КРАТКОЕ ОПИСАНИЕ ПРОДУКТОВ SONICWALL

МСЭ Нового поколения

Высокопроизводительные МСЭ: серия NS*sp* 12000
NS*sp* 12800/12400

Масштабируемая, передовая система безопасности для крупных распределенных предприятий, ЦОД и сервис-провайдеров, использующая возможности облачного интеллекта

МСЭ среднего размера: серия NS*a*
NS*a* 9650/9450/9250/ 6650/5650/4650/3650/2650

Проверенная в отрасли эффективность безопасности и производительность для средних сетей, филиалов и распределенных предприятий

Начальный уровень: серия TZ
TZ600/TZ500/TZ400/ TZ350/ TZ300/ SOHO 250/SOHO

Интегрированная платформа предотвращения угроз и SD-WAN для малых и средних организаций и распределенных предприятий

Виртуальные МСЭ: серия NSv

Виртуальные МСЭ с гибкими моделями лицензирования для защиты критически важных компонентов вашей публичной и частной облачной инфраструктуры

Защита беспроводных сетей

Серия SonicWave
SonicWave 432e/432i/432o/ 231c/224w/231o

Безопасность и производительность для нового поколения беспроводных устройств, управляемых через облако или МСЭ

Защищенный удаленный доступ

Серия SMA: SMA 8200v/7200/ 6200/500v/410/210

Простой, защищенный доступ к сетевым и облачным ресурсам с контролем политик безопасности

Устройства защиты электронной почты

ESA 9000/7000/5000/
VM Software/Cloud Service

Многоуровневое решение для защиты электронной почты от сложных угроз

Управление и аналитика

Capture Security Center
Global Management System (GMS)
Analytics

Контроль и знание вашей сети – это сила

Средства ускорения WAN

WXA 6000 (SW)
WXA 5000 (VM)/500 (SW)

Значительное повышение скорости передачи данных приложений и повышение производительности труда сотрудников

Capture Client

Унифицированная клиентская платформа, которая обеспечивает защиту множественных конечных точек, включая расширенную защиту от вредоносных программ, изолированную программную среду, контроль устройств и механизм восстановления в случае заражения

МСЭ веб-приложений (WAF)

Безопасность веб-приложений, предотвращение утечек данных и соответствие нормативным требованиям, как на собственной площадке, так и в облачной среде

Защита облачных приложений

Решение CASB, обеспечивающее безопасность нового поколения для приложений SaaS, таких как Office 365 и G Suite, для защиты электронной почты, данных и учетных записей пользователей от расширенных угроз при обеспечении соответствия требованиям в облаке

Подписка на сервисы для МСЭ нового поколения

Включены в Advanced Gateway Security Suite (AGSS); Комбинируются с Next-Gen Firewall в TotalSecure Advanced Edition

- Многопоточная облачная «песочница» Capture Advanced Threat Protection (ATP)
- Антивирусный шлюз и защита от шпионского ПО
- Сервис предотвращения вторжений
- Контроль приложений
- Сервис фильтрации контента/веб
- Поддержка 24x7

Безопасность как сервис (SECaaS)

Аутсорсинг вашей сетевой безопасности с нашим решением под ключ

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.

Узнайте больше: www.sonicwall.com/en-us/products

Квалификационные вопросы

Межсетевой экран нового поколения

- Как вы измеряете эффективность ваших мер безопасности?
- Каков ваш план исправления выявленных пробелов в безопасности?
- Как снизить риск уязвимых веб-приложений, к которым могут получить доступ ваши пользователи?
- Какой тип подключения к интернету у вас есть? На какой скорости?
- Нужно ли жертвовать производительностью, чтобы повысить безопасность своей сети?
- Что вы делаете для защиты от новых угроз, таких как атаки «нулевого дня»?
- Насколько ваша команда способна исправлять уязвимости в течение 12 часов после выпуска исправления?
- Может ли ваша «песочница» обнаруживать и блокировать угрозы, скрытые в глубокой памяти?
- Сколько механизмов обработки в вашей песочнице?
- Может ли ваша «песочница» задерживать файлы в шлюзе перед их выпуском?
- Знаете ли вы, что большинство веб-сеансов зашифрованы, и может ли ваш МСЭ их расшифровать и проверить?
- Знаете ли вы, проверяет ли межсетевой экран вашей организации трафик HTTPS или нет?
- Были ли у вас сбои в работе сети или простои из-за проверки трафика HTTPS?
- Является ли ваш виртуальный межсетевой экран таким же надежным, как и физический?
- Как вы защищаете свои публичные или частные облачные среды?
- Можете ли вы реализовать правильное зонирование безопасности и микросегментацию в вашей виртуальной сети?
- Есть ли у вас полная видимость и контроль вашего виртуального трафика?
- Поддерживает ли ваш текущий МСЭ PoE/PoE + или вам нужен коммутатор для питания устройств с поддержкой PoE?
- Заинтересованы ли вы в сокращении затрат путем замены MPLS на SD-WAN для безопасной частной сети?
- Нужно ли вам лицензирование на основе подписки для виртуальных МСЭ?

Capture Client

- Нуждаются ли ваши конечные точки в последовательной расширенной защите от вымогательского ПО и зашифрованных угроз?
- Насколько легко вы можете обеспечить соблюдение политики и управление лицензиями на всех конечных точках?
- Стремитесь ли вы отслеживать состояние конечных точек и управления своей безопасностью?
- Ваш продукт безопасности конечных точек соединен со средой «песочницы»?
- Текущее решение контролирует состояние вашей системы постоянно?
- Можете ли вы восстановить ущерб, нанесенный вымогателями, до ранее известного чистого состояния?
- Есть ли у вас возможность заблокировать неизвестные и потенциально зараженные устройства от соединения с конечными точками?

МСЭ веб-приложений

- Как вы в настоящее время защищаете свои критически важные для бизнеса веб-ресурсы и веб-серверы?
- Какие меры безопасности вы принимаете, чтобы соответствовать требованиям PCI?

Защита облачных приложений

- Используете ли вы O365 или G Suite?
- Используете ли вы Proofpoint или Mimecast для защиты O365/G Suite?
- Сканируете ли вы внутреннюю электронную почту O365?
- Сколько санкционированных приложений SaaS использует ваша организация?
- Боретесь ли вы за соответствие требованиям данных, хранящихся в приложениях SaaS?
- Как вы узнаете, что учетные данные ваших пользователей скомпрометированы?
- У вас есть представление о том, кто получает доступ к данным, откуда и когда? (BYOD)

Защита беспроводных сетей

- Жалуются ли ваши сотрудники/партнеры/ клиенты на низкую производительность Wi-Fi?
- Каким будет максимальное количество пользователей беспроводной связи в единый момент времени?
- Есть ли у вас опасения по поводу стоимости добавления безопасного беспроводного решения в вашу сеть?
- Насколько вы знакомы с беспроводным стандартом 802.11ac Wave 2?
- Нужна ли вам гибкость для управления точками доступа - управление через облако или МСЭ?
- Вы эффективно спланировали свою сеть WiFi?
- Нужно ли вам, чтобы точки доступа были отвязаны от МСЭ?
- Вы беспокоитесь о предоставлении расширенных функций безопасности в вашей сети Wi-Fi?

Защищенный удаленный доступ

- В настоящее время ваша организация перемещает или планирует перенести бизнес-приложения и ресурсы в облако?
- Предоставляете ли вы пользователям унифицированный «единый вход» для локальных и облачных приложений?
- Используют ли ваши сотрудники Dropbox или личную электронную почту для обмена файлами?
- Как ваши сотрудники управляют многочисленными URL и паролями?
- Какова ваша текущая стратегия мобильности/BYOD?
- Есть ли у вас возможность просматривать каждое устройство, которое подключается к вашей сети?

Защита электронной почты

- Обеспокоены ли вы сложными угрозами для электронной почты, такими как вымогательское ПО, направленный фишинг и компрометация деловой переписки?
- Предоставляет ли ваше текущее решение для защиты электронной почты функции Advanced Threat Protection?
- Обеспокоены ли вы тем, что электронные письма, содержащие конфиденциальную информацию, могут утечь в сеть?
- Как вы соблюдаете такие нормативы, как GDPR, Sarbanes-Oxley, GLBA или HIPAA?
- Заинтересованы ли вы в том, чтобы предлагать управляемые услуги безопасности электронной почты (MSSP) своим клиентам?

Управление и аналитика

- Какие проблемы вы могли бы решить, объединив свои средства безопасности под одной общей платформой управления с единой панелью?
- С какими экономическими и эксплуатационными проблемами вы сталкиваетесь при управлении своей инфраструктурой безопасности?
- Насколько вы уверены в своей способности продемонстрировать соответствие требованиям кибербезопасности, таким как PCI, HIPPA и GDPR?
- Как бы изменилось ваше состояние безопасности, если бы вы могли быстрее и точнее обнаруживать угрозы и риски и реагировать на них?
- Какое значение вы и ваша команда руководителей придаете полной видимости киберугроз и рисков для вашего бизнеса?

Ускорение WAN

- Имеет ли ваша организация удаленные офисы? Как много?
- Офисы подключены к сети через соединение VPN или выделенный канал WAN (MPLS)?
- Используют ли ваши сотрудники такие приложения, как общий доступ к файлам Microsoft Windows, SharePoint, Office или FTP?
- Хотели бы вы снизить потребление полосы пропускания и стоимость, не платя за увеличение емкости каналов?

Узнайте больше: www.sonicwall.com/en-us/products

Datasheet-SonicWallProductLineAtAGlance-RUS-VG-216

SONICWALL®