
- REST API;
- Расшифровку и проверку зашифрованного трафика;
- Сервис предотвращения вторжений (IPS);
- Защиту от вредоносного ПО;
- Аналитику, контроль и визуализацию приложений;
- Фильтрацию веб-сайтов/URL (контентную фильтрацию);
- Виртуальные частные сети (VPN) поверх SSL или IPSec;
- Безопасность беспроводных сетей;
- Гибридную и мультиоблачную безопасность;
- Аварийное переключение/восстановление с учетом состояний соединений.

Кроме того, МСЭ SonicWall, благодаря группе по исследованию угроз Capture Labs, обеспечивают быструю реакцию и постоянную защиту от угроз «нулевого дня». Эта группа собирает, анализирует и проверяет перекрестную векторную информацию об угрозах из различных источников информации, включая более миллиона датчиков, размещенных по всему миру в своей сети Capture Threat Network.

Серия устройств SonicWall Network Security services platform (NS*sp*)

Платформа МСЭНП серии SonicWall NS*sp* 12000 спроектирована для обеспечения в крупных сетях масштабируемости, надежности и глубокой защиты на мультигигабитных скоростях.

NSS Labs провела оценку МСЭ SonicWall с использованием одного из самых строгих реальных тестов производительности МСЭНП, и SonicWall продемонстрировал в ходе него высокую эффективность защиты, производительность, масштабируемость, надежность и низкую совокупную стоимость владения. В пятый раз МСЭ SonicWall установили стандарт для высокопроизводительного контроля приложений и предотвращения угроз в различных вариантах развертывания, от небольших предприятий до крупных центров обработки данных, операторов связи и сервис-провайдеров.

Серия NS*sp* 12000 обеспечивает высокий уровень качества обслуживания с бесперебойной доступностью сети и возможностями подключения, которые требуются современным предприятиям, правительственным учреждениям, сервис-провайдерам и университетам с инфраструктурой 40/10 Гбит/с. Используя инновационные технологии безопасности с глубоким обучением на облачной платформе SonicWall Capture, серия NS*sp* 12000 обеспечивает надежную защиту от самых современных угроз без снижения производительности.

**Патенты США 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723*

Серия устройств SonicWall Network Security appliance (NS*a*)

Серия устройств SonicWall Network Security appliance (NS*a*) – одна из самых безопасных и высокопроизводительных линеек МСЭНП. Она обеспечивает бескомпромиссную защиту и производительность бизнес-класса, используя ту же архитектуру, что и флагманская линия МСЭНП NS*sp* 12000, первоначально разработанную для самых требовательных операторов и предприятий. В то же время, она предлагает признанную простоту использования и высокий потребительский потенциал SonicWall.

Серия NS*a* была разработана с «нуля» на основе многолетних исследований и разработок для распределенных предприятий, предприятий малого и среднего бизнеса, филиалов, школьных кампусов и государственных учреждений. Серия NS*a* сочетает в своем высокомасштабируемом дизайне революционную многоядерную архитектуру с облачной технологией глубокой проверки памяти в реальном времени (RTDMI) и запатентованный однопроходный механизм предотвращения угроз RFDPI. Это обеспечивает лучшую в отрасли защиту, производительность и масштабируемость характеризующиеся наибольшим числом одновременных соединений, минимальной задержкой, отсутствием ограничений по размеру файлов и превосходными в своем классе показателями поддержки новых соединений в секунду.

Серия устройств SonicWall TZ

Серия SonicWall TZ состоит из высоконадежных МСЭ унифицированного управления угрозами (UTM) с высокой степенью защиты, предназначенных для малых и средних предприятий (SMB), розничных сетей, государственных организаций и распределенных предприятий с удаленными площадками и филиалами. В отличие от продуктов потребительского уровня, серия TZ объединяет высокоэффективные функции защиты от вредоносных программ, предотвращения вторжений, фильтрации контента/URL-адресов и контроля приложений в проводных и беспроводных сетях, вместе с широкой поддержкой мобильных платформ для ноутбуков, смартфонов и планшетов. Она обеспечивает полную глубокую проверку пакетов (DPI) с очень высоким уровнем производительности, устраняя узкие места в сети, которыми обычно становятся другие продукты, и позволяет организациям добиться повышения эффективности работы.

Как и все МСЭ SonicWall, устройство серии TZ для обеспечения полной защиты проверяет весь файл, включая файлы с шифрованием TLS/SSL. Кроме того, серия TZ предлагает распознавание и контроль приложений, расширенную аналитику и отчетность по трафику приложений, защиту с использованием протоколов IPsec и SSL VPN, аварийное переключение нескольких ISP, распределение нагрузки и SD-WAN. Дополнительные интегрированный модуль питания по Ethernet (PoE) и высокоскоростное беспроводное соединение 802.11ac позволяют организациям легко и безопасно расширять границы своей сети. В сочетании с коммутаторами Dell серий N и X устройства серии TZ обеспечивают гибкость для безопасного роста бизнеса без увеличения сложности инфраструктуры.

Серия SonicWall Network Security virtual (NS*v*)

Виртуальные МСЭ NS*v* расширяют возможности автоматического обнаружения и предотвращения взломов в гибридных и мультиоблачных средах с виртуализированными версиями МСЭНП SonicWall. Благодаря полнофункциональным средствам и сервисам безопасности, эквивалентным МСЭ SonicWall NS*a*, NS*v* эффективно защищает ваши виртуальные и облачные среды от атак с использованием нецелевого использования ресурсов, атак с использованием нескольких виртуальных машин, атак по побочным каналам, а также всех распространенных сетевых атак и угроз.

NS*v* легко развертывается и настраивается в многопользовательской виртуальной среде, обычно между виртуальными сетями (VN). Для автоматического предотвращения взлома он устанавливает меры контроля доступа для сохранения данных и безопасности виртуальных машин при захвате виртуального трафика между виртуальными машинами и сетями. Благодаря поддержке инфраструктуры для реализации высокой доступности (HA), NS*v* отвечает требованиям масштабируемости и доступности, предъявляемым к программно-определяемым центрам данных (SDDC). Легко развертывается как виртуальное устройство на платформах частного облака, таких как VMWare или Microsoft Hyper-V, или в общедоступных облачных средах AWS или Microsoft Azure. Используйте гибкую модель лицензирования NS*v* и предоставьте организациям все преимущества безопасности физического МСЭ с эксплуатационными и экономическими преимуществами виртуализации.

Серия устройств безопасности беспроводных сетей SonicWave

SonicWall делает беспроводные сети безопасными, простыми и доступными благодаря инновационному решению SonicWall Wireless Network Security. Это решение сочетает в себе высокопроизводительные беспроводные точки доступа SonicWave серии 802.11ac Wave 2 с SonicWall WiFi Cloud Manager (WCM) или ведущими в отрасли МСЭ SonicWall для обеспечения сетевой безопасности нового поколения и производительности в беспроводных сетях. WCM - это интуитивно понятная, масштабируемая и централизованная облачная система управления сетью WiFi, подходящая для сетей любого размера. Доступ к ней можно получить через Центр безопасности SonicWall Capture. Планировщик WiFi, доступный через WCM, позволяет оптимально спроектировать и развернуть сеть WiFi. При развертывании точек доступа мобильное приложение SonicWiFi позволяет настраивать, управлять и отслеживать беспроводные сети WiFi. Вместе эти беспроводные решения гарантируют безопасность пользователей Wi-Fi.

Наше решение выходит за рамки простых решений безопасности для беспроводных сетей, обеспечивая защиту беспроводных сетей с использованием технологий RTDMI и RFDPI и обеспечивая двойную защиту путем шифрования беспроводного трафика и его обезвреживания от сетевых угроз, а также защиту сети от беспроводных атак. Кроме того, точки доступа SonicWave обеспечивают расширенные функции безопасности, такие как Capture и CFS, непосредственно на точке доступа.

Благодаря быстрому роумингу пользователи могут без проблем перемещаться из одного места в другое. Богатый набор функций включает в себя автоматический выбор канала, анализ спектра, справедливость распределения эфирного времени, управление диапазонами и инструменты анализа сигналов для мониторинга и устранения неполадок. SonicWall снижает совокупную стоимость владения (TCO), позволяя администраторам избегать внедрения и отдельного управления дорогостоящим беспроводным решением, которое работает параллельно с существующей проводной сетью.

МСЭ веб-приложений SonicWall Web Application Firewall (WAF)

Серия SonicWall WAF защищает веб-приложения, работающие в частной, публичной или гибридной облачной среде. Он оснащен передовыми инструментами и сервисами веб-безопасности для обеспечения соответствия данных и веб-настроек нормативным требованиям, а также безопасности, бесперебойной работы и максимальной производительности веб-приложений. WAF использует свои возможности доставки приложений на уровне 7, которые обеспечивают балансировку нагрузки с учетом типа приложений, разгрузку SSL и ускорение для обеспечения устойчивости, а также расширенное цифровое взаимодействие.

В WAF используется комбинация механизмов глубокой проверки пакетов на основе сигнатур и профилирования приложений для защиты от типичных атак на веб-приложения, подобных тем, которые были описаны в проекте Open Web Application Security Project (OWASP), а также от более сложных угроз веб-приложениям, таких как атаки типа «отказ в обслуживании» (DoS) и контекстно-зависимые эксплойты. В дополнение к защите веб-приложений WAF также предотвращает утечку данных за счет использования методов маскирования данных и блокировки страниц для определенных шаблонов конфиденциальных данных, таких как информация о платежных картах (PCI) и идентификационных документов, выданных правительством.

Для оптимальной защиты от вредоносных загрузок, внедрения вредоносных программ или расширенных угроз WAF использует исследования угроз SonicWall Capture Labs и добавляет в свой набор сервисов веб-безопасности SonicWall Capture ATP и RTDMI™. Кроме того, API-интерфейсы предоставляют администраторам возможность программного мониторинга и управления операциями WAF для повышения автоматизации и эффективности веб-безопасности.

WAF обеспечивает экономические преимущества виртуализации по масштабированию и может быть развернут как виртуальное устройство в частных облаках на базе VMWare ESXi или Microsoft Hyper-V, или в средах публичных облаков AWS или Microsoft Azure.

Capture Client

Управление конечными точками и их безопасность имеют в современном деловом мире решающее значение. Когда конечные пользователи входят и выходят из сети со своими устройствами, а также когда неконтролируемые зашифрованные угрозы достигают конечных точек, необходимо что-то предпринять для их защиты. С ростом числа вымогательского ПО и постоянно реализуемой угрозой кражи учетных данных конечные точки являются полем битвы на современном ландшафте угроз.

Кроме того, администраторы борются за прозрачность и управление безопасностью конечных точек. Они также сталкиваются с необходимостью обеспечить постоянную гарантию безопасности клиента, а также простую в использовании и действенную аналитику и отчетность.

Продукты для защиты конечных точек существуют на рынке уже давно, однако администраторы все еще борятся за:

- Поддержание актуальности продуктов безопасности;
- Обеспечение соблюдения политик и соответствия;
- Получение отчетов;
- Защиту от угроз по зашифрованным каналам;
- Понимание предупреждений и необходимых ответных мер;
- Управление лицензиями;
- Защиту от вымогательского ПО;
- Защиту от атак, основанных не на файлах и от инфицированных устройств USB, обходящих защиту периметра.

SonicWall Capture Client - это унифицированная клиентская платформа, которая предоставляет множество возможностей защиты конечных точек. Это решение оснащено облачной консолью управления и полной интеграцией с МСЭ SonicWall нового поколения для унификации средств безопасности для клиентов SonicWall. В сочетании с возможностью принудительного применения политик SonicWall Capture Client может гарантировать, что на конечных точках запущено программное обеспечение безопасности и/или имеется встроенный сертификат SSL для проверки зашифрованного трафика. Кроме того, чтобы упростить проверку трафика SSL (DPI-SSL) и улучшить взаимодействие с конечным пользователем, клиент Capture позволяет администраторам передавать SSL-сертификаты конечной точке гораздо проще, чем это было раньше.

Кроме того, Capture Client оснащен усовершенствованным антивирусным механизмом, разработанным для предотвращения внедрения наиболее сложных вредоносных программ, с возможностью восстановления для возврата системы в предыдущее незараженное состояние. Кроме того, Capture Client Advanced интегрируется с защитой от сложных угроз SonicWall Capture Advanced Threat Protection (ATP) для проверки подозрительных файлов, в целях улучшения характеристик предотвращения атак перед их активацией.

Функционал SonicWall Capture Client включает в себя:

- Обеспечение выполнения требований безопасности;
- Управление сертификатами DPI-SSL;
- Постоянный поведенческий мониторинг;
- Высокоточные определения, достигаемые с помощью машинного обучения;
- Многоуровневые эвристические методы;
- Уникальные возможности возврата к предыдущему состоянию (только Capture Client Advanced);
- Интеграция с сетевой «песочницей» Capture Advanced Threat Protection (только Capture Client Advanced);
- Поиск в один клик подозрительных файлов в базе данных положительных и отрицательных решений системы Capture ATP;
- Защита от веб-угроз путем блокировки известных вредоносных сайтов и IP-адресов;
- Управление устройствами на основе политик для блокировки потенциально зараженных устройств хранения.

SonicWall WAN Acceleration (WXA)

Серия ускорителей WAN SonicWall WAN Acceleration (WXA) снижает задержку приложений и сохраняет полосу пропускания, значительно повышая производительность приложений WAN и удобство работы для малых и средних организаций с удаленными офисами и филиалами. После первоначальной передачи данных серия WXA значительно уменьшает весь последующий трафик, передавая по сети только новые или измененные данные. WXA дедуплицирует данные, проходящие через WAN, запоминает ранее переданные данные и заменяет повторяющиеся последовательности байтов идентификатором, тем самым уменьшая задержку приложения и экономя полосу пропускания. Другие функции ускорения включают кэширование данных, дедупликацию файлов, кэширование метаданных, HTTP (веб) кэширование и сжатие данных «на лету».

В отличие от автономных продуктов для ускорения WAN, решения WXA представляют собой интегрированные дополнения к МСЭ серий SonicWall NSa и TZ. Такой подход позволяет оптимизировать размещение, развертывание, настройку, маршрутизацию, управление и интеграцию WXA с другими компонентами, такими как VPN. При развертывании в сочетании с МСЭНП SonicWall, на котором работает служба анализа и управления приложениями, WXA предлагает уникальный комбинированный функционал как приоритизации трафика приложений, так и минимизации трафика между площадками, что обеспечивает оптимальную производительность сети.

Узнайте больше о продуктах сетевой безопасности SonicWall по адресу: www.sonicwall.com/en-us/products.

Сервисы сетевой безопасности и дополнительные продукты

Сервисы и дополнения сетевой безопасности МСЭ SonicWall обеспечивают высокоэффективную, расширенную защиту для организаций любого размера, помогая защищаться от угроз, усиливать контроль безопасности, повышать производительность и снижать затраты.

Сервисы и дополнения включают в себя:

- Пакет TotalSecure Advanced - межсетевой экран и пакет Advanced Gateway Security Suite («песочница» с несколькими механизмами обработки, антивирус, защита от шпионского ПО, система предотвращения вторжений, анализ приложений, контент/веб-фильтрация и поддержка 24x7);
- Пакет Advanced Gateway Security Suite - защита от сложных угроз Capture Advanced Threat Protection, антивирусная защита на шлюзе, защита от шпионских программ, система предотвращения вторжений, контент/веб-фильтрация и поддержка 24x7;
- Сервисы безопасности шлюза Gateway security services - антивирус на шлюзе, защита от шпионского ПО, система предотвращения вторжений, анализ и контроль приложений;
- Защита от сложных угроз Capture Advanced Threat Protection (ATP);
- Сервисы контентной фильтрации;
- Принудительный клиентский антивирус и защита от шпионского ПО;
- Сервис комплексной защиты от спама;
- Глубокая проверка пакетов зашифрованного трафика TLS/SSL (DPI-SSL);
- Анализ и контроль приложений;
- Система предотвращения вторжений (IPS).

Узнайте больше о сервисах сетевой безопасности и дополнениях по адресу: www.sonicwall.com/en-us/products/firewalls/security-services.

Глубокая проверка памяти

Патентованная технология SonicWall Real-Time Deep Memory Inspection (RTDMI) проактивно обнаруживает и блокирует неизвестные массовые вредоносные программы посредством глубокой проверки памяти в режиме реального времени. Доступный уже сейчас механизм с помощью облачной «песочницы» SonicWall Capture Advanced Threat Protection (ATP) выявляет и устраняет даже самые коварные современные угрозы, включая будущие эксплойты Meltdown.

Безопасность облачных приложений

Cloud App Security

SonicWall Cloud App Security обеспечивает безопасность нового поколения для приложений SaaS, таких как Office 365 и G Suite, защищая электронную почту, данные и учетные записи пользователя от расширенных угроз, обеспечивая при этом соответствие регулирующим требованиям в облаке. Если вы переходите в облако, SonicWall обеспечивает лучшую в своем классе защиту на основе API с низкой совокупной стоимостью владения, минимальными затратами на развертывание и удобством работы с пользователем.

Безопасность нового поколения для облачной электронной почты

В дополнение к традиционным уровням защиты электронной почты таким как проверки SPF, DKIM и DMARC, а также фильтрации URL-адресов за счет использования трех основных источников данных для черных списков URL, уникальная архитектура Cloud App Security обеспечивает защиту, которая невозможна для решений с внешним шлюзом:

1. **Дополнительный уровень расширенной защиты от угроз:** Cloud App Security блокирует фишинговые сообщения, пропущенные в Office 365 и G Suite. В решении используются машинное обучение, искусственный интеллект и анализ больших данных, что обеспечивает мощную защиту от фишинга, проверку вложений в «песочнице», анализ URL-адресов в момент нажатия на ссылку и защиту от имперсонации.
2. **Мониторинг входящей, исходящей и внутренней электронной почты:** Интеграция SaaS с Cloud App Security позволяет сканировать и помещать в карантин каждое электронное письмо до того, как оно попадет в почтовый ящик пользователя, независимо от того, поступает ли оно из-за пределов организации или от скомпрометированной внутренней учетной записи.
3. **Сканирование старых сообщений на наличие угроз:** При первом подключении Cloud App Security сканирует старые сообщения (даже закрытых учетных записей) на предмет потенциальных нарушений или компрометации учетных записей.
4. **Глобальный отзыв сообщений электронной почты:** Вредоносные сообщения могут быть отредактированы или отозваны в любое время, в случаях если они являются вредоносными, содержат конфиденциальную информацию или если сотрудник случайно выбрал вариант «ответа всем».

Поскольку защита электронной почты Cloud App Security применяется до ящика входящей почты, но после собственных фильтров Microsoft или Google (а также любого развернутого внешнего шлюза MTA), ее алгоритмы машинного обучения специально настроены для выявления угроз, которые эти фильтры могли пропустить. Cloud App Security также может включать результаты их сканирований в свои собственные алгоритмы обнаружения.

Безопасность нового поколения для пакета офисных приложений

Cloud App Security предлагает полную, всестороннюю защиту для Office 365 или G Suite. Используете ли вы электронную почту, общие диски, мгновенные сообщения или полную среду совместной работы, решение поможет вам выполнить следующие действия по обеспечению безопасности:

1. Предотвратить распространение фишинга и вредоносного ПО внутри вашей организации или среди ваших клиентов и партнеров.
2. Проверить каждый файл на наличие вредоносного содержимого, используя «песочницу» Capture ATP и анализ активного контента, чтобы изолировать угрозы перед их загрузкой пользователями.
3. Выявить конфиденциальную информацию и применить облачные политики, которые удержат ее в пределах организации или рабочей группы. Ваши пользователи смогут использовать все возможности облачного офисного пакета, в то время как автоматизированные рабочие процессы обеспечат соблюдение требований, гарантируя, что PCI, HIPAA, PII или другие конфиденциальные данные не будут передаваться вовне.

Безопасность штатного IT

SonicWall Cloud App Security анализирует весь трафик (журналы событий, действия пользователей, файлы данных и объекты, состояние конфигурации и т. д.) и обеспечивает необходимые политики безопасности посредством прямой интеграции с собственными API-интерфейсами облачных сервисов. Поскольку решение использует собственные API-интерфейсы, оно не использует прокси-сервер и не находится между пользователем и облаком. Это позволяет решению обеспечить покрытие для санкционированных приложений независимо от устройства или сети пользователя. Кроме того, подход, основанный на API, обеспечивает простоту развертывания, детальный контроль и отсутствие влияния на работу пользователя.

Видимость и контроль «теневого» IT

МСЭНП SonicWall анализирует и регистрирует весь трафик, входящий и исходящий из сети. Журналы, сгенерированные для данных исходящего трафика, не четко различают используемые облачные приложения и не дают оценку риска для каждого приложения, используемого сотрудниками. Для удаленных сотрудников, перенаправленных через МСЭНП с использованием VPN, решение собирает дополнительную информацию из этих журналов о действиях, которые пользователи выполняют в облачных сервисах. Cloud App Security обрабатывает файлы журналов от МСЭНП SonicWall и выявляет, какие облачные сервисы используются какими пользователями, объемы данных, загружаемые и выгружаемые из облака, а также риски и категории каждого облачного сервиса. По сути, Cloud App Security делает существующую инфраструктуру ориентированной на облака. Благодаря тому, что сотрудники все чаще используют облачные приложения для работы, Cloud App Security позволяет администраторам обнаруживать пробелы в состоянии безопасности, классифицировать облачные приложения на санкционированные и несанкционированные и применять политики доступа для блокирования рискованных приложений. Безопасность облачных приложений является важной частью концепции SonicWall по предоставлению клиентам автоматических возможностей обнаружения и предотвращения нарушений в реальном времени при внедрении облачных технологий.

Узнайте больше о SonicWall Cloud App Security по адресу: www.sonicwall.com/casb.

Продукты безопасности для удаленного доступа

SonicWall SMA - это унифицированный шлюз безопасного доступа для организаций, сталкивающихся с проблемами в области мобильности, BYOD и облачной миграции. Решение позволяет организации предоставлять доступ в любое время, в любом месте и с любого устройства к критически важным корпоративным ресурсам. Детальный механизм политики контроля доступа SMA, авторизация устройств с учетом контекста, VPN на уровне приложений и расширенная аутентификация с единой регистрацией позволяют организациям использовать BYOD и мобильность в гибридной IT-среде.

Кроме того, SMA уменьшает площадь поверхности для угроз, предоставляя такие функции, как определение геолокации IP-адресов и ботнетов, интеграция MCЭ веб-приложений WAF и «песочницы» Capture ATP.

Мобильность и BYOD

Для организаций, желающих использовать BYOD, гибкий рабочий режим или оффшорное программирование, SMA становится центральным элементом применения политик. SMA обеспечивает лучшую в своем классе защиту для минимизации внешних угроз, а также делает организации более безопасными, поддерживая новейшие криптографические алгоритмы и шифры. SMA SonicWall позволяет администраторам предоставлять безопасный мобильный доступ и привилегии на основе ролей, поэтому конечные пользователи получают быстрый и простой доступ к бизнес-приложениям, данным и ресурсам, которые им требуются. В то же время организации могут устанавливать безопасные политики BYOD для защиты своих корпоративных сетей и данных от мошеннического доступа и вредоносного ПО.

Движение к облаку

Для организаций, начинающих миграцию к облачной среде, SMA предлагает инфраструктуру единого входа (SSO), которая использует единый веб-портал для аутентификации пользователей в гибридной IT-среде. Независимо от того, находится ли корпоративный ресурс локально, в интернете или в развернутом облаке, доступ к данным становится единообразным и беспрепятственным. Пользователям не нужно запоминать все отдельные URL-адреса приложений и вести подробный каталог закладок. С Workplace, порталом централизованного доступа, вы даете пользователям один URL для доступа ко всем критически важным приложениям из стандартного веб-браузера. SMA предоставляет интегрированный единый вход для приложений SaaS, размещенных в облаке, которые используют SAML 2.0, и приложений, размещенных в кампусе, которые используют RADIUS или Kerberos. SMA интегрируется с несколькими серверами аутентификации, авторизации и учета и ведущими технологиями многофакторной аутентификации (MFA) для дополнительной безопасности. Безопасный SSO предоставляется только авторизованным конечным устройствам после проверки состояния и уровня соответствия требованиям.

Провайдеры управляемых услуг

Для организаций с центрами обработки данных или для поставщиков управляемых услуг SMA предоставляет готовое решение для обеспечения высокой степени непрерывности бизнеса и масштабируемости. SMA SonicWall может поддерживать до 20 000 одновременных подключений на одном устройстве с возможностью масштабирования до сотен тысяч пользователей с помощью интеллектуальной кластеризации. Снизьте затраты центров обработки данных с помощью кластеров высокой доступности типа «активный/активный» (Global High Availability) и встроенных динамических балансировщиков нагрузки (Global Traffic Optimizer), которые перераспределяют глобальный трафик в наиболее оптимизированный ЦОД в режиме реального времени в зависимости от потребностей пользователей. SMA позволяет владельцам сервисов с помощью ряда инструментов предоставлять услуги без простоев и позволяет выполнять очень агрессивные SLA.

Устройства SMA

SonicWall SMA может быть развернут как защищенное высокопроизводительное устройство или как виртуальное устройство, использующее общие вычислительные ресурсы для оптимизации использования, упрощения миграции и снижения капитальных затрат. Аппаратные устройства основаны на многоядерной архитектуре, которая обеспечивает высокую производительность с ускорением SSL, большой пропускной способностью VPN и мощными прокси для обеспечения надежного безопасного доступа. Для регулируемых и федеральных организаций SMA доступен с сертификацией FIPS 140-2 Level 2. Виртуальные устройства SMA предлагают такие же надежные возможности безопасного доступа на основных виртуальных платформах, таких как Hyper-V и VMware. Независимо от того, выбираете ли вы развертывание физических устройств, виртуальных устройств или их комбинации, SMA легко впишется в вашу существующую IT-инфраструктуру.

Управление и отчеты

SonicWall предоставляет интуитивно понятную веб-платформу управления для оптимизации управления устройствами и предоставления широких возможностей отчетности. Простой в использовании графический интерфейс вносит ясность в управление несколькими машинами. Унифицированное управление политиками помогает создавать и контролировать политики и конфигурации доступа. Единая политика управляет вашими пользователями, устройствами, приложениями, данными и сетями. Автоматизируйте рутинные задачи и планируйте действия, освобождая группы безопасности от повторяющихся задач, чтобы сосредоточиться на стратегических задачах безопасности, таких как реагирование на инциденты.

Расширьте возможности своего IT-отдела, чтобы обеспечить лучшую эффективность работы и максимально безопасный доступ в зависимости от сценария пользователя. Выберите из целого ряда вариантов от полностью бесклиентского безопасного веб-доступа для поставщиков и сторонних подрядчиков до более традиционных клиентов с полнофункциональными VPN-туннелями для руководителей. Если вам необходимо обеспечить надежный безопасный доступ для 5 пользователей из одного центра обработки данных или масштабировать его до тысяч пользователей из глобально распределенных ЦОД, SonicWall SMA предоставит вам решение.

Узнайте больше о продуктах безопасности SonicWall для удаленного доступа по адресу: www.sonicwall.com/en-us/products/remote-access.

Продукты защиты электронной почты

Электронная почта имеет решающее значение для вашего делового общения, но она также является вектором атаки №1 для таких угроз, как вымогательское ПО, фишинг, компрометация деловой электронной почты (BEC), спуфинг, спам и вирусы. Более того, в соответствии с государственными нормативными актами ваша компания несет ответственность за защиту конфиденциальных данных и защиту от их утечки, также вы должны быть уверены в безопасности обмена электронной почтой, содержащей важные данные клиентов или конфиденциальную информацию. Независимо от того, является ли ваша организация растущим малым или средним бизнесом, крупным распределенным предприятием или поставщиком управляемых услуг (MSP), вам необходим экономически эффективный способ развертывания защиты и шифрования электронной почты, а также масштабируемость, позволяющая легко наращивать емкость и делегировать управление по организационным подразделениям и доменам.

Кроме того, для управления затратами и ресурсами организации внедряют Microsoft Office 365 и Google G. Хотя Office 365 и G Suite предлагают встроенные функции безопасности, для борьбы со сложными угрозами электронной почте организациям требуется решение для обеспечения безопасности электронной почты нового поколения, которое легко интегрируется с Office 365 и G Suite, чтобы защитить их от современных сложных угроз.

Устройства для защиты электронной почты SonicWall Email Security

Система SonicWall Email Security проста в настройке и администрировании и рассчитана на экономичное масштабирование от 10 до 100 000 почтовых ящиков. Ее можно развернуть как аппаратное устройство, как виртуальное устройство, использующее общие вычислительные ресурсы, или как программное обеспечение, в том числе как ПО, оптимизированное для Microsoft Windows Server или Small Business Server. Физические устройства SonicWall Email Security идеально подходят для организаций, которым необходимо выделенное локальное решение. Наше многоуровневое решение обеспечивает комплексную защиту входящего и исходящего трафика и доступно в различных вариантах аппаратных устройств, которые масштабируются до 10 000 пользователей на устройство. SonicWall Email Security также доступен как виртуальное устройство или как программное приложение, которое идеально подходит для организаций, которым требуется гибкость, которую сопровождает виртуализация. Решение можно настроить для обеспечения высокой доступности в режиме разделения, для централизованного и надежного управления крупномасштабными развертываниями.

В решении для защиты электронной почты SonicWall используются такие технологии, как машинное обучение, эвристика, анализ репутации и контента, защита URL-адресов в момент нажатия ссылки и «песочница» для вложений и URL-адресов для обеспечения комплексной защиты входящих и исходящих сообщений.

Для предотвращения атак спуфинга и мошенничества с электронной почтой решение также включает в себя мощные механизмы проверки подлинности электронной почты - Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) и аутентификацию сообщений на основе доменов, отчетность и обеспечение соответствия требованиям (DMARC).

- Остановите сложные угрозы, прежде чем они попадут в ваш почтовый ящик.
- Защититесь от мошенничества с электронной почтой и целенаправленных фишинговых атак.
- Получите современную защиту с помощью анализа угроз в реальном времени.
- Защитите свой облачный почтовый сервис (Office 365, G-Suite).
- Включите предотвращения потери данных электронной почты и контроль соответствия.
- Легкое управление и отчетность.
- Гибкие варианты развертывания.

Администрирование решения Email Security интуитивно понятно, быстро и просто. Вы можете безопасно делегировать управление спамом конечным пользователям, сохраняя при этом полный контроль над обеспечением безопасности. Вы также можете легко управлять учетными записями пользователей и групп с помощью бесшовной синхронизации нескольких LDAP. Решение также обеспечивает простую интеграцию для Office 365 и G Suite для защиты от сложных угроз электронной почте.

В больших распределенных средах поддержка коллективной аренды позволяет делегировать субадминистраторов для управления настройками в нескольких подразделениях (таких как корпоративные отделы или клиенты MSP) в рамках одного развертывания Email Security.

Сервис безопасности SonicWall Hosted Email Security

Доверьтесь быстрому развертыванию и простоте администрирования размещенных сервисов, чтобы защитить свою организацию от угроз, передаваемых по электронной почте, таких как вымогательское ПО, угрозы «нулевого дня», фишинг и BEC, при соблюдении требований и нормативных актов, предъявляемых к электронной почте. Получите тот же уровень расширенной защиты электронной почты с нашим размещенным решением, которое предлагает функциональный паритет с физическими и виртуальными устройствами. Это решение также обеспечивает непрерывность работы электронной почты, чтобы гарантировать, что электронные письма всегда доставляются, а производительность не снижается во время плановых и внеплановых отключений локальных серверов электронной почты или облачного провайдера, такого как Office 365 и G suite.

SonicWall Hosted Email Security предлагает превосходную облачную защиту от входящих и исходящих угроз по доступной, предсказуемой и гибкой месячной или годовой цене подписки. Вы можете минимизировать время и затраты на предварительное развертывание, а также текущие расходы на администрирование без ущерба для безопасности.

SonicWall предлагает VAR и MSP больше возможностей для конкуренции и увеличения доходов при минимизации рисков, накладных расходов и текущих затрат. SonicWall Hosted Email Security включает в себя MSP-дружественные функции, такие как надежная многопользовательская поддержка, централизованное управление несколькими подписчиками, интеграция с Office 365, гибкие варианты покупки и автоматическое выделение ресурсов.

Узнайте больше о продуктах безопасности электронной почты SonicWall Email Security по адресу: www.sonicwall.com/en-us/products/secure-email.

Управление, отчеты и аналитика

SonicWall считает, что комплексный подход к управлению безопасностью является не только фундаментом для хорошей превентивной практики безопасности, но и формирует основу для единой стратегии управления безопасностью, соответствием требованиям и управления рисками. С решениями SonicWall для управления, отчетности и аналитики организации получают интегрированную, защищенную и расширяемую платформу для создания надежной, унифицированной стратегии защиты и реагирования на инциденты безопасности в своих проводных и беспроводных сетях, на конечных точках и в мобильных устройствах, а также в мультиоблачных средах. Полное внедрение этой общей платформы дает организациям глубокое понимание безопасности для принятия обоснованных решений в этой области и быстрого перехода к совместной работе, обмену информацией и знаниями в рамках общей инфраструктуры безопасности.

Глобальная система управления SonicWall Global Management System

Развертываемая на месте как программное обеспечение или виртуальное устройство, SonicWall Global Management System (GMS) связно управляет операциями сетевой безопасности с помощью бизнес-процессов и уровней обслуживания, в отличие от менее эффективного подхода «от устройства к устройству». GMS позволяет организациям различных размеров и типов легко консолидировать управление устройствами безопасности, уменьшить сложности администрирования и устранения неполадок и объединить все эксплуатационные аспекты инфраструктуры безопасности. Это включает в себя централизованное управление и применение политик, мониторинг событий в режиме реального времени, детальный анализ данных и отчетность, журналы аудита, механизм быстрого развертывания Zero-Touch, провижининг SD-WAN и многое другое в рамках единой корпоративной платформы.

GMS также отвечает требованиям организации по управлению изменениями конфигурации МСЭ благодаря автоматизации рабочих процессов. Этот встроенный автоматизированный процесс обеспечивает корректность изменений и их соответствие политикам, обеспечивая четкий процесс конфигурирования, сравнения, проверки, просмотра и утверждения политик управления безопасностью перед их развертыванием. Группы утверждения являются гибкими, что позволяет придерживаться политик безопасности компании и обеспечивает развертывание корректных политик межсетевого экрана в нужное время и в соответствии с регулирующими правилами.

Центр безопасности SonicWall Capture Security Center

Являясь частью облачной платформы SonicWall Capture, Capture Security Center представляет собой открытую, масштабируемую платформу для управления безопасностью, мониторинга, отчетности и аналитики, которая поставляется в виде экономически эффективного «программного обеспечения как услуги» (SaaS). Он предназначен для различных размеров организаций и вариантов использования, включая распределенные предприятия и сервис-провайдеров, которые внедряют облачные вычисления для повышения своей экономической эффективности. Capture Security Center является идеальной платформой управления облачной безопасностью для создания устойчивой, полностью скоординированной работы систем защиты в любых сетях.

Для клиентов Capture Security Center предлагает максимальную прозрачность, гибкость и емкость для управления всей экосистемой безопасности сети SonicWall с большой ясностью, точностью и скоростью: все из одной точки, независимо от местоположения. Благодаря общеорганизационному взгляду на среду безопасности и данные анализа в режиме реального времени, доступные нужным сотрудникам организации, можно вырабатывать точные политики и принимать решения по управлению в целях укрепления безопасности.

Для сервис-провайдеров Capture Security Center упрощает дискретное управление операциями безопасности нескольких клиентов. Это создает возможности для MSP/MSSP повысить гибкость их сервисов безопасности при одновременном снижении эксплуатационных расходов и сложности поддержки единичной инфраструктуры.

Система SonicWall Analytics

Выходя за рамки управления безопасностью и отчетности, SonicWall Analytics обеспечивает полный взгляд на все, что происходит в среде сетевой безопасности. Ее мощный интеллектуальный аналитический механизм автоматизирует агрегацию, нормализацию и контекстуализацию данных безопасности, проходящих через все управляемые МСЭ SonicWall. Прилагаемая панель управления обеспечивает полный обзор, полномочия и гибкость на одной панели для проведения глубокого расследования и криминалистического анализа.

SonicWall Analytics представляет данные безопасности в осмысленном, действенном и легко используемом виде для заинтересованных сторон для интерпретации, определения приоритетов, принятия решений и надлежащих защитных мер. Эти глубокие знания и понимание среды безопасности обеспечивают полную прозрачность и способность не только обнаруживать, но и организовывать меры по устранению угроз безопасности, а также мониторить и отслеживать результаты с большей ясностью, уверенностью и скоростью. Кроме того, встраивание SonicWall Analytics в бизнес-процесс помогает внедрить аналитику за счет автоматизации оповещений в реальном времени, организации политики безопасности и средств контроля в упреждающем и автоматическом режиме и мониторинга результатов для обеспечения большего уровня безопасности.

SonicWall Analytics оптимизирована как для облачного, так и для локального развертывания. Она лицензируется как экономически эффективное «программное обеспечение как услуга» (SaaS) через Capture Security Center, как виртуальное устройство в средах частного облака VMWare или Microsoft Hyper-V или в публичных облачных средах AWS или Microsoft Azure. Помимо предоставления организациям эксплуатационных и экономических преимуществ виртуализации и облачных вычислений, она также обеспечивает динамическое масштабирование хранилища данных для удовлетворения растущих требований к сохранению данных практически от неограниченного числа узлов МСЭ.

Узнайте больше о продуктах управления и отчетности SonicWall по адресу: www.sonicwall.com/en-us/products/firewalls/management-and-reporting.

Корпоративные услуги SonicWall Enterprise Services

Достигайте большего со своим решением SonicWall для сетевой безопасности и получите необходимую поддержку, когда она вам понадобится. Благодаря корпоративной поддержке SonicWall и профессиональным услугам вы получите долгосрочную выгоду от своего решения.

Услуги глобальной поддержки Global Support Services

Получите удобную поддержку, чтобы ваш бизнес шел гладко:

Техническая поддержка

- **8x5** – С понедельника по пятницу, с 8 утра до 5 вечера для некритических сред.
- **7x24** – Круглосуточная поддержка, включая выходные и праздничные дни, для критически важных для бизнеса сред.

Дополнительная поддержка

- **Премиальная поддержка (Premier Support)** предоставляет корпоративным средам выделенного технического аккаунт-менеджера (TAM). Ваш TAM действует от вашего имени как надежный консультант, который работает с вашим персоналом, чтобы помочь свести к минимуму незапланированные простои, оптимизировать IT-процессы, предоставить оперативные отчеты для повышения эффективности и является вашей единственной точкой ответственности за бесперебойную поддержку.
- **Выделенный инженер поддержки (DSE)** предоставляет выделенный инженерный ресурс для поддержки корпоративного аккаунта. Ваш DSE будет знать и понимать вашу среду, политики и задачи в области IT, чтобы быстро решать технические вопросы, когда вам нужна поддержка.

Глобальные профессиональные услуги Global Professional Services

Нужна помощь в определении наилучшего решения безопасности для вашего бизнеса, а также в настройке вашей существующей инфраструктуры? Давайте позаботимся об этом. С Global Professional Services вы получаете единую точку контакта для всех ваших потребностей в развертывании и интеграции. Вы получите услуги, адаптированные к вашей уникальной среде, и помощь в:

- **Планировании:** определении и понимание ваших требований к межсетевому экрану.
- **Внедрении/Развертывании:** оценке и развертывании вашего решения.
- **Передаче знаний:** использовании, управлении и обслуживании вашего устройства.
- **Миграции:** сведении к минимуму простоя и обеспечении непрерывности бизнеса.

Корпоративные услуги SonicWall доступны для продуктов серий NS*sp*/NS*a*/TZ/SRA/SMA/Email Security/GMS.

Узнайте больше: https://support.software.com/essentials/support-offerings.

Заключение

Откройте для себя продукты безопасности SonicWall

Интегрируйте свое оборудование, программное обеспечение и услуги для обеспечения лучшей в своем классе безопасности. Узнайте больше на www.sonicwall.com. Узнайте о возможностях покупки и обновления на сайте www.sonicwall.com/how-to-buy. И попробуйте сами решения SonicWall на сайте www.sonicwall.com/trials.

О компании SonicWall

Компания SonicWall более 27 лет борется с индустрией киберпреступности, защищая малый и средний бизнес, предприятия и правительственные учреждения по всему миру. Опираясь на результаты исследований, проводимых SonicWall Capture Labs, наши отмеченные наградами решения для обнаружения и предотвращения взломов в режиме реального времени защищают более миллиона сетей, а также их электронную почту, приложения и данные в более чем 215 странах и территориях. Таким образом эти организации могут работать более эффективно и меньше опасаться за свою безопасность. Для получения дополнительной информации посетите www.sonicwall.com или следуйте за нашими публикациями в Twitter, LinkedIn, Facebook и Instagram.

Если у вас есть какие-либо вопросы относительно потенциального использования этого материала вами, свяжитесь с нами по адресу:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Посетите наш веб-сайт
для получения дополнительной информации.
www.sonicwall.com