Gartner peerinsights customers' choice 2018

SONICWALL

Семейство устройств сетевой безопасности SonicWall Network Security appliance (NSa)

Проверенная на практике эффективность безопасности и производительность для сетей среднего размера, распределенных предприятий и центров обработки данных

Серия устройств SonicWall Network Security appliance (NS*a*) предоставляет организациям, масштаб которых может варьироваться от сетей среднего размера до распределенных предприятий и центров обработки данных, высокопроизводительную платформу безопасности с расширенным механизмом предотвращения угроз. Используя инновационные технологии глубокого обучения в облачной платформе SonicWall Capture, серия NS*a* обеспечивает организациям так необходимое им автоматизированное обнаружение и предотвращение взломов в реальном времени.

Передовое предотвращение угроз в сочетании с превосходной производительностью

Сегодняшние сетевые угрозы применяют сложные методы уклонения и их все труднее идентифицировать с использованием традиционных методов обнаружения. Чтобы избежать сложных атак, требуется более современный подход, который в значительной степени использует возможности облачной аналитики безопасности. Без этого облачного интеллекта решения по обеспечению безопасности шлюзов не могут идти в ногу с современными сложными угрозами. Межсетевые экраны нового поколения (NGFW) серии NS*a* объединяют в себе две передовые технологии безопасности для обеспечения предотвращения угроз, что ставит вашу сеть на шаг впереди. Использующий несколько механизмов обнаружения сервис защиты от сложных угроз SonicWall Capture Advanced Threat Protection (ATP) дополняет наша запатентованная технология глубокой проверки памяти в реальном времени (RTDMI™). Механизм RTDMI активно обнаруживает и блокирует массовые угрозы, угрозы «нулевого дня» и неизвестные вредоносные программы путем осуществления проверки непосредственно в памяти. Благодаря архитектуре реального времени технология SonicWall RTDMI является точной, сводит к минимуму ложные срабатывания, а также выявляет и противодействует сложным атакам, когда действие вредоносного ПО осуществляется менее 100 наносекунд. В совокупности запатентованный* SonicWall механизм однопроходной глубокой проверки пакетов без сборки (RFDPI) проверяет каждый байт каждого пакета, инспектируя как входящий, так и исходящий трафик на межсетевом экране. Благодаря использованию облачной платформы SonicWall Capture в дополнение к встроенным возможностям, включающих защиту от вторжений, защиту от вредоносных программ и фильтрацию веб/URL-адресов, устройства серии NS*a* блокируют даже самые сложные угрозы на шлюзе.

Кроме того, МСЭ SonicWall обеспечивают полную защиту, выполняя полную расшифровку и проверку зашифрованных соединений TLS/SSL и SSH независимо от порта или протокола. МСЭ ищет аномалии протоколов, угрозы, атаки «нулевого дня», вторжения и даже события, соответствующие определенным критериям, просматривая каждый пакет. Механизм глубокой проверки пакетов обнаруживает и предотвращает скрытые атаки, использующие криптографию. Он также блокирует зашифрованные загрузки вредоносного ПО, предотвращает распространение инфекций и препятствует обмену данными с центрами управления вредоносного ПО и утечке данных. Правила включения и исключения позволяют полностью контролировать, какой трафик подвергается дешифровке и проверке на основе конкретных организационных требований и/или требований законодательства.

Преимущества:

Превосходные производительность и предотвращение угроз

- Запатентованая технология глубокой проверки памяти в реальном времени
- Запатентованная технология глубокой проверки пакетов без сборки
- Встроенная и облачная защита от угроз
- Расшифровка и проверка TLS/SSL
- Эффективность безопасности, проверенная в отрасли
- Многоядерная архитектура аппаратной платформы
- Специальная группа по исследованию угроз Capture Labs

Контроль сети и гибкость использования

- Защищенный SD-WAN
- Мощная ОС SonicOS
- Аналитика и контоль приложений
- Сегментация сети с VLAN
- Защита высокоскоростных беспроводных сетей

Простые развертывание, настройка и управление

- Развертывание Zero-Touch Deployment
- Облачное и локальное централизованное управление
- Масштабируемая линейка межсетевых экранов
- Низкая совокупная стоимость владения

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

Когда организации активируют на своих МСЭ функции глубокой проверки пакетов, такие как IPS, антивирус, защиту от шпионского ПО, расшифровку/проверку TLS/SSL и другие, производительность сети часто и иногда резко снижается. Поэтому межсетевые экраны серии NS*a* оснащены многоядерной аппаратной архитектурой, в которой используются специализированные микропроцессоры безопасности. В сочетании с нашими модулями RTDMI и RFDPI этот уникальный дизайн исключает возможность снижения сетевой производительности, с которой сталкиваются другие МСЭ.

Контроль сети и гибкость

Ядром серии NS*a* является SonicOS, многофункциональная операционная система SonicWall. SonicOS предоставляет организациям неоходимые им контроль сети и гибкость использования, благодаря аналитике и контролю приложений, визуализации в режиме реального времени, системе предотвращения вторжений (IPS), оснащенной сложной технологией противодействия уклонениям, высокоскоростной виртуальной частной сети (VPN) и другими надежными функциями безопасности.

Используя аналитику и контроль приложений, сетевые администраторы могут идентифицировать и отделить производительные приложения от непродуктивных или потенциально опасных, а также контролировать этот трафик с помощью мощных политик уровня приложений как для каждого пользователя, так и для группы (наряду с расписаниями и списками исключений). Важнейшим бизнес-приложениям можно назначать приоритеты и выделять большую полосу пропускания, тогда как полоса пропускания второстепенных приложений может быть ограничена. Мониторинг и визуализация в реальном времени обеспечивает графическое представление приложений, пользователей и использования полосы пропускания для детального анализа трафика в сети.

Для распределенных организаций, которым требуется повышенная гибкость при проектировании своей сети, технология SD-WAN в SonicOS является идеальным дополнением к межсетевым экранам NS*a*, развернутым в штаб-квартире или в удаленных офисах и филиалах. Вместо того чтобы полагаться на более дорогие устаревшие технологии, такие как MPLS и T1, организации, использующие SD-WAN, могут выбирать более дешевые общедоступные интернет-услуги, продолжая при этом достигать высокого уровня доступности приложений и предсказуемой производительности.

В каждый МСЭ серии NS*a* встроен контроллер беспроводного доступа, который позволяет организациям безопасно расширять периметр сети с помощью беспроводной технологии. Межсетевые экраны SonicWall и беспроводные точки доступа SonicWave 802.11ac Wave 2 совместно создают решение для обеспечения безопасности беспроводной сети, которое сочетает в себе передовую технологию МСЭ нового поколения с высокоскоростной беспроводной связью для обеспечения сетевой безопасности корпоративного класса и производительности беспроводной сети.

Простые развертывание, настройка и управление

Как и все МСЭ SonicWall, серия NS*a* тесно интегрирует ключевые технологии безопасности, подключения и гибкости в единое комплексное решение. Это включает точки беспроводного доступа SonicWave и серию SonicWall WAN Acceleration (WXA), которые автоматически обнаруживаются и настраиваются управляющим МСЭ NS*a*. Консолидация нескольких возможностей избавляет от необходимости покупать и устанавливать точечные продукты, которые не всегда хорошо работают вместе. Это уменьшает усилия, необходимые для развертывания решения в сети и его настройки, экономя время и деньги.

Облачное централизованное управление, отчетность, лицензирование и аналитика осуществляются через SonicWall Capture Security Center. Ключевым компонентом Capture Security Center является система развертывания Zero-Touch Deployment. Эта облачная функция упрощает и ускоряет развертывание и подготовку МСЭ SonicWall в удаленных офисах и филиалах. Вместе упрощенное развертывание и настройка, а также простота управления позволяют организациям снизить совокупную стоимость владения и обеспечить высокую отдачу от инвестиций.

Безопасная и высокоскоростная беспроводная сеть

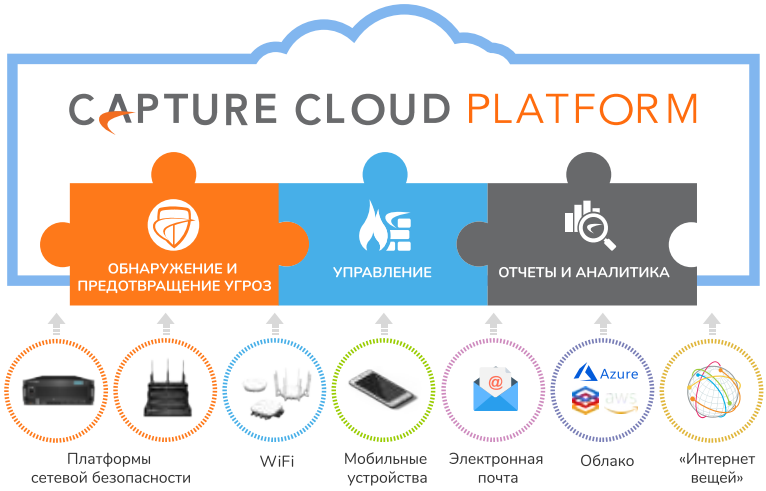
Объедините МСЭ нового поколения серии NS*a* с беспроводной точкой доступа SonicWall SonicWave 802.11ac Wave 2, чтобы создать решение для обеспечения безопасности высокоскоростной беспроводной сети. Устройства серии NS*a* и точки доступа SonicWave имеют порты 2.5 GbE, которые обеспечивают с помощью беспроводной технологии Wave 2 многогигабитную пропускную способность. МСЭ сканирует весь беспроводной трафик, входящий и выходящий из сети, с использованием технологии глубокой проверки пакетов, а затем удаляет угрозы, такие как вредоносные программы и попытки вторжения, даже те, которые используют зашифрованные соединения. Дополнительные функции безопасности и контроля, такие как фильтрация контента, контроль приложений и аналитика, а также Capture Advanced Threat Protection, могут быть использованы в беспроводной сети для обеспечения дополнительных уровней защиты.

Платформа Capture Cloud Platform

SonicWall's Capture Cloud Platform обеспечивает облачное предотвращение угроз и управление сетью, а также отчеты и аналитику для организаций любого размера. Платформа объединяет информацию об угрозах, собранную из нескольких источников, включая наш сервис «песочницы», использующий несколько механизмов работы Capture Advanced Threat Protection, а также более 1 миллиона датчиков SonicWall, расположенных по всему миру.

Если обнаруживается, что данные, поступающие в сеть, содержат ранее неизвестный вредоносный код, специальная группа SonicWall, занимающаяся исследованиями угроз Capture Labs, разрабатывает сигнатуры, которые хранятся в базе данных Capture Cloud Platform и развертываются на межсетевых экранах клиентов для своевременной защиты. Новые обновления вступают в силу немедленно, без перезагрузок и прерываний. Сигнатуры, хранящиеся на устройстве, защищают от широкого спектра атак, охватывающих десятки тысяч отдельных угроз. В дополнение к контрмерам на устройстве, МСЭ NS*a* также имеют постоянный доступ к базе данных Capture Cloud Platform, которая расширяет встроенный интеллектуальный сигнатурный анализ десятками миллионов сигнатур.

В дополнение к предотвращению угроз, облачная платформа Capture предлагает единую панель управления, а администраторы могут легко создавать отчеты о сетевой активности как в режиме реального времени, так и за прошедшие отрезки времени.

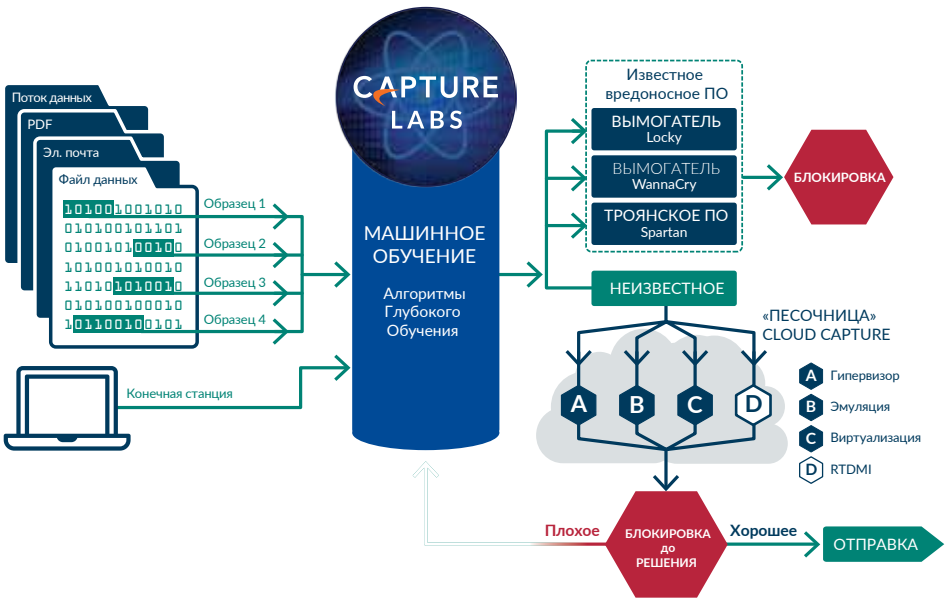


Advanced threat protection

В центре автоматизированной защиты SonicWall в режиме реального времени находится сервис SonicWall Capture Advanced Threat Protection, облачная многопоточная «песочница», которая расширяет механизмы защиты МСЭ для обнаружения и предотвращения угроз «нулевого дня». Подозрительные файлы отправляются в облако, где они анализируются с использованием алгоритмов глубокого обучения с возможностью удерживать их в шлюзе до вынесения решения. Многопоточная платформа «песочницы», включающая в себя глубокую проверку проверку памяти в реальном времени, виртуализированную изолированную программную среду, полную эмуляцию системы и технологию анализа на уровне гипервизора, выполняет подозрительный код и анализирует его поведение. Когда файл определяется как вредоносный, он блокируется, и в Capture ATP немедленно создается его хэш. Вскоре после этого сигнатура отправляется в МСЭ для предотвращения последующих атак.

Сервис анализирует широкий спектр операционных систем и типов файлов, включая исполняемые программы, DLL, PDF, документы MS Office, архивы, JAR и APK.

Для полной защиты конечных точек клиент SonicWall Capture сочетает в себе антивирусную технологию следующего поколения с многопоточной изолированной программной средой SonicWall.



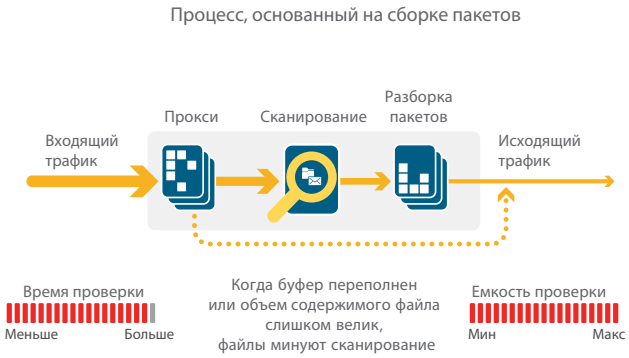
SONICWALL®

Механизм глубокой проверки пакетов без сборки

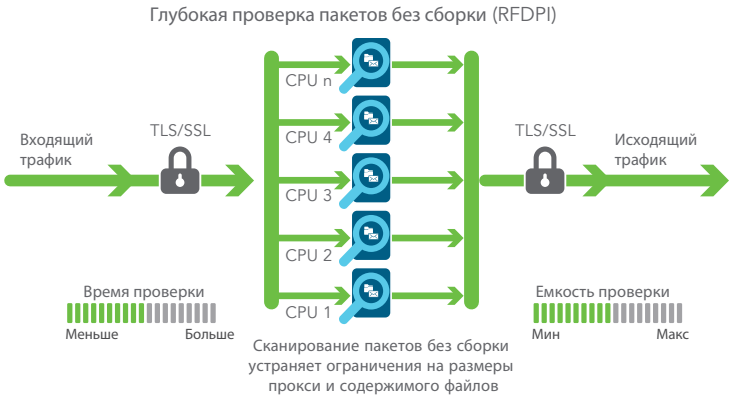
Глубокая проверка пакетов SonicWall без сборки (Reassembly-Free Deep Packet Inspection, RFDPI) – это однопроходная система проверки с малой задержкой, которая выполняет потоковый двунаправленный анализ трафика на высокой скорости без прокси или буферизации для эффективного обнаружения попыток вторжения и загрузки вредоносных программ при одновременной идентификации трафика приложения независимо от порта и протокола. Этот запатентованный механизм основан на проверке полезной нагрузки потокового трафика для обнаружения угроз на уровнях 3-7 и принимает сетевые потоки посредством обширной и многократной нормализации и дешифрования, чтобы нейтрализовать передовые методы уклонения, которые пытаются запутать механизмы обнаружения и внедрить вредоносный код в сеть.

После того, как пакет подвергся необходимой предварительной обработке, включая расшифровку TLS/SSL, он анализируется относительно единого запатентованного представления памяти трех баз данных сигнатур: атак вторжения, вредоносных программ и приложений. Затем состояние соединения продвигается на следующий этап, чтобы представить позицию потока относительно этих баз данных, пока не встретится состояние атаки или другое событие «совпадения», в этот момент выполняется заранее заданное действие.

В большинстве случаев соединение прерывается и производятся надлежащие действия регистрации в журнале и посылка уведомления. Однако механизм также может быть сконфигурирован только для проверки трафика или, в случае задачи обнаружения приложений, в целях управления полосой пропускания на уровне 7 для остальной части потока данного приложения, как только оно было идентифицировано.



Конкурентная прокси-архитектура



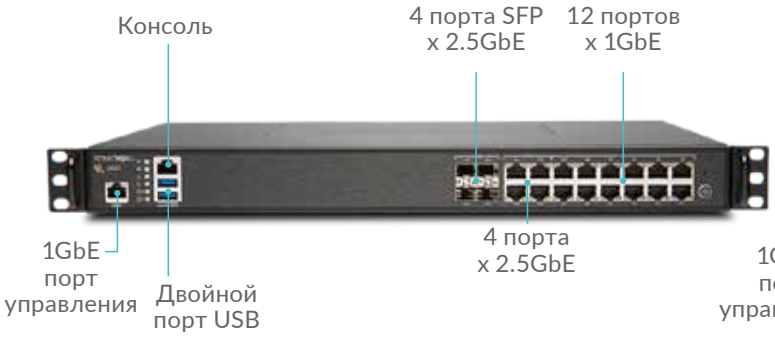
Потоковая архитектура SonicWall

Централизованное управление и отчеты

Для организаций со строгим регламентом, желающих достичь полностью скоординированной стратегии управления безопасностью, соответствием и рисками, SonicWall предоставляет администраторам унифицированную, безопасную и расширяемую платформу для управления МСЭ SonicWall, точками беспроводного доступа и коммутаторами Dell серий N и X с помощью коррелированных и аудируемых рабочих процессов. Предприятия могут легко консолидировать управление устройствами безопасности, уменьшить сложность администрирования и устранения неполадок, а также управлять всеми эксплуатационными аспектами инфраструктуры безопасности, включая централизованное управление политиками и их применением, мониторинг событий в режиме реального времени, пользовательские действия, идентификацию приложений, аналитику потоков и криминалистику, создание отчетов о соответствии, аудит и многое другое. Кроме того, предприятия отвечают требованиям управления изменениями межсетевых экранов благодаря автоматизации рабочих процессов, которая обеспечивает гибкость и уверенность в развертывании правильных политик МСЭ в нужное время и согласно требованиям соответствия. Доступные в вариантах для развертывания как на площадке предприятия (SonicWall Global Management System), так и в облаке (Capture Security Center) решения для управления и отчетности SonicWall обеспечивают согласованный способ управления сетевой безопасностью посредством бизнес-процессов и уровней обслуживания, что значительно упрощает управление жизненным циклом вашей общей среды безопасности по сравнению с управлением каждого устройства в отдельности.

NS*a* 2650

Устройство NS*a* 2650 обеспечивает высокоскоростное предотвращение угроз для тысяч зашифрованных и еще большего числа незашифрованных соединений для организаций среднего размера и распределенных предприятий.



Межсетевой экран	NS*a* 2650
Пропускная способность МСЭ	3.0 Гбит/с
Пропускная способность IPS	1.4 Гбит/с
Пропускная способность Anti-malware	1.3 Гбит/с
Пропускная способность Threat Prevention	1.5 Гбит/с
Макс. число соединений	1,000,000
Число новых соединений/с	14,000/с
Модуль хранения данных	16 ГБ
Описание	**SKU**
NS*a* 2650 только МСЭ	01-SSC-1936
NS*a* 2650 с подпиской TotalSecure Advanced (1 год)	01-SSC-1988

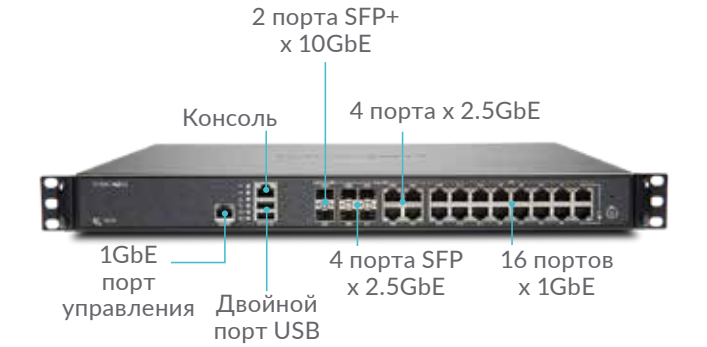
NS*a* 3650

Устройство SonicWall NS*a* 3650 идеально подходит для филиалов, малых и средних корпоративных сред, заинтересованных в пропускной способности и производительности.

Межсетевой экран	NS*a* 3650
Пропускная способность МСЭ	3.75 Гбит/с
Пропускная способность IPS	1.8 Гбит/с
Пропускная способность Anti-malware	1.5 Гбит/с
Пропускная способность Threat Prevention	1.75 Гбит/с
Макс. число соединений	2,000,000
Число новых соединений/с	14,000/с
Модуль хранения данных	32 ГБ
Описание	**SKU**
NS*a* 3650 только МСЭ	01-SSC-1937
NS*a* 3650 с подпиской TotalSecure Advanced (1 год)	01-SSC-4081

NS*a* 4650

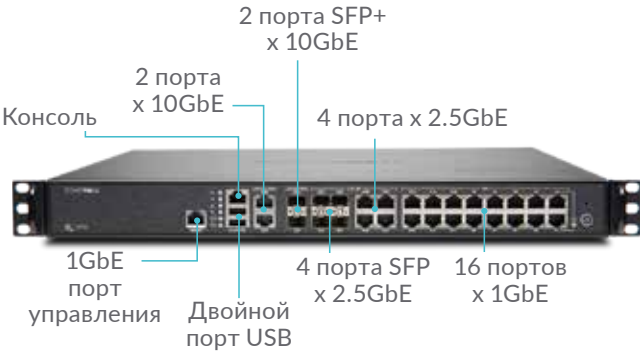
SonicWall NS*a* 4650 обеспечивает растущие организации и филиалы среднего размера функциями безопасности корпоративного класса и бескомпромиссной производительностью.



Межсетевой экран	NS*a* 4650
Пропускная способность МСЭ	6.0 Гбит/с
Пропускная способность IPS	2.3 Гбит/с
Пропускная способность Anti-malware	2.45 Гбит/с
Пропускная способность Threat Prevention	2.5 Гбит/с
Макс. число соединений	3,000,000
Число новых соединений/с	40,000/с
Модуль хранения данных	32 ГБ
Описание	**SKU**
NS*a* 4650 только МСЭ	01-SSC-1938
NS*a* 4650 с подпиской TotalSecure Advanced (1 год)	01-SSC-4094

NS*a* 5650

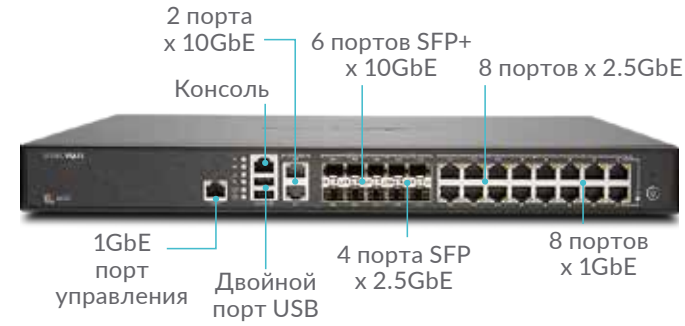
SonicWall NS*a* 5650 идеально подходит для распределенных, филиальных офисов и корпоративных сред, требующих значительной пропускной способности и высокой плотности портов.



Межсетевой экран	NS*a* 5650
Пропускная способность МСЭ	6.25 Гбит/с
Пропускная способность IPS	3.4 Гбит/с
Пропускная способность Anti-malware	2.8 Гбит/с
Пропускная способность Threat Prevention	3.4 Гбит/с
Макс. число соединений	4,000,000
Число новых соединений/с	40,000/с
Модуль хранения данных	64 ГБ
Описание	**SKU**
NS*a* 5650 только МСЭ	01-SSC-1939
NS*a* 5650 с подпиской TotalSecure Advanced (1 год)	01-SSC-4342

NS*a* 6650

SonicWall NS*a* идеально подходит для крупных распределенных и корпоративных центральных площадок, требующих высокой пропускной способности и производительности.



Межсетевой экран	NS*a* 6650
Пропускная способность МСЭ	12.0 Гбит/с
Пропускная способность IPS	6.0 Гбит/с
Пропускная способность Anti-malware	5.4 Гбит/с
Пропускная способность Threat Prevention	5.5 Гбит/с
Макс. число соединений	5,000,000
Число новых соединений/с	90,000/с
Модуль хранения данных	64 ГБ
Описание	**SKU**
NS*a* 6650 только МСЭ	01-SSC-1940
NS*a* 6650 с подпиской TotalSecure Advanced (1 год)	01-SSC-2209

NS*a* 9250/9450/9650

Устройства SonicWall NS*a* 9250/9450/9650 предоставляют распределенным предприятиям и центрам обработки данных масштабируемую и глубокую защиту с мульти-гигабитной скоростью.

Межсетевой экран	NS*a* 9250	NS*a* 9450	NS*a* 9650
Пропускная способность МСЭ	12.0 Гбит/с	17.1 Гбит/с	17.1 Гбит/с
Пропускная способность IPS	7.2 Гбит/с	10.2 Гбит/с	10.3 Гбит/с
Пропускная способность Anti-malware	6.5 Гбит/с	8.0 Гбит/с	8.5 Гбит/с
Пропускная способность Threat Prevention	6.5 Гбит/с	9.0 Гбит/с	9.4 Гбит/с
Макс. число соединений	7,500,000	10,000,000	12,500,000
Число новых соединений/с	90,000/с	130,000/с	130,000/с
Модули хранения данных	1 ТБ, 128 ГБ	1 ТБ, 128 ГБ	1 ТВ, 256 ГБ
Описание	**SKU**	**SKU**	**SKU**
NS*a* только МСЭ	01-SSC-1941	01-SSC-1942	01-SSC-1943
NS*a* с подпиской TotalSecure Advanced (1 год)	01-SSC-2854	01-SSC-4358	01-SSC-3475

Функционал

МЕХАНИЗМ RFDPI	
Функция	Описание
Глубокая проверка пакетов без сборки (RFDPI)	Этот высокопроизводительный запатентованный механизм проверки выполняет потоковый двунаправленный анализ трафика без прокси и буферизации, для выявления попыток вторжения и вредоносных программ, а также для идентификации трафика приложений независимо от порта.
Двунаправленная проверка	Сканирование на наличие угроз одновременно как во входящем, так и в исходящем трафике, для того чтобы убедиться, что сеть не используется для распространения вредоносного ПО и не становится платформой для запуска атак в случае наличия зараженной машины внутри сети.
Потоковая проверка	Технология проверки без прокси и без буферизации обеспечивает производительность со сверхнизкой задержкой для глубокой проверки пакетов (DPI) миллионов одновременных сетевых потоков без ограничения размера файлов и потоков и может применяться к обычным протоколам, а также к необработанным потокам TCP.
Высокая параллельность обработки и масштабируемость	Уникальный дизайн механизма RFDPI работает с многоядерной архитектурой, чтобы обеспечить высокую пропускную способность глубокой проверки пакетов и поддержку чрезвычайно высоких скоростей установления новых соединений, чтобы справиться с пиками трафика в нагруженных сетях.
Однопроходная проверка	Однопроходная архитектура глубокой проверки пакетов одновременно обеспечивает сканирование на наличие вредоносных программ, вторжений и идентификацию приложений, значительно сокращая задержку DPI и обеспечивая корреляцию всей информации об угрозах в одной архитектуре.

МЕЖСЕТЕВОЙ ЭКРАН И СЕТЕВЫЕ ФУНКЦИИ	
Функция	Описание
Защищенный SD-WAN	Защищенный SD-WAN является альтернативой более дорогим технологиям, таким как MPLS и позволяет распределенным корпоративным организациям создавать, эксплуатировать и управлять безопасными высокопроизводительными сетями на удаленных узлах с целью совместного использования данных, приложений и услуг с использованием легкодоступных низкозатратных публичных интернет-сервисов.
Интерфейс REST API	Позволяет МСЭ получать и использовать любые проприетарные, оригинальные устройства производителя и сторонние интеллектуальные каналы для борьбы с такими продвинутыми угрозами, как угрозы «нулевого дня», инсайдеры, взломанные учетные данные, вымогательское ПО и сложные постоянные угрозы.
Проверка пакетов с учетом состояния соединения	Весь сетевой трафик проверяется, анализируется и приводится в соответствие с политиками доступа межсетевого экрана.
Высокая доступность/кластеризация	Устройства серии NS*a* поддерживают высокую доступность в режимах Активный/Пассивный (A/P) с синхронизацией состояния, Активный/Активный (A/A) DPI и Активный/Активный с кластеризацией. В режиме Активный/Активный DPI нагрузка глубокой проверки пакетов переносится на ядра пассивного устройства, чтобы повысить пропускную способность.
Защита от атак класса DDoS/DoS	Защита от атак SYN flood обеспечивает защиту от DoS-атак с использованием технологии прокси-сервера SYN уровня 3 и технологий внесения в черный список SYN уровня 2. Кроме того, этот механизм защищает от DoS/DDoS посредством защиты от атак насыщения UDP/ICMP и ограничения скорости соединений.
Поддержка IPv6	Интернет-протокол версии 6 (IPv6) сейчас находится на ранней стадии для замены IPv4. С SonicOS аппаратная платформа будет поддерживать реализацию фильтрации и «прозрачного» режима МСЭ.
Гибкие варианты развертывания	Устройство NS*a* может быть развернуто в режимах традиционного NAT, моста 2-го уровня, «прозрачного» режима («виртуального провода») и сетевого отвода.
Балансировка нагрузки WAN	Балансировка нагрузки нескольких интерфейсов WAN с использованием методов Round Robin, Spillover или Percentage.
Расширенное качество обслуживания (QoS)	Гарантирует качество обслуживания для критических сервисов с помощью 802.1p, маркировку DSCP и перемаппирование трафика VoIP в сети.
Поддержка гейткипера H.323 и SIP-прокси	Блокирует спам-вызовы, требуя, чтобы все входящие вызовы были авторизованы и аутентифицированы гейткипером H.323 или прокси-сервером SIP.
Управление одиночными и каскадируемыми коммутаторами Dell серий N и X	Управляйте настройками безопасности дополнительных портов сетевых коммутаторов Dell серий N и X, включая функции Portshield, HA, PoE и PoE+ с помощью панели управления МСЭ.
Биометрическая аутентификация	Поддерживает аутентификацию мобильного устройства, такую как распознавание отпечатков пальцев, которую нельзя легко дублировать или использовать совместно, для безопасной аутентификации личности пользователя при доступе в сеть.
Открытая аутентификация и вход через социальные сети	Предоставляет гостевым пользователям возможность использовать свои учетные данные из социальных сетей, таких как Facebook, Twitter или Google+, для входа в систему и получения доступа к Интернет и другим гостевым службам через беспроводную зону, локальную сеть или зону DMZ, используя сквозную аутентификацию.

УПРАВЛЕНИЕ И ОТЧЕТЫ	
Функция	Описание
Локальное и облачное управление	Конфигурация и управление устройствами SonicWall доступны через облако посредством SonicWall Capture Security Center и локально, используя SonicWall Global Management System (GMS).
Мощная система управления одним устройством	Интуитивно понятный веб-интерфейс обеспечивает быструю и удобную настройку, дополняя богатый интерфейс командной строки и поддержку SNMPv2/3.
Отчет по трафику приложений с использованием IPFIX/NetFlow	Экспортирует аналитику трафика приложений и данные об использовании по протоколам IPFIX или NetFlow для мониторинга и отчетности в режимах реального времени и исторического обзора с помощью инструментов, поддерживающих IPFIX и NetFlow с расширениями.

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)	
Функция	Описание
Автоматичесое создание VPN	Упрощает и сокращает время сложного развертывания распределенного МСЭ за счет автоматизации первоначальной инициализации VPN-шлюза между площадками с межсетевыми экранами SonicWall, так что подключение и его защита происходят мгновенно и автоматически.
IPSec VPN для связи между площадками	Высокопроизводительный IPSec VPN позволяет устройствам серии NS*a* выступать в качестве концентратора VPN для тысяч других больших площадок, филиалов или домашних офисов.
Удаленный доступ с использованием клиентов SSL VPN или IPSec	Использует бесклиентную технологию SSL VPN или простой в управлении клиент IPSec для быстрого доступа к электронной почте, файлам, компьютерам, сайтам интранета и приложениям с различных платформ.
Избыточный шлюз VPN	При использовании нескольких каналов WAN первичный и вторичный VPN могут быть настроены так, чтобы обеспечить плавное автоматическое переключение всех сеансов VPN при сбоях и восстановлениях.
VPN с маршрутизацией	Возможность динамической маршрутизации по VPN-каналам обеспечивает непрерывную работу в случае временного сбоя VPN-туннеля за счет плавного перенаправления трафика между конечными точками через альтернативные маршруты.

УЧЕТ ОСОБЕННОСТЕЙ КОНТЕНТА И КОНТЕКСТА	
Функция	Описание
Отслеживание действий пользователей	Идентификация и отслеживание активности пользователей становятся доступны благодаря бесшовной интеграции средств единого входа AD/LDAP/Citrix/терминальных сервисов в сочетании с обширной информацией, полученной от системы DPI.
Идентификация страны трафика по GeoIP	Определяет и контролирует сетевой трафик, направляемый в определенные страны или приходящий из них, для защиты от атак известных или предполагаемых источников угроз или для расследования подозрительного трафика, исходящего из сети. Предоставляет возможность создавать пользовательские списки стран и ботнетов для переопределения неверной страны или тега ботнета, связанного с IP-адресом. Устраняет нежелательную фильтрацию IP-адресов из-за неправильной классификации.
Фильтрация DPI на основе регулярных выражений	Предотвращает утечку данных, выявляя и контролируя контент, передающийся по сети, путем сопоставления с регулярными выражениями. Предоставляет возможность создавать пользовательские списки стран и ботнетов для переопределения неверной страны или тега ботнета, связанного с IP-адресом.

Сервисы по предотвращению взлома (по подписке)

ЗАЩИТА ОТ СЛОЖНЫХ УГРОЗ Capture Advance Threat Protection	
Функция	Описание
Использование нескольких механизмов «песочницы»	Платформа «песочницы» с несколькими механизмами обработки, которая включает в себя виртуализированную изолированную программную среду, эмуляцию всей системы и технологию анализа на уровне гипервизора, выполняет подозрительный код и анализирует его поведение, обеспечивая полную картину вредоносных действий.
Глубокая проверка памяти в реальном времени (RTDMI)	Эта запатентованная облачная технология обнаруживает и блокирует вредоносное ПО, которое не демонстрирует какого-либо вредоносного поведения и скрывает свои инструменты воздействия с помощью шифрования. Заставляя вредоносные программы открыть свои инструменты в памяти, механизм RTDMI активно обнаруживает и блокирует массовые угрозы, угрозы «нулевого дня» и неизвестные вредоносные программы.
Блокировка до решения	Чтобы предотвратить попадание в сеть потенциально вредоносных файлов, файлы, отправляемые в облако для анализа, можно хранить на шлюзе до вынесения решения по ним.
Анализ широкого диапазона типов и размеров файлов	Поддерживает анализ широкого спектра типов файлов, по отдельности или в группе, включая исполняемые программы (PE), DLL, PDF, документы MS Office, архивы, JAR и APK, а также несколько операционных систем, включая Windows, Android, Mac OS X и мультибраузерные среды.
Быстрое развертывание сигнатур	Когда файл определяется как вредоносный, его сигнатура немедленно развертывается на МСЭ с подпиской SonicWall Capture ATP и передается в базы данных сигнатур Антивирусного шлюза и IPS, а также в базы данных репутаций URL, IP и доменов в течение 48 часов.
Capture Client	Capture Client - это унифицированная клиентская платформа, которая предоставляет несколько возможностей защиты конечных точек, включая расширенную защиту от вредоносных программ и поддержку проверки зашифрованного трафика. Он использует многоуровневые технологии защиты, комплексную отчетность и обеспечение защиты конечных точек.
ПРЕДОТВРАЩЕНИЕ ЗАШИФРОВАННЫХ УГРОЗ	
Функция	Описание
Расшифровка и проверка TLS/SSL	Расшифровывает и проверяет зашифрованный трафик TLS/SSL на лету, без использования прокси, на наличие вредоносных программ, попыток вторжения и утечек данных, а также применяет политики управления приложениями, URL-адресами и контентом для защиты от угроз, скрытых в зашифрованном трафике. Включено в подписку безопасности для всех моделей серии NSa.
Проверка SSH	Глубокая проверка пакетов SSH (DPI-SSH) расшифровывает и проверяет данные, проходящие через туннель SSH, для предотвращения атак, использующих SSH.
ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ	
Функция	Описание
Защита на основе противодействия	Тесно интегрированная система предотвращения вторжений (IPS) использует сигнатуры и другие контрмеры для сканирования полезной нагрузки пакетов на наличие уязвимостей и эксплойтов, охватывая широкий спектр атак и уязвимостей.
Автоматическое обновление сигнатур	Команда SonicWall Threat Research постоянно исследует и внедряет обновления для обширного списка контрмер IPS, который охватывает более 50 категорий атак. Новые обновления вступают в силу немедленно без перезагрузки или прерывания обслуживания.
Внутризонная защита IPS	Усиливает внутреннюю безопасность, сегментируя сеть на несколько зон безопасности с предотвращением вторжений, предотвращая распространение угроз через границы зон.
Обнаружение и блокировка центров управления ботнетами (CnC)	Определяет и блокирует командный и управляющий трафик, исходящий от ботов в локальной сети, по IP-адресам и доменам, которые определены как распространяющие вредоносные программы или являются известными точками управления ботнетами (CnC).
Искажение/аномалия протоколов	Определяет и блокирует атаки, которые используют нарушения протоколов в попытке проникнуть через IPS.
Защита от угроз «нулевого дня»	Защищает сеть от атак «нулевого дня» с помощью постоянных обновлений против новейших методов и приемов атак эксплуатации, содержащих тысячи отдельных эксплойтов.
Технология противодействия уклонению	Обширная нормализация потока, декодирование и другие методы гарантируют, что угрозы не попадут в сеть незамеченными, используя методы уклонения на уровнях 2-7.
ПРЕДОТВРАЩЕНИЕ УГРОЗ	
Функция	Описание
Противодействие вредоносному ПО на шлюзе	Механизм RFDPI сканирует весь входящий, исходящий и внутризонный трафик на наличие вирусов, троянов, перехватчиков клавиатурного ввода и других вредоносных программ в файлах неограниченной длины и размера по всем портам и потокам TCP.
Защита от вредоносного ПО Capture Cloud	Постоянно обновляемая база данных с десятками миллионов сигнатур угроз находится на облачных серверах SonicWall и используется для расширения возможностей встроенной базы данных сигнатур, обеспечивая RFDPI широкий охват угроз.
Постоянное обновление безопасности	Новые обновления угроз автоматически отправляются на МСЭ, работающие в полевых условиях с активными сервисами безопасности и вступают в силу немедленно без перезагрузок или прерываний.
Двунаправленная проверка необработанного TCP	Механизм RFDPI способен сканировать необработанные потоки TCP на любом порту в двух направлениях, предотвращая атаки, которые они могут преодолеть устаревшие системы безопасности, которые сосредоточены на защите только нескольких известных портов.
Расширенная поддержка протоколов	Определяет общие протоколы, такие как HTTP/S, FTP, SMTP, SMBv1/v2 и другие, которые не отправляют данные в необработанном TCP, и декодирует их полезную нагрузку для проверки на наличие вредоносных программ, даже если они не работают на стандартных, хорошо известных портах.

АНАЛИЗ И КОНТРОЛЬ ПРИЛОЖЕНИЙ

Функция	Описание
Контроль приложений	Контролирует приложения или отдельные функции приложений, которые идентифицируются механизмом RFDPI по постоянно расширяющейся базе данных, содержащей более тысячи сигнатур приложений, для повышения безопасности и увеличения производительности сети.
Идентификация пользовательских приложений	Контролирует пользовательские приложения, создавая сигнатуры на основе определенных параметров или паттернов, уникальных для сетевого обмена данными данного приложения, для получения дополнительного контроля над сетью.
Управление полосой пропускания приложений	Детально распределяет и регулирует доступную полосу пропускания для критически важных приложений или категорий приложений, одновременно блокируя трафик несущественных приложений.
Детальное управление	Управляет приложениями или конкретными компонентами приложений на основе расписаний, групп пользователей, списков исключений и ряда действий с полной идентификацией пользователя системы единого входа посредством интеграции с LDAP/AD/терминальными сервисами/Citrix.

КОНТЕНТНАЯ ФИЛЬТРАЦИЯ

Функция	Описание
Внутренняя/внешняя фильтрация контента	С помощью сервиса фильтрации контента и клиента фильтрации контента применяет политики допустимого использования и блокирует доступ к веб-сайтам HTTP/HTTPS, содержащим информацию или изображения, которые являются нежелательными или непродуктивными.
Клиент контентной фильтрации с механизмом применения политик	Расширяет применение политик безопасности для блокировки интернет-контента для устройств Windows, Mac OS, Android и Chrome, расположенных за пределами периметра МСЭ.
Детальные настройки управления	Блокирует контент, используя предопределенные категории или любую комбинацию категорий. Фильтрация может быть запланирована по времени суток, например, в школьные или рабочие часы, и применяться к отдельным пользователям или группам.
Веб-кэширование	Рейтинги URL кэшируются локально на МСЭ SonicWall, поэтому время отклика для последующего доступа к часто посещаемым сайтам составляет лишь долю секунды.

ЗАЩИТА ОТ ВИРУСОВ И ШПИОНСКОГО ПО

Функция	Описание
Многоуровневая защита	Использует возможности МСЭ в качестве первого уровня защиты по периметру в сочетании с защитой конечных точек для блокирования проникновения вирусов в сеть через ноутбуки, флэш-накопители и другие незащищенные системы.
Возможность автоматического применения политик безопасности	Контролирует, что на каждом компьютере, подключающемся к сети, установлено и активно соответствующее антивирусное программное обеспечение и/или сертификат DPI-SSL, что исключает издержки, обычно связанные с управлением антивирусами на рабочем столе.
Возможность автоматизированного развертывания и инсталляции	Автоматическое развертывание и установка антивирусных и антишпионских клиентов в сети происходит автоматически, что сводит к минимуму административные издержки.
Антивирус нового поколения	Клиент Capture использует модуль статического искусственного интеллекта (AI) для определения угроз до того, как они могут быть реализованы, и возврата к предыдущему незараженному состоянию.
Защита от шпионского ПО	Мощная защита от шпионского ПО сканирует и блокирует установку широкого спектра программ-шпионов на настольных компьютерах и ноутбуках, прежде чем они передадут конфиденциальные данные, обеспечивая более высокую безопасность и производительность рабочих станций.

Сводка функционала SonicOS

Межсетевой экран

- Проверка пакетов с учетом состояния соединения
- Глубокая проверка пакетов без их сборки
- Защита от атак DDoS (UDP/ICMP/SYN flood)
- Поддержка IPv4/IPv6
- Биометрическая аутентификация для удаленного доступа
- DNS-прокси
- REST API

Расшифровка и проверка TLS/SSL/SSH[1]

- Глубокая проверка пакетов для TLS/SSL/SSH
- Включение/исключение объектов, групп и имен хостов
- Контроль TLS/SSL
- Детальный контроль DPI SSL по зонам или правилам

Защита от сложных угроз Capture advanced threat protection[1]

- Глубокая проверка памяти в реальном времени
- Облачный анализ с применением нескольких механизмов
- Виртуализованная «песочница»
- Анализ на уровне гипервизора
- Полная системная эмуляция
- Проверка широкого спектра типов файлов
- Автоматизированная и ручная отсылка
- Обновления аналитики по угрозам в реальном времени
- Блокировка до вынесения решения
- Capture Client

Предотвращение вторжений[1]

- Сканирование по сигнатурам
- Автоматические обновления сигнатур
- Двунаправленная проверка
- Возможность тонкой настройки правил IPS
- Фильтрация по GeoIP
- Фильтрация ботнетов с динамическими списками
- Сопоставление по регулярным выражениям

Защита от вредоносного ПО[1]

- Потоковое сканирование для обнаружения вредоносного ПО
- Антивирус на шлюзе
- Защита от шпионского ПО на шлюзе
- Двунаправленная проверка
- Отсутствие ограничений на размер файла
- Облачная база данных вредоносного ПО

Распознавание приложений[1]

- Контроль приложений
- Управление полосой пропускания приложений
- Создание сигнатур для пользовательских приложений
- Предотвращение утечки данных
- Отчет о приложениях с использованием NetFlow/IPFIX
- Исчерпывающая база данных сигнатур приложений

Визуализация трафика и аналитика

- Активность пользователей
- Использование приложений/полосы пропускания/угроз
- Облачная аналитика

Фильтрация веб-контента HTTP/HTTPS[1]

- Фильтрация URL
- Технология обхода прокси
- Блокировка по ключевым словам
- Фильтрация по политикам (исключения/включения)
- Вставки в заголовок HTTP
- Управление полосой пропускания по рейтингу категорий CFS
- Унифицированная модель политики с контролем приложений
- Клиент контентной фильтрации

VPN

- Автоматический провижининг VPN
- IPSec VPN для соединений между площадками
- Удаленный доступ с использованием SSL VPN и клиента IPSec
- Избыточный шлюз VPN
- Мобильный доступ из iOS, Mac OS X, Windows, Chrome, Android и Kindle Fire
- VPN с использованием маршрутизации (OSPF, RIP, BGP)

Сетевые функции

- Защищенная SD-WAN
- PortShield
- Jumbo-фреймы
- Расширенное журналирование
- Транки с VLAN
- RSTP (Rapid Spanning Tree Protocol)
- Зеркалирование портов
- Качество обслуживания (QoS) на уровне 2
- Безопасность портов
- Динамическая маршрутизация (RIP/OSPF/BGP)
- Беспроводный контроллер SonicWall
- Маршрутизация по политикам (ToS/metric и ECMP)
- NAT
- Защита DNS
- Сервер DHCP
- Управление полосой пропускания
- Агрегирование каналов (статическое и динамическое)
- Резервирование портов
- Высокая доступность A/P с синхронизацией состояния
- Кластеризация A/A
- Балансировка входящей/исходящей нагрузки
- Режим моста L2, режим «провод»/«виртуальный провод», режим отвода от линии
- Аварийное переключение WAN на 3G/4G
- Асиммертичная маршрутизация
- Поддержка Common Access Card (CAC)

Беспроводная сеть

- WIDS/WIPS
- Анализ радиочастотного спектра
- Предотвращение несанкционированных точек доступа
- Быстрый роуминг (802.11k/r/v)
- Автоматический выбор канала
- Floor plan view/Topology view
- Технология Band steering
- Формирование луча WiFi
- Функция AirTime fairness
- Ретранслятор MiFi
- Гостевая циклическая квота
- Гостевой портал LHM

VoIP

- Детальная настройка качества обслуживания (QoS)
- Управление полосой пропускания
- Изменения SIP и H.323 в соответствии с правилами доступа
- Поддержка гейткипера H.323 и SIP-прокси

Управление и мониторинг

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2/v3
- Журналирование
- Экспорт Netflow/IPFix
- Облачное резервное копирование конфигураций
- BlueCoat Security Analytics Platform
- Управление точками доступа SonicWall
- Управление коммутаторами Dell серий N и X, включая каскадирование

Локальное хранилище данных

- Журналы
- Отчеты
- Резервные копии прошивок

[1]Необходима дополнительная подписка

SONICWALL®

Системные спецификации устройств серии NS*a*

Общие параметры МСЭ	NS*a* 2650	NS*a* 3650	NS*a* 4650	NS*a* 5650
Операционная система	SonicOS 6.5.4			
Интерфейсы	4 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE порт управления, 1 консольный порт	2 x 10-GbE SFP+, 8 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE порт управления, 1 консольный порт	2 x 10-GbE SFP+, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE порт управления, 1 консольный порт	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE порт управления, 1 консольный порт
Расширение	1 слот расширения (задний)*			
Встроенное хранилище данных (SSD)	16 ГБ	32 ГБ	32 ГБ	64 ГБ
Управление	CLI, SSH, Web UI, Capture Security Center, GMS, REST API			
Число пользователей системы единого входа (SSO)	40,000	50,000	60,000	70,000
Число точек доступа (максимальное)	48	96	128	192
Журналирование	Analyzer, локальный журнал, Syslog			
Производительность МСЭ/VPN	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Пропускная способность МСЭ[1]	3.0 Гбит/с	3.75 Гбит/с	6.0 Гбит/с	6.25 Гбит/с
Пропускная способность в режиме Threat Prevention[2]	1.5 Гбит/с	1.75 Гбит/с	2.5 Гбит/с	3.4 Гбит/с
Пропускная способность в режиме Application inspection[2]	1.85 Гбит/с	2.1 Гбит/с	3.0 Гбит/с	4.25 Гбит/с
Пропускная способность в режиме IPS[2]	1.4 Гбит/с	1.8 Гбит/с	2.3 Гбит/с	3.4 Гбит/с
Пропускная способность в режиме проверки на вредоносное ПО[2]	1.3 Гбит/с	1.5 Гбит/с	2.45 Гбит/с	2.8 Гбит/с
Пропускная способность в режиме проверки и расшифровки (DPI SSL)[2]	300 Мбит/с	320 Мбит/с	675 Мбит/с	800 Мбит/с
Пропускная способность VPN[3]	1.45 Гбит/с	1.5 Гбит/с	3.0 Гбит/с	3.5 Гбит/с
Число новых соединений в секунду	14,000/с	14,000/с	40,000/с	40,000/с
Макс. число соединений (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
Макс. число соединений (DPI)	500,000	750,000	1,000,000	1,500,000
Число соединений DPI SSL (макс./по умолчанию)	100,000/60,000	100,000/40,000	175,000/145,000	175,000/125,000
VPN	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Число туннелей VPN «площадка-площадка»	1,000	3,000	4,000	6,000
Число клиентов IPSec VPN (макс.)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
Число клиентов SSL VPN NetExtender (макс.)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Шифрование/аутентификация	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Обмен ключами	Diffie Hellman Groups 1, 2, 5, 14v			
VPN с маршрутизацией	RIP, OSPF, BGP			
Сеть	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Присвоение IP-адресов	Статическое, (клиент DHCP, PPPoE, L2TP и PPTP), Внутренний сервер DHCP, ретрансляция DHCP			
Режимы NAT	1:1, 1:много, много:1, много:много, гибкий NAT (с перекрытием IP-адресов), PAT, прозрачный режим			
Число интерфейсов VLAN	256	256	400	500
Протоколы маршрутизации	BGP, OSPF, RIPv1/v2, статические маршруты, маршрутизация на основе политик			
QoS	Приоритет полосы пропускания, максимальная полоса пропускания, гарантированная полоса пропускания, маркировка DSCP, 802.1p			
Аутентификация	LDAP (множественные домены), XAUTH/RADIUS, SSO, Novell, внутренняя база данных пользователей, терминальные сервисы, Citrix, Common Access Card (CAC)			
VoIP	Полная поддержка H323-v1-5, SIP			
Стандарты	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Сертификации (в процессе получения)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall и IPS), UC APL, USGv6, CsFC			
Высокая доступность[5]	Активный/Пассивный с синхронизацией состояний	Активный/Пассивный с синхронизацией состояний Активный/Активный с кластеризацией		Активный/Пассивный с синхронизацией состояний, Активный/Активный DPI с синхронизацией состояний, Активный/Активный с кластеризацией
Аппаратная платформа	**NS*a* 2650**	**NS*a* 3650**	**NS*a* 4650**	**NS*a* 5650**
Блок питания	Двойной, резервированный 120Вт (один в комплекте)		Двойной, резервированный 350Вт (один комплекте)	
Вентиляторы	Двойные, фиксированные		Двойные, съемные	
Входное питание	100-240 В AC, 50-60 Гц			
Макс. потребляемая мощность (Вт)	37.2	46	93.6	103.6
Среднее время наработки на отказ @25°C в часах	162,231	156,681	154,529	153,243
Среднее время наработки на отказ @25°C в годах	18.5	17.9	17.6	17.5
Форм-фактор	1U для монтажа в стойку			
Размеры	16.9 x 12.8 x 1.8" (43 x 32.5 x 4.5 см)		16.9 x 16.3 x 1.8" (43 x 41.5 x 4.5 см)	
Вес	11.5 фунтов (5.2 кг)	11.7 фунтов (5.3 кг)	15.2 фунтов (6.9 кг)	15.2 фунтов (6.9 кг)
Вес WEEE	12.1 фунтов (5.5 кг)	12.3 фунтов (5.6 кг)	19.6 фунтов (8.9 кг)	19.6 фунтов (8.9 кг)
Вес с упаковкой	17.0 фунтов (7.7 кг)	17.2 фунтов (7.8 кг)	24.9 фунтов (11.3 кг)	24.9 фунтов (11.3 кг)
Соответствие главным нормативам	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI			
Допустимая температура окружающей среды (Эксплуатация/Хранение)	32°-105° F (0°-40° C)/от -40° до 158° F (от -40° до 70° C)			
Влажность	10-90% без конденсации			

Системные спецификации устройств серии NS*a* (продолжение)

Общие параметры МСЭ	NS*a* 6650	NS*a* 9250	NS*a* 9450	NS*a* 9650
Операционная система	SonicOS 6.5.4			
Интерфейсы	6 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE порт управления, 1 консольный порт	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE порт управления, 1 консольный порт	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE порт управления, 1 консольный порт	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE порт управления, 1 консольный порт
Расширение	1 слот расширения (задний)*			
Встроенное хранилище данных (SSD)	64 ГБ	1ТВ, 128 ГБ	1ТВ, 128 ГБ	1ТВ, 256 ГБ
Управление	CLI, SSH, Web UI, Capture Security Center, GMS, REST API	CLI, SSH, Web UI, GMS, REST API		
Число пользователей системы единого входа (SSO)	70,000	80,000	90,000	100,000
Число точек доступа (максимальное)	192	192	192	192
Журналирование	Analyzer, локальный журнал, Syslog, IPFIX, NetFlow			
Производительность МСЭ/VPN	**NS*a* 6650**	**NS*a* 9250**	**NS*a* 9450**	**NS*a* 9650**
Пропускная способность МСЭ[1]	12.0 Гбит/с	12.0 Гбит/с	17.1 Гбит/с	17.1 Гбит/с
Пропускная способность в режиме Threat Prevention[2]	5.5 Гбит/с	6.5 Гбит/с	9.0 Гбит/с	9.4 Гбит/с
Пропускная способность в режиме Application inspection[2]	6.0 Гбит/с	7.8 Гбит/с	10.8 Гбит/с	11.5 Гбит/с
Пропускная способность в режиме IPS[2]	6.0 Гбит/с	7.2 Гбит/с	10.2 Гбит/с	10.3 Гбит/с
Пропускная способность в режиме проверки на вредоносное ПО[2]	5.4 Гбит/с	6.5 Гбит/с	8.0 Гбит/с	8.5 Гбит/с
Пропускная способность в режиме проверки и расшифровки (DPI SSL)[2]	1.45 Гбит/с	1.5 Гбит/с	2.1 Гбит/с	2.25 Гбит/с
Пропускная способность VPN[3]	6.0 Гбит/с	6.75 Гбит/с	10.0 Гбит/с	10.0 Гбит/с
Число новых соединений в секунду	90,000/с	90,000/с	130,000/с	130,000/с
Макс. число соединений (SPI)	5,000,000	7,500,000	10,000,000	12,500,000
Макс. число соединений (DPI)	2,000,000	3,000,000	4,000,000	5,000,000
Число соединений DPI SSL (макс./по умолчанию)	250,000/170,000	250,000/170,000	450,000/290,000	550,000/320,000
VPN	**NS*a* 6650**	**NS*a* 9250**	**NS*a* 9450**	**NS*a* 9650**
Число туннелей VPN «площадка-площадка»	8,000	12,000	12,000	12,000
Число клиентов IPSec VPN (макс.)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)
Число клиентов SSL VPN NetExtender (макс.)	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)
Шифрование/аутентификация	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Обмен ключами	Diffie Hellman Groups 1, 2, 5, 14v			
VPN с маршрутизацией	RIP, OSPF, BGP			
Сеть	**NS*a* 6650**	**NS*a* 9250**	**NS*a* 9450**	**NS*a* 9650**
Присвоение IP-адресов	Статическое, (клиент DHCP, PPPoE, L2TP и PPTP), Внутренний сервер DHCP, ретрансляция DHCP			
Режимы NAT	1:1, 1:много, много:1, много:много, гибкий NAT (с перекрытием IP-адресов), PAT, прозрачный режим			
Число интерфейсов VLAN	512			
Протоколы маршрутизации	BGP, OSPF, RIPv1/v2, статические маршруты, маршрутизация на основе политик			
QoS	Приоритет полосы пропускания, максимальная полоса пропускания, гарантированная полоса пропускания, маркировка DSCP, 802.1p			
Аутентификация	LDAP (множественные домены), XAUTH/RADIUS, SSO, Novell, внутренняя база данных пользователей, терминальные сервисы, Citrix, Common Access Card (CAC)			
VoIP	Полная поддержка H323-v1-5, SIP			
Стандарты	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Сертификации (в процессе получения)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall и IPS), UC APL, USGv6, CsFC			
Высокая доступность[5]	Активный/Пассивный с синхронизацией состояний, Активный/Активный DPI с синхронизацией состояний, Активный/Активный с кластеризацией			
Аппаратная платформа	**NS*a* 6650**	**NS*a* 9250**	**NS*a* 9450**	**NS*a* 9650**
Блок питания	Двойной, резервированный 350Вт (один комплекте)	Двойной, резервированный 350Вт		
Вентиляторы	Тройные, съемные			
Входное питание	100-240 VAC, 50-60 Hz			
Макс. потребляемая мощность (Вт)	144.3	86.7	90.9	113.1
Среднее время наработки на отказ @25°C в часах	157,193	139,783	134,900	116,477
Среднее время наработки на отказ @25°C в годах	17.9	15.96	15.4	13.3
Форм-фактор	1U для монтажа в стойку			
Размеры	16.9 x 16.3 x 1.8" (43 x 41.5 x 4.5 см)			
Вес	17.9 фунтов (8.1 кг)	17.9 фунтов (8.1 кг)		
Вес WEEE	22.5 фунтов (10.2 кг)	22.5 фунтов (10.2 кг)		
Вес с упаковкой	27.8 фунтов (12.6 кг)	27.8 фунтов (12.6 кг)		
Соответствие главным нормативам	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI			
Допустимая температура окружающей среды (Эксплуатация/Хранение)	32°-105° F (0°-40° C)/от -40° до 158° F (от -40° до 70° C)			
Влажность	10-90% без конденсации			

[1] Методологии тестирования: Максимальная производительность по RFC 2544 (для МСЭ). Фактическая производительность может варьироваться в зависимости от условий сети и активированных сервисов.

[2] Пропускная способность Threat Prevention (предотвращения угроз)/Gateway AV (антивирусного шлюза)/Anti-Spyware (защиты от шпионского ПО)/IPS измерялась с использованием стандартного теста производительности Spirent WebAvalanche HTTP и инструментария тестирования Ixia. Тестирование было выполнено с несколькими потоками через несколько пар портов. Пропускная способность по предотвращению угроз измеряется при включенном антивирусном шлюзе, защите от шпионского ПО, IPS и контроля приложений. Производительность DPI SSL измерялась на трафике HTTPS с включенным IPS.

[3] Пропускная способность VPN измерялась с использованием трафика UDP с пакетами размера 1280 байт в соответствии с RFC 2544. Все технические характеристики, функции и их наличие могут быть изменены.

[4] Для каждого уменьшения соединений DPI на 125,000 DPI число доступных соединений DPI SSL увеличивается на 3,000 за исключением моделей NSa 9250 и старше.

[5] Режимы «Активный/Активный с кластеризацией» и «Активный/Активный DPI с синхронизацией состояний» требуют покупки Расширенной Лицензии за исключением моделей NSa 9250 и старше.

**Для будущего использования. Все технические характеристики, функции и их наличие могут быть изменены.*

Информация по заказу устройств семейства NS*a*

NS*a* 2650	SKU
NS*a* 2650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-1988
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 2650 (1 год)	01-SSC-1783
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 2650 (1 год)	01-SSC-1935
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 2650 (1 год)	01-SSC-1976
Поддержка 24x7 для NS*a* 2650 (1 год)	01-SSC-1541
Сервис контентной фильтрации для NS*a* 2650 (1 год)	01-SSC-1970
Capture Client	Зависит от числа пользователей
Комплексный анти-спам сервис для NS*a* 2650 (1 год)	01-SSC-2001
NS*a* 3650	**SKU**
NS*a* 3650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-4081
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 3650 (1 год)	01-SSC-3451
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 3650 (1 год)	01-SSC-3457
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 3650 (1 год)	01-SSC-3632
Поддержка 24x7 для NS*a* 3650 (1 год)	01-SSC-3439
Сервис контентной фильтрации для NS*a* 3650 (1 год)	01-SSC-3469
Capture Client	Зависит от числа пользователей
Комплексный анти-спам сервис для NS*a* 3650 (1 год)	01-SSC-4030
NS*a* 4650	**SKU**
NS*a* 4650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-4094
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 4650 (1 год)	01-SSC-3493
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 4650 (1 год)	01-SSC-3499
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 4650 (1 год)	01-SSC-3589
Поддержка 24x7 для NS*a* 4650 (1 год)	01-SSC-3487
Сервис контентной фильтрации для NS*a* 4650 (1 год)	01-SSC-3583
Capture Client	Зависит от числа пользователей
Комплексный анти-спам сервис для NS*a* 4650 (1 год)	01-SSC-4062
NS*a* 5650	**SKU**
NS*a* 5650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-4342
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 5650 (1 год)	01-SSC-3674
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 5650 (1 год)	01-SSC-3680
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 5650 (1 год)	01-SSC-3698
Поддержка 24x7 для NS*a* 5650 (1 год)	01-SSC-3660
Сервис контентной фильтрации для NS*a* 5650 (1 год)	01-SSC-3692
Capture Client	Зависит от числа пользователей
Комплексный анти-спам сервис для NS*a* 5650 (1 год)	01-SSC-4068
NS*a* 6650	**SKU**
NS*a* 6650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-2209
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 6650 (1 год)	01-SSC-8761
Защита от сложных угроз Capture Advanced Threat Protection для NSa 6650 (1 год)	01-SSC-8930
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 6650 (1 год)	01-SSC-8979
Поддержка 24x7 для NS*a* 6650 (1 год)	01-SSC-8663
Сервис контентной фильтрации для NS*a* 6650 (1 год)	01-SSC-8972
Capture Client	Зависит от числа пользователей
Комплексный анти-спам сервис для NS*a* 6650 (1 год)	01-SSC-9131
NS*a* 9250	**SKU**
NS*a* 9250 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-2854
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 9250 (1 год)	01-SSC-0038
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 9250 (1 год)	01-SSC-0121
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 9250 (1 год)	01-SSC-0343
Поддержка 24x7 для NS*a* 9250 (1 год)	01-SSC-0032
Сервис контентной фильтрации для NS*a* 9250 (1 год)	01-SSC-0331
Capture Client	Зависит от числа пользователей
NS*a* 9450	**SKU**
NS*a* 9450 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-4358
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 9450 (1 год)	01-SSC-0414
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 9450 (1 год)	01-SSC-0855

Информация по заказу устройств семейства NS*a* (продолжение)

NS*a* 9450	SKU
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 9450 (1 год)	01-SSC-1196
Поддержка 24x7 для NS*a* 9450 0 (1 год)	01-SSC-0407
Сервис контентной фильтрации для NS*a* 9450 (1 год)	01-SSC-1158
Capture Client	Зависит от числа пользователей
NS*a* 9650	**SKU**
NS*a* 9650 с подпиской TotalSecure Advanced Edition (1 год)	01-SSC-3475
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, Threat Prevention, управление МСЭ и отчеты, наблюдение за «теневым IT» и поддержка 24x7 для NS*a* 9650 (1 год)	01-SSC-2036
Защита от сложных угроз Capture Advanced Threat Protection для NS*a* 9650 (1 год)	01-SSC-2042
Threat Prevention – Предотвращение вторжений, антивирус на шлюзе, защита от шпионского ПО на шлюзе, облачный антивирус для NS*a* 9650 (1 год)	01-SSC-2142
Поддержка 24x7 для NS*a* 9650 0 (1 год)	01-SSC-1989
Сервис контентной фильтрации для NS*a* 9650 (1 год)	01-SSC-2136
Capture Client	Зависит от числа пользователей
Модули и аксессуары*	**SKU**
Модуль 10GBASE-SR SFP+ Short Reach	01-SSC-9785
Модуль 10GBASE-LR SFP+ Long Reach	01-SSC-9786
Кабель Twinax 10GBASE SFP+ 1M	01-SSC-9787
Кабель Twinax 10GBASE SFP+ 3M	01-SSC-9788
Модуль 1000BASE-SX SFP Short Haul	01-SSC-9789
Модуль 1000BASE-LX SFP Long Haul	01-SSC-9790
Модуль 1000BASE-T SFP медный	01-SSC-9791

**Пожалуйста, проконсультируйтесь с вашим локальным поставщиком SonicWall о полном списке модулей SFP и SFP+*

Бандлы межсетевых экранов SonicWall NS*a*/NS*v*

Следующие МСЭ серии NS*a* могут получить годовую лицензию на соответствующую подписку TotalSecure для виртуального устройства NSv* без дополнительной платы.

МСЭ NS*a*	Соответствующий МСЭ NSv
NS*a* 5650	NSv 200
NS*a* 6650	NSv 200
NS*a* 9250	NSv 400
NS*a* 9450	NSv 400
NS*a* 9650	NSv 400

** Подписка NSv Virtual Appliance TotalSecure включает виртуальный МСЭ NSv, антивирус на шлюзе, защиту от шпионского ПО, предотвращение вторжений и сервис МСЭ для приложений, сервис контентной фильтрации и поддержку 24x7.*

Нормативные номера моделей:

NS*a* 2650 - 1RK38-0C8
NS*a* 3650 - 1RK38-0C7
NS*a* 4650 - 1RK39-0C9
NS*a* 5650 - 1RK39-0CA
NS*a* 6650 - 1RK39-0CB
NS*a* 9250 - 1RK39-0CC
NS*a* 9450 - 1RK39-0CD
NS*a* 9650 - 1RK39-0CE

Профессиональные услуги партнеров

Нужна помощь в планировании, развертывании или оптимизации вашего решения SonicWall? Партнеры по расширенным услугам SonicWall смогут предоставить вам профессиональные услуги мирового уровня. Узнайте больше на странице www.sonicwall.com/PES.

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.

Логотип Gartner Peer Insights Customer's Choice является товарным знаком и знаком сервиса Gartner, Inc. и/или ее дочерних компаний и используется в настоящем документе с разрешения. Все права защищены. Различия в выборе клиентов Gartner Peer Insights определяются субъективными мнениями отдельных конечных пользователей, основанными на их собственном опыте, количестве опубликованных обзоров Gartner Peer Insights и общих рейтингов для данного поставщика на рынке, как описано далее, и никоим образом не предназначены для представления взглядов Gartner или его филиалов.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2019 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Datasheet-NetworkSecurityAppliance-RUS-VG-MKTG5872