Gartner peerinsights customers' choice 2018

SONICWALL

Семейство устройств SonicWall TZ

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

Семейство устройств SonicWall TZ позволяет малым и средним организациям и распределенным предприятиям реализовать преимущества интегрированного решения безопасности, которое содержит весь необходимый функционал. Сочетая технологию высокоскоростного предотвращения угроз и программно-определяемых глобальных сетей (SD-WAN) с широким спектром сетевых и беспроводных функций, а также упрощенным развертыванием и централизованным управлением, серия TZ обеспечивает унифицированное решение безопасности при низкой совокупной стоимости владения.

Гибкое интегрированное решение безопасности

Основой серии TZ является SonicOS – многофункциональная операционная система SonicWall. SonicOS включает в себя мощный набор функций, которые предоставляют организациям возможность гибко настраивать эти шлюзы безопасности UTM (Unified Threat Management) в соответствии со своими конкретными сетевыми требованиями. Например, создание защищенной высокоскоростной беспроводной сети упрощается благодаря встроенному беспроводному контроллеру и поддержке стандарта IEEE 802.11ac или добавлению точек доступа SonicWave 802.11ac Wave 2. Чтобы снизить стоимость и сложность подключения высокоскоростных точек беспроводного доступа и других устройств с поддержкой Power over Ethernet (PoE), таких как IP-камеры, телефоны и принтеры, TZ300P и TZ600P обеспечивают питание PoE/PoE+.

Распределенные предприятия розничной торговли и университетские городки могут воспользоваться различным функционалом SonicOS, чтобы получить еще большие преимущества. Удаленные филиалы могут безопасно обмениваться информацией с центральным офисом, используя виртуальные частные сети (VPN). Создание виртуальных локальных сетей (VLAN) позволяет сегментировать сеть на отдельные корпоративные группы и группы клиентов с правилами, определяющими уровень взаимодействия с устройствами в других VLAN. SD-WAN предлагает безопасную альтернативу дорогостоящим каналам MPLS, обеспечивая при этом стабильную производительность и доступность приложений. Развертывание межсетевых экранов (МСЭ) TZ в удаленных местах может быть легко выполнено с помощью технологии Zero-Touch Deployment, которая позволяет осуществить дистанционный провижининг МСЭ через облако.

Превосходные производительность и предотвращение угроз

Наше видение защиты сетей в современном, постоянно меняющемся ландшафте киберугроз - это автоматическое обнаружение и предотвращение угроз в режиме реального времени. Благодаря сочетанию облачных и встроенных технологий мы развертываем на наших межсетевых экранах защиту, чрезвычайно высокой эффективность которой была проверена независимым сторонним тестированием. Неизвестные угрозы отправляются в облачную многопоточную изолированную программную среду Capture Advanced Threat Protection (ATP) SonicWall для анализа. Систему Capture ATP дополняет наша запатентованная технология глубокой проверки памяти в реальном времени RTDMI™. Механизм RTDMI обнаруживает и блокирует вредоносные программы и угрозы «нулевого дня», выполняя проверку непосредственно в памяти. Технология RTDMI является точной, сводит к минимуму ложные срабатывания, а также выявляет и смягчает изощренные атаки, когда вредоносное ПО воздействует менее чем за 100 на-

Преимущества:

Гибкое интегрированное решение безопасности

- Защищенный SD-WAN
- Мощная ОС SonicOS
- Высокоскоростная беспроводная сеть стандарта 802.11ac
- Питание по Ethernet (PoE/PoE+)
- Сегментация сети с VLAN

Превосходные производительность и предотвращение угроз

- Запатентованная 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
- Специальная группа по исследованию угроз Capture Labs
- Безопасность конечных точек с помощью Capture Client

Простые развертывание, настройка и управление

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

носекунд. В совокупности наш запатентованный однопроходный механизм глубокого анализа пакетов без сборки (RFDPI) проверяет каждый байт каждого пакета, как входящего, так и исходящего трафика непосредственно на МСЭ. Благодаря использованию Capture ATP с технологией RTDMI в облачной платформе SonicWall Capture в дополнение к встроенным возможностям, включая предотвращение вторжений, защиту от вредоносного ПО и фильтрацию веб/URL-адресов, устройства серии TZ останавливают вредоносные программы, вымогательское ПО и другие угрозы на шлюзе. Для мобильных устройств, используемых вне периметра МСЭ, SonicWall Capture Client обеспечивает дополнительный уровень защиты, применяя передовые методы защиты от угроз, такие как машинное обучение и восстановление (rollback) системы. В Capture Client также используется глубокий контроль зашифрованного трафика TLS (DPI-SSL) на устройствах серии TZ путем установки и управления доверенными сертификатами TLS.

Продолжающийся рост использования шифрования для защиты веб-сеансов означает, что МСЭ обязательно должны сканировать зашифрованный трафик на наличие угроз. Устройства серии TZ 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.

Простые развертывание, настройка и управление

SonicWall предоставляет простые настройку и управление устройствами серии TZ и точками доступа SonicWave 802.11ac Wave 2 независимо от того, где вы их развернули. Централизованное управление, отчетность, лицензирование и аналитика осуществляются через наш облачный центр безопасности Capture, который обеспечивает максимальную прозрачность, гибкость и возможность централизованно управлять всей экосистемой безопасности SonicWall, используя единый экран.

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. Процесс требует минимального вмешательства пользователя и полностью автоматизирован для масштабирования МСЭ всего за несколько шагов. Это значительно сокращает время, стоимость и сложность, связанные с установкой и настройкой, а настройка безопасности и подключение происходят мгновенно и автоматически. Вместе упрощенное развертывание и настройка, а также простота управления позволяют организациям снизить совокупную стоимость владения и обеспечить высокую отдачу от инвестиций.

** 802.11ac в настоящее время не доступен на моделях SOHO/SOHO 250; Модели SOHO/SOHO 250 поддерживают стандарт 802.11a/b/g/n*

Интегрированная защита и обеспечение питанием ваших устройств PoE

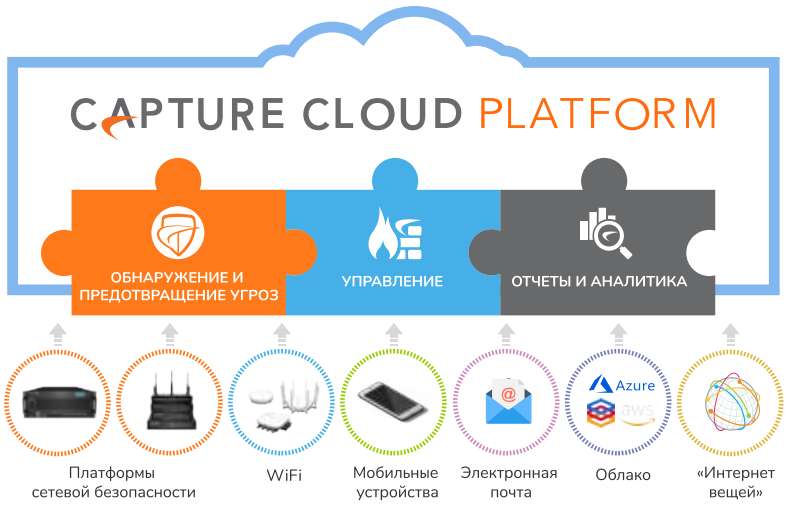
Обеспечьте питание устройств с поддержкой PoE без затрат и сложностей коммутаторов или инжекторов Power over Ethernet. Межсетевые экраны TZ300P и TZ600P объединяют технологию IEEE 802.3at для питания устройств PoE и PoE+, таких как точки беспроводного доступа, камеры, IP-телефоны и многих других. МСЭ сканирует весь трафик, приходящий с каждого устройства на каждое устройство, используя технологию глубокой проверки пакетов, а затем удаляет опасные угрозы, такие как вредоносные программы и попытки вторжения, даже в зашифрованных соединениях.

Платформа Capture Cloud Platform

Платформа SonicWall 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 TZ 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.

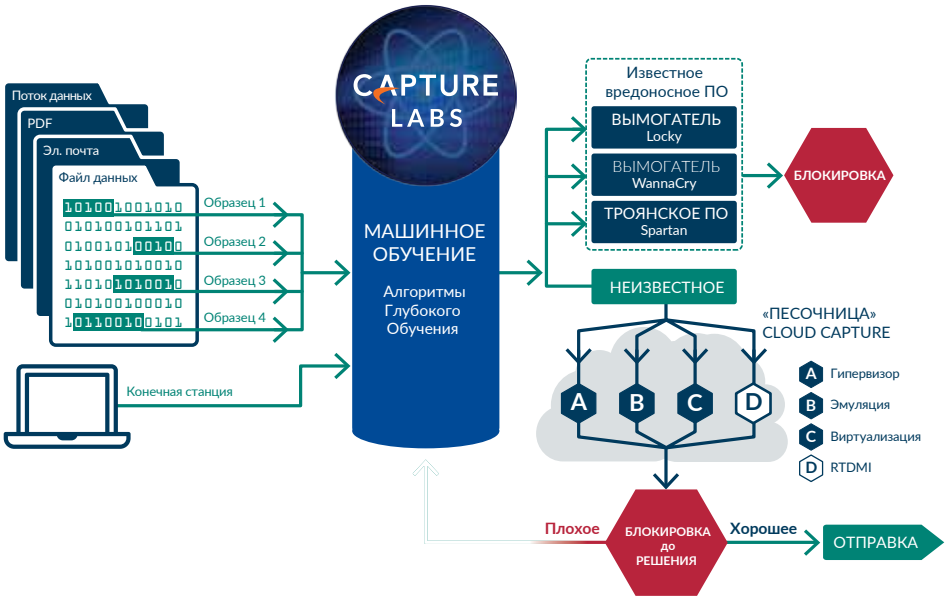


Advanced Threat Protection

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 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.



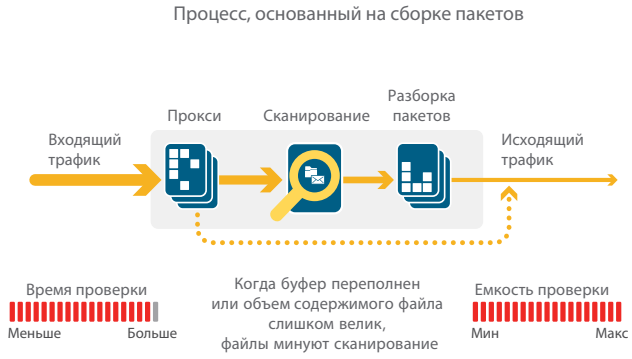
SONICWALL®

Механизм глубокой проверки пакетов без сборки

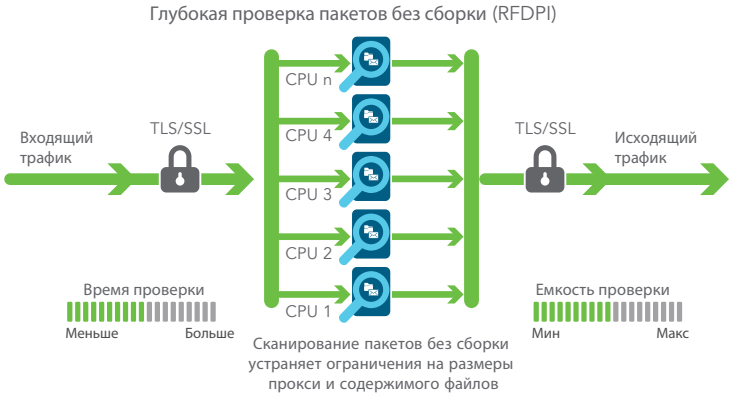
Глубокая проверка пакетов SonicWall без сборки (Reassembly-Free Deep Packet Inspection, RFDPI) – это однопроходная система проверки с малой задержкой, которая выполняет потоковый двунаправленный анализ трафика на высокой скорости без прокси или буферизации для эффективного обнаружения попыток вторжения 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



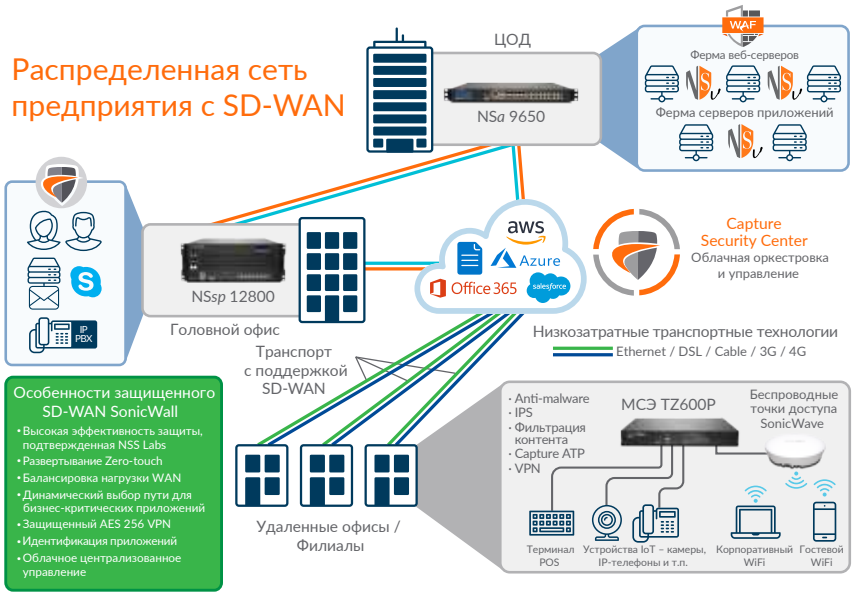
Потоковая архитектура SonicWall

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.

Распределенные сети

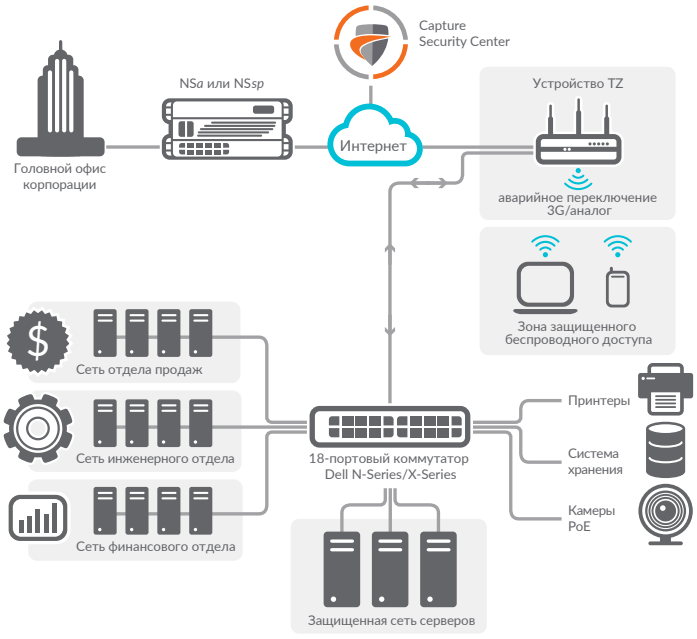
Благодаря своей гибкости межсетевые экраны серии TZ идеально подходят как для распределенного корпоративного развертывания, так и для развертывания на одной площадке. В распределенных сетях, подобных тем, которые есть в розничных организациях, каждый сайт имеет свое собственное устройство TZ, которое часто подключается к Интернету через локального провайдера, используя DSL, кабельную линию или соединение 3G/4G. В дополнение к доступу в Интернет каждый МСЭ использует соединение Ethernet для передачи пакетов между удаленными узлами и центральным офисом. Веб-сервисы и приложения SaaS, такие как Office 365, Salesforce и другие, предоставляются из центра обработки данных. С помощью технологии mesh VPN IT-администраторы могут создать топологию типа «звезда» для безопасной передачи данных между всеми площадками.



Технология SD-WAN в SonicOS является идеальным дополнением к МСЭ TZ, развернутым на удаленных площадках и в 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.

Capture Security Center

Задачу связывания распределенной сети воедино решает облачный центр безопасности Capture Security (CSC) SonicWall, который централизует развертывание, текущее управление и аналитику в реальном времени для устройств TZ. Ключевой особенностью CSC является система развертывания Zero-Touch Deployment. Настройка и развертывание МСЭ на нескольких площадках отнимает много времени и требует личного присутствия персонала на площадке. Zero-Touch Deployment устраняет эти проблемы, упрощая и ускоряя развертывание и провижининг SonicWall удаленно через облако. Точно так же CSC облегчает текущее управление, предоставляя облачное управление на одной панели для устройств SonicWall в сети. Для полной ситуационной осведомленности о среде сетевой безопасности SonicWall Analytics предлагает обзор на одной панели всех действий, происходящих внутри сети. Организации таким образом получают более глубокое представление об использовании приложений и производительности, уменьшая при этом влияние «теневой IT».



Единая площадка

Для развертываний на одной площадке очень выгодно применение интегрированного решения для безопасности сети. Межсетевые экраны серии TZ сочетают высокую эффективность безопасности с такими функциями, как встроенная беспроводная сеть 802.11ac и, в случае TZ300P и TZ600P, поддержка PoE/PoE+. Один и тот же механизм безопасности, используемый в нашей серии NSa среднего класса и высокопроизводительной серии NSsp представлен в устройствах серии TZ наряду с широким набором функций SonicOS. Конфигурирование и управление легко производится с помощью интуитивно понятного пользовательского интерфейса SonicOS. Организации экономят ценное место в стойке благодаря компактному форм-фактору настольного устройства.

SONICWALL®

Серия SonicWall TZ600

Для новых предприятий, предприятий розничной торговли и филиалов, которым нужна безопасность, производительность и такие опции, как поддержка 802.3at PoE+ по доступной цене, SonicWall TZ600 предоставляет защиту сетей с функционалом корпоративного класса и бескомпромиссной производительностью.

Спецификация	Серия TZ600
Пропускная способность МСЭ	1.9 Гбит/с
Пропускная способность Threat Prevention	800 Мбит/с
Пропускная способность Anti-malware	800 Мбит/с
Пропускная способность IPS	1.2 Гбит/с
Макс. число соединений	150,000
Число новых соединений/сек	12,000

TZ600P

Порты PoE/PoE+ (4 PoE/PoE+)

Светодиод «Питание»

Светодиод «Test»

Порт USB (аварийное переключение WAN 3G/4G)

Светодиодные индикаторы соединения и активности

Модуль расширения

Консольный порт

Коммутатор 8x1-GbE (конфигурируемый)

Порт X0 LAN
Порт X1 WAN

Питание 12B DC 2A

Серия SonicWall TZ500

Для растущих филиалов, малых и средних предприятий серия SonicWall TZ500 обеспечивает высокоэффективную бескомпромиссную защиту с сохранением производительности сети и опциональным встроенным двухдиапазонным беспроводным модулем стандарта 802.11ac.

Спецификация	Серия TZ500
Пропускная способность МСЭ	1.4 Гбит/с
Пропускная способность Threat Prevention	700 Мбит/с
Пропускная способность Anti-malware	700 Мбит/с
Пропускная способность IPS	1.0 Гбит/с
Макс. число соединений	150,000
Число новых соединений/сек	8,000

Светодиод «Питание»

Светодиод «Test»

Порт USB (аварийное переключение WAN 3G/4G)

Светодиодные индикаторы соединения и активности

Опциональный модуль беспроводной сети 802.11ac

Консольный порт

Коммутатор 6x1-GbE (конфигурируемый)

Порт X0 LAN
Порт X1 WAN

Питание 12B DC 2A

SONICWALL®

Серия SonicWall TZ400

Для предприятий малого бизнеса, розничной торговли и филиалов серия SonicWall TZ400 обеспечивает защиту корпоративного уровня. Устройство также предоставляет возможность развертывания беспроводной сети с помощью дополнительного двухдиапазонного беспроводного модуля стандарта 802.11ac, встроенного в межсетевой экран.

Спецификация	Серия TZ400
Пропускная способность МСЭ	1.3 Гбит/с
Пропускная способность Threat Prevention	600 Мбит/с
Пропускная способность Anti-malware	600 Мбит/с
Пропускная способность IPS	900 Мбит/с
Макс. число соединений	150,000
Число новых соединений/сек	6,000

Серия SonicWall TZ350/TZ300

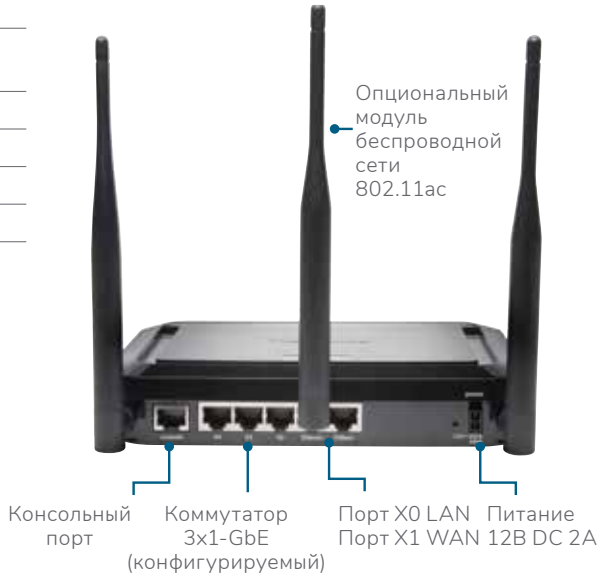
Серии SonicWall TZ300 и TZ350 предлагают комплексное решение, защищающее сети от современных атак. В отличие от продуктов потребительского уровня, эти устройства UTM сочетают в себе высокоскоростное предотвращение вторжений, защиту от вредоносных программ и фильтрацию контента/URL-адресов, а также широкую поддержку безопасного мобильного доступа для ноутбуков, смартфонов и планшетов вместе с опциональной встроенной беспроводной связью стандарта 802.11ac. Кроме того, TZ300 дополнительно предлагает поддержку стандарта 802.3at PoE+ для питания устройств с поддержкой PoEs.

Спецификация	Серия TZ350	Серия TZ300
Пропускная способность МСЭ	1.0 Гбит/с	750 Мбит/с
Пропускная способность Threat Prevention	335 Мбит/с	235 Мбит/с
Пропускная способность Anti-malware	335 Мбит/с	235 Мбит/с
Пропускная способность IPS	400 Мбит/с	300 Мбит/с
Макс. число соединений	100,000	100,000
Число новых соединений/сек	6,000	5,000

Серия SonicWall SOHO 250/SOHO

Для проводных и беспроводных сетей малого и домашнего офиса устройства серий SonicWall SOHO 250 и SOHO обеспечивают такую же защиту бизнес-класса, как и у крупных организаций, но по более доступной цене. Добавьте дополнительную беспроводную сеть стандарта 802.11n, чтобы обеспечить сотрудникам, клиентам и гостям безопасное беспроводное соединение.

Спецификация	Серия SOHO 250	Серия SOHO
Пропускная способность МСЭ	600 Мбит/с	300 Мбит/с
Пропускная способность Threat Prevention	200 Мбит/с	150 Мбит/с
Пропускная способность Anti-malware	200 Мбит/с	150 Мбит/с
Пропускная способность IPS	250 Мбит/с	200 Мбит/с
Макс. число соединений	50,000	10,000
Число новых соединений/сек	3,000	1,800



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.

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	Модели SonicWall TZ500 и TZ600 поддерживают высокую доступность в режиме Active/Standby с синхронизацией состояний. Модели SonicWall TZ300 и TZ400 поддерживают высокую доступность без синхронизации Active / Standby. На моделях SonicWall SOHO функция высокой доступности отсутствует.
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 внедрения для замены IPv4. С SonicOS аппаратная платформа будет поддерживать реализацию фильтрации и «прозрачного» режима МСЭ.
Гибкие варианты развертывания	Устройство серии TZ 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 (недоступно для модели SOHO).
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.
Безопасность беспроводных сетей	Беспроводная технология IEEE 802.11ac, доступная в качестве встроенной опции для SonicWall TZ300 - TZ500, может обеспечить пропускную способность до 1,3 Гбит/с с большей дальностью и надежностью. Дополнительный функционал стандарта 802.11a/b/g/n доступен на моделях SonicWall SOHO.

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
Автоматическое 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 TZ выступать в качестве концентратора VPN для тысяч других больших площадок, филиалов или домашних офисов.
Удаленный доступ с использованием клиентов SSL VPN или IPSec	Использует безклиентную 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[1]/терминальных сервисов[1] 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 неверных страны или тега ботнета, связанного с IP-адресом.
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 TZ, кроме SOHO. Для моделей SOHO доступна как отдельная лицензия.
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.

ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ (ПРОДОЛЖЕНИЕ)	
Функция	Описание
Внутризонная защита IPS	Усиливает внутреннюю безопасность, сегментируя сеть на несколько зон безопасности с IPS, 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 мер 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 могут преодолеть устаревшие системы безопасности, сосредоточенные 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, подключающимся 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 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/Ботнетам
- 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 приложения 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 анти-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
- Расширенное журналирование
- Качество обслуживания (QoS) на уровне 2
- Безопасность портов
- Динамическая маршрутизация (RIP/OSPF/BGP)
- Беспроводной контроллер SonicWall
- Маршрутизация по политикам (ToS/metric и ECMP)
- Асимметричная маршрутизация
- Сервер DHCP
- NAT
- Управление полосой пропускания
- Высокая доступность - Активный/Резервный с синхронизацией состояния[2]
- Балансировка входящей/исходящей нагрузки
- Режим моста L2, режим NAT
- Аварийное переключение WAN на 3G/4G
- Поддержка Common Access Card (CAC)

VoIP

- Детальная настройка качества обслуживания (QoS)
- Управление полосой пропускания
- DPI для трафика VoIP
- Поддержка гейткипера H.323 и SIP-прокси

Управление и мониторинг

- Графический пользовательский веб-интерфейс
- Интерфейс командной строки(CLI)
- SNMPv2/v3
- Централизованное управление и отчеты с помощью SonicWall GMS и Capture Security Center
- Журналирование
- Экспорт Netflow/IPFix
- Облачное резервное копирование конфигураций
- Визуализация приложений и полосы пропускания
- Управление по IPv4 и IPv6
- Управление коммутаторами Dell серий N и X, включая каскадирование[2]

Встроенная беспроводная сеть

- Два диапазона (2.4 ГГц и 5.0 ГГц)
- Поддержка беспроводных стандартов 802.11 a/b/g/n/ac[2]
- WIDS/WIPS
- Сервисы гостевой беспроводной сети
- Обмен сообщениями на хот-спот Lightweight hotspot messaging
- Сегментация виртуальной точки доступа
- Портал авторизации
- Облачный список доступа (ACL)

[1] *Необходима дополнительная подписка*
[2] *Функционал высокой доступности с синхронизацией состояния доступна только на моделях SonicWall TZ500 и SonicWall TZ600*

Системные спецификации устройств серии SonicWall TZ

ОБЩИЕ ПАРАМЕТРЫ МСЭ	СЕРИЯ SOHO	СЕРИЯ SOHO 250	СЕРИЯ TZ300	СЕРИЯ TZ350
Операционная система	SonicOS			
Интерфейсы	5x1GbE, 1 USB, 1 консольный		5x1GbE, 1 USB, 1 консольный	5x1GbE, 1 USB, 1 консольный
Поддержка питания по Ethernet (PoE)	—	—	TZ300P - 2 порта (2 PoE или 1 PoE+)	—
Расширения	USB			
Управление	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs			
Число пользователей системы единого входа (SSO)	250	350	500	500
Число интерфейсов VLAN	25			
Число точек доступа (максимальное)	2	4	8	8
ПРОИЗВОДИТЕЛЬНОСТЬ МСЭ/VPN	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Пропускная способность в режиме проверки МСЭ[1]	300 Мбит/с	600 Мбит/с	750 Мбит/с	1.0 Гбит/с
Пропускная способность в режиме Threat Prevention[2]	150 Мбит/с	200 Мбит/с	235 Мбит/с	335 Мбит/с
Пропускная способность в режиме Application inspection[2]	—	275 Мбит/с	375 Мбит/с	600 Мбит/с
Пропускная способность в режиме IPS[2]	200 Мбит/с	250 Мбит/с	300 Мбит/с	400 Мбит/с
Пропускная способность проверки на вредоносное ПО[2]	150 Мбит/с	200 Мбит/с	235 Мбит/с	335 Мбит/с
Пропускная способность в режиме проверки и расшифровки TLS/SSL (DPI SSL)[2]	30 Мбит/с	50 Мбит/с	60 Мбит/с	65 Мбит/с
Пропускная способность IPSec VPN[3]	150 Мбит/с	200 Мбит/с	300 Мбит/с	430 Мбит/с
Число новых соединений в секунду	1,800	3,000	5,000	6,000
Макс. число соединений (SPI)	10,000	50,000	100,000	100,000
Макс. число соединений (DPI)	10,000	50,000	90,000	90,000
Макс. число соединений (DPI SSL)	250	25,000	25,000	25,000
VPN	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Число туннелей VPN «площадка-площадка»	10	10	10	15
Число клиентов IPSec VPN (макс.)	1 (5)	1 (5)	1 (10)	1 (10)
Число лицензий SSL VPN (макс.)	1 (10)	1 (25)	1 (50)	1 (75)
Число лицензий Virtual assist в комплекте (макс.)	—	1 (30-дн. пробная)	1 (30-дн. пробная)	1 (30-дн. пробная)
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			
Поддержка сертификатов	Verisign, Thawte, Cybertrust, RSA Keon, Entrust и Microsoft CA для SonicWall-to-SonicWall VPN, SCEP			
Функции VPN	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Избыточный шлюз VPN, VPN с маршрутизацией			
Поддерживаемые платформы клиентов VPN	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10			
Платформы для NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE			
Мобильные платформы для Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)			
СЕРВИСЫ БЕЗОПАСНОСТИ	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Сервисы глубокой проверки пакетов	Антивирус на шлюзе, защита от шпионского ПО, предотвращение вторжений, DPI SSL			
Сервис контентной фильтрации (CFS)	HTTP URL, HTTPS IP, сканирование по ключевым словам и контенту, комплексная фильтрация на основе типа файлов, таких как ActiveX, Java, Cookies для обеспечения приватности, разрешающие/запрещающие списки			
Комплексный анти-спам сервис	Поддерживается			
Визуализация приложений	Нет	Да	Да	Да
Контроль приложений	Да	Да	Да	Да
Capture Advanced Threat Protection	Нет	Да	Да	Да
СЕТЬ	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
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			
Протоколы маршрутизации[4]	BGP[4], OSPF, RIPv1/v2, статические маршруты, маршрутизация на основе политик			
Качество обслуживания (QoS)	Приоритет полосы пропускания, максимальная полоса пропускания, гарантированная полоса пропускания, маркировка DSCP, 802.1e (WMM)			

Системные спецификации устройств серии SonicWall TZ (продолжение)

СЕТЬ (ПРОДОЛЖЕНИЕ)	СЕРИЯ SOHO	СЕРИЯ SOHO 250	СЕРИЯ TZ300	СЕРИЯ TZ350
Аутентификация	LDAP (множественные домены), XAUTH/RADIUS, SSO, Novell, внутренняя база данных пользователей		LDAP (множественные домены), XAUTH/RADIUS, SSO, Novell, внутренняя база данных пользователей, терминальные сервисы, Citrix, Common Access Card (CAC)	
Число пользователей в локальной базе данных	150			
VoIP	Полная поддержка H.323v1-5, SIP			
Стандарты	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Сертификации	FIPS 140-2 (с Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus			
Ожидаемые сертификации	Common Criteria NDPP (МСЭ и IPS)			
Common Access Card (CAC)	Поддерживается			
Высокая доступность	Нет		Активный/резервный	
АППАРАТНАЯ ПЛАТФОРМА	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Форм-фактор	Настольный			
Источник питания	24 Вт внешний		24 Вт внешний 65 Вт внешний (только TZ300P)	24 Вт внешний
Макс. потребляемая мощность (Вт)	6.4 / 11.3	6.9 / 11.3	6.9 / 12.0	6.9 / 12.0
Входное питание	100 to 240 В AC, 50-60 Гц, 1 А			
Совокупное тепловыделение	21.8 / 38.7 BTU	23.5 / 38.7 BTU	23.5 / 40.9 BTU	23.5 / 40.9 BTU
Размеры	3.6 x 14.1 x 19 см 1.42 x 5.55 x 7.48"		3.5 x 13.4 x 19 см 1.38 x 5.28 x 7.48"	3.5 x 13.4 x 19 см 1.38 x 5.28 x 7.48"
Вес	0.34 кг / 0.75 фунт. 0.48 кг / 1.06 фунт.		0.73 кг / 1.61 фунт. 0.84 кг / 1.85 фунт.	0.73 кг / 1.61 фунт. 0.84 кг / 1.85 фунт.
Вес WEEE	0.80 кг / 1.76 фунт. 0.94 кг / 2.07 фунт.		1.15 кг / 2.53 фунт. 1.26 кг / 2.78 фунт.	1.15 кг / 2.53 фунт. 1.26 кг / 2.78 фунт.
Вес с упаковкой	1.20 кг / 2.64 фунт. 1.34 кг / 2.95 фунт.		1.37 кг / 3.02 фунт. 1.48 кг / 3.26 фунт.	1.37 кг / 3.02 фунт. 1.48 кг / 3.26 фунт.
Среднее время наработки на отказ (в годах)	58.9/56.1 (беспроводные модели)	56.1	56.1	56.1
Допустимая температура окружающей среды (Эксплуатация/Хранение)	32°-105° F (0°-40° C)/от -40° до 158° F (от -40° до 70° C)			
Влажность	5-95% без конденсации			
СООТВЕТСТВИЕ НОРМАТИВАМ	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Соответствие главным нормативам (модели с проводной сетью)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP		FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP	
Соответствие главным нормативам (модели с беспроводной сетью)	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH		FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	
ИНТЕГРИРОВАННАЯ БЕСПРОВОДНАЯ СЕТЬ	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Стандарты	802.11 a/b/g/n		802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	

Системные спецификации устройств серии SonicWall TZ (продолжение)

Частотные диапазоны[5]	802.11a: 5.180-5.825 ГГц; 802.11b/g: 2.412-2.472 ГГц; 802.11n: 2.412-2.472 ГГц, 5.180-5.825 ГГц		802.11a: 5.180-5.825 ГГц; 802.11b/g: 2.412-2.472 ГГц; 802.11n: 2.412-2.472 ГГц, 5.180-5.825 ГГц; 802.11ac: 2.412-2.472 ГГц, 5.180-5.825 ГГц	
ИНТЕГРИРОВАННАЯ БЕСПРОВОДНАЯ СЕТЬ	**СЕРИЯ SOHO**	**СЕРИЯ SOHO 250**	**СЕРИЯ TZ300**	**СЕРИЯ TZ350**
Рабочие каналы	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 ГГц): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 ГГц): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64;		802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 ГГц): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 ГГц): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64	
Выходная мощность передачи	На основании нормативного домена, указанного системным администратором			
Управление мощностью передачи	Поддерживается			
Поддерживаемые скорости передачи данных	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11b: 1, 2, 5.5, 11 Мбит/с на канал; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Мбит/с на канал		802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11b: 1, 2, 5.5, 11 Мбит/с на канал; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Мбит/с на канал; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Мбит/с на канал	
Технологии модуляции	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)		802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	

*Для будущего использования.

[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.*

[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] *BGP доступен только на моделях SonicWall TZ400, TZ500 и TZ600.*

[5] *Все модели TZ с интегрированной беспроводной сетью могут поддерживать диапазон 2.4 ГГц или 5 ГГц. Для поддержки двух диапазонов, пожалуйста, используйте беспроводные точки доступа SonicWall.*

Системные спецификации устройств серии SonicWall TZ (продолжение)

ОБЩИЕ ПАРАМЕТРЫ МСЭ	СЕРИЯ TZ400	СЕРИЯ TZ500	СЕРИЯ TZ600
Операционная система		SonicOS	
Интерфейсы	7x1GbE, 1 USB, 1 консольный	8x1GbE, 2 USB, 1 консольный	10x1GbE, 2 USB, 1 консольный, 1 слот расширения
Поддержка питания по Ethernet (PoE)	—	—	TZ600P - 4 порта (4 PoE или 4 PoE+)
Расширения	USB	2 USB	Слот расширения (задний)*, 2 USB
Управление	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs		
Число пользователей системы единого входа (SSO)	500	500	500
Число интерфейсов VLAN	50	50	50
Число точек доступа (максимальное)	16	16	24
ПРОИЗВОДИТЕЛЬНОСТЬ МСЭ/VPN	**СЕРИЯ TZ400**	**СЕРИЯ TZ500 SERIES**	**СЕРИЯ TZ600**
Пропускная способность в режиме проверки МСЭ[1]	1.3 Гбит/с	1.4 Гбит/с	1.9 Гбит/с
Пропускная способность в режиме предотвращения угроз[2]	600 Мбит/с	700 Мбит/с	800 Мбит/с
Пропускная способность проверки приложений[2]	1.2 Гбит/с	1.3 Гбит/с	1.8 Гбит/с
Пропускная способность в режиме IPS[2]	900 Мбит/с	1.0 Гбит/с	1.2 Гбит/с
Пропускная способность проверки на вредоносное ПО[2]	600 Мбит/с	700 Мбит/с	800 Мбит/с
Пропускная способность в режиме проверки и расшифровки TLS/SSL (DPI SSL)[2]	180 Мбит/с	225 Мбит/с	300 Мбит/с
Пропускная способность IPSec VPN[3]	900 Мбит/с	1.0 Гбит/с	1.1 Гбит/с
Число новых соединений в секунду	6,000	8,000	12,000
Макс. число соединений (SPI)	150,000	150,000	150,000
Макс. число соединений (DPI)	125,000	125,000	125,000
Макс. число соединений (DPI SSL)	25,000	25,000	25,000
VPN	**СЕРИЯ TZ400**	**СЕРИЯ TZ500**	**СЕРИЯ TZ600**
Число туннелей VPN «площадка-площадка»	20	25	50
Число клиентов IPSec VPN (макс.)	2 (25)	2 (25)	2 (25)
Число лицензий SSL VPN (макс.)	2 (100)	2 (150)	2 (200)
Число лицензий Virtual assist в комплекте (макс.)	1 (30-дн. пробная)	1 (30-дн. пробная)	1 (30-дн. пробная)
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		
Поддержка сертификатов	Verisign, Thawte, Cybertrust, RSA Keon, Entrust и Microsoft CA для SonicWall-to- SonicWall VPN, SCEP		
Функции VPN	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Избыточный шлюз VPN, VPN с маршрутизацией		
Поддерживаемые платформы клиентов VPN	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10		
Платформы для NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE		
Мобильные платформы для Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)		
СЕРВИСЫ БЕЗОПАСНОСТИ	**СЕРИЯ TZ400**	**СЕРИЯ TZ500**	**СЕРИЯ TZ600**
Сервисы глубокой проверки пакетов	Антивирус на шлюзе, защита от шпионского ПО, предотвращение вторжений, DPI SSL		
Сервис контентной фильтрации (CFS)	HTTP URL, HTTPS IP, сканирование по ключевым словам и контенту, комплексная фильтрация на основе типа файлов, таких как ActiveX, Java, Cookies для обеспечения приватности, разрешающие/запрещающие списки		
Комплексный анти-спам сервис	Поддерживается		
Визуализация приложений	Да	Да	Да
Контроль приложений	Да	Да	Да
Capture Advanced Threat Protection	Да	Да	Да
СЕТЬ	**СЕРИЯ TZ400**	**СЕРИЯ TZ500**	**СЕРИЯ TZ600**
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		
Протоколы маршрутизации[4]	BGP[4], OSPF, RIPv1/v2, статические маршруты, маршрутизация на основе политик		
Качество обслуживания (QoS)	Приоритет полосы пропускания, максимальная полоса пропускания, гарантированная полоса пропускания, маркировка DSCP, 802.1e (WMM)		

Системные спецификации устройств серии SonicWall TZ (продолжение)

СЕТЬ	СЕРИЯ TZ400	СЕРИЯ TZ500	СЕРИЯ TZ600
Аутентификация	LDAP (множественные домены), XAUTH/RADIUS, SSO, Novell, внутренняя база данных пользователей, терминальные сервисы, Citrix, Common Access Card (CAC)		
Число пользователей в локальной базе данных	150	250	
VoIP	Полная поддержка H.323v1-5, SIP		
Стандарты	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Сертификации	FIPS 140-2 (с Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus		
Ожидаемые сертификации	Common Criteria NDPP (Firewall и IPS)		
Common Access Card (CAC)	Поддерживается		
Высокая доступность	Активный/резервный	Активный/резервный с синхронизацией состояний	
АППАРАТНАЯ ПЛАТФОРМА	**СЕРИЯ TZ400**	**СЕРИЯ TZ500**	**СЕРИЯ TZ600**
Форм-фактор	Настольный		
Блок питания	24 Вт внешний	36 Вт внешний	60 Вт внешний 180 Вт внешний (только TZ600P)
Макс. потребляемая мощность (Вт)	9.2 / 13.8	13.4 / 17.7	16.1
Входное питание	100-240 В AC, 50-60 Гц, 1 A		
Совокупное тепловыделение	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
Размеры	3.5 x 13.4 x 19 см 1.38 x 5.28 x 7.48"	3.5 x 15 x 22.5 см 1.38 x 5.91 x 8.86"	3.5 x 18 x 28 см 1.38 x 7.09 x 11.02"
Вес	0.73 кг / 1.61 фунт. 0.84 кг / 1.85 фунт.	0.92 кг / 2.03 фунт. 1.05 кг / 2.31 фунт.	1.47 кг / 3.24 фунт.
Вес WEEE	1.15 кг / 2.53 фунт. 1.26 кг / 2.78 фунт.	1.34 кг / 2.95 фунт. 1.48 кг / 3.26 фунт.	1.89 кг /4.16 фунт.
Вес с упаковкой	1.37 кг / 3.02 фунт. 1.48 кг / 3.26 фунт.	1.93 кг / 4.25 фунт. 2.07 кг / 4.56 фунт.	2.48 кг / 5.47 фунт.
Среднее время наработки на отказ (в годах)	54.0	40.8	18.4
Допустимая температура окружающей среды (Эксплуатация/Хранение)	32°-105° F (0°-40° C)/от -40° до 158° F (от -40° до 70° C)		
Влажность	5-95% без конденсации		
СООТВЕТСТВИЕ НОРМАТИВАМ	**СЕРИЯ TZ400**	**СЕРИЯ TZ500**	**СЕРИЯ TZ600**
Соответствие главным нормативам (модели с проводной сетью)	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP	FCC Class B, ICES Class B, CE (EMC, LVD, RoHS), C-Tick, VCCI Class B, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, KCC/MSIP
Соответствие главным нормативам (модели с беспроводной сетью)	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	FCC Class B, FCC RF ICES Class B, IC RF CE (RED, RoHS), RCM, VCCI Class B, MIC/TELEC, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH	—

Системные спецификации устройств серии SonicWall TZ (продолжение)

ИНТЕГРИРОВАННАЯ БЕСПРОВОДНАЯ СЕТЬ	СЕРИЯ TZ400	СЕРИЯ TZ500	СЕРИЯ TZ600
Стандарты	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS		—
Частотные диапазоны[5]	802.11a: 5.180-5.825 ГГц; 802.11b/g: 2.412-2.472 ГГц; 802.11n: 2.412-2.472 ГГц, 5.180-5.825 ГГц; 802.11ac: 2.412-2.472 ГГц, 5.180-5.825 ГГц		—
Рабочие каналы	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4; 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only); 802.11n (2.4 ГГц): US and Canada 1-11, Europe 1-13, Japan 1-13; 802.11n (5 ГГц): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64; 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64		—
Выходная мощность передачи	На основании нормативного домена, указанного системным администратором		—
Управление мощностью передачи	Поддерживается		—
Поддерживаемые скорости передачи данных	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11b: 1, 2, 5.5, 11 Мбит/с на канал; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с на канал; 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Мбит/с на канал; 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 Мбит/с на канал		—
Технологии модуляции	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)		—

Информация по заказу устройств семейства SonicWall TZ

Устройства	SKU
SOHO 250 с годовой подпиской TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC с годовой подпиской TotalSecure Advanced Edition	02-SSC-1824
TZ300 с годовой подпиской TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC с годовой подпиской TotalSecure Advanced Edition	01-SSC-1703
TZ300P с годовой подпиской TotalSecure Advanced Edition	02-SSC-0602
TZ350 с годовой подпиской TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC с годовой подпиской TotalSecure Advanced Edition	02-SSC-1851
TZ400 с годовой подпиской TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC с годовой подпиской TotalSecure Advanced Edition	01-SSC-1706
TZ500 с годовой подпиской TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC с годовой подпиской TotalSecure Advanced Edition	01-SSC-1709
TZ600 с годовой подпиской TotalSecure Advanced Edition	01-SSC-1711
TZ600P с годовой подпиской TotalSecure Advanced Edition	02-SSC-0600
Варианты с высокой доступностью (каждое устройство должно быть одной и той же модели)	
TZ500 High Availability	01-SSC-0439
TZ600 High Availability	01-SSC-0220

Сервисы	SKU
Для серии SonicWall SOHO 250	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	02-SSC-1726
Защита от сложных угроз Capture Advanced Threat Protection для SOHO 250 (1 год)	02-SSC-1732
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	02-SSC-1750
Сервис контентной фильтрации (1 год)	02-SSC-1744
Комплексный анти-спам сервис (1 год)	02-SSC-1823
Поддержка 24x7 (1 год)	02-SSC-1720
Для серии SonicWall TZ300	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	01-SSC-1430
Защита от сложных угроз Capture Advanced Threat Protection для TZ300 (1 год)	01-SSC-1435
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	01-SSC-0602
Сервис контентной фильтрации (1 год)	01-SSC-0608
Комплексный анти-спам сервис (1 год)	01-SSC-0632
Поддержка 24x7 (1 год)	01-SSC-0620
Для серии SonicWall TZ350	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	02-SSC-1773
Защита от сложных угроз Capture Advanced Threat Protection для TZ350 (1 год)	02-SSC-1779
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	02-SSC-1797
Сервис контентной фильтрации (1 год)	02-SSC-1791
Комплексный анти-спам сервис (1 год)	02-SSC-1809
Поддержка 24x7 (1 год)	02-SSC-1767

Информация по заказу устройств семейства SonicWall TZ

Для серии SonicWall TZ400	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	01-SSC-1440
Защита от сложных угроз Capture Advanced Threat Protection для TZ400 (1 год)	01-SSC-1445
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	01-SSC-0534
Сервис контентной фильтрации (1 год)	01-SSC-0540
Комплексный анти-спам сервис (1 год)	01-SSC-0561
Поддержка 24x7 (1 год)	01-SSC-0552
Для серии SonicWall TZ500	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	01-SSC-1450
Защита от сложных угроз Capture Advanced Threat Protection для TZ500 (1 год)	01-SSC-1455
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	01-SSC-0458
Сервис контентной фильтрации (1 год)	01-SSC-0464
Комплексный анти-спам сервис (1 год)	01-SSC-0482
Поддержка 24x7 (1 год)	01-SSC-0476
Для серии SonicWall TZ600	
Advanced Gateway Security Suite - Защита от сложных угроз Capture ATP, предотвращение угроз, управление МСЭ и отчеты, наблюдение за «теневым IT», и поддержка 24x7 (1 год)	01-SSC-1460
Защита от сложных угроз Capture Advanced Threat Protection для TZ600 (1 год)	01-SSC-1465
Антивирус на шлюзе, предотвращение вторжений и контроль приложений (1 год)	01-SSC-0228
Сервис контентной фильтрации (1 год)	01-SSC-0234
Комплексный анти-спам сервис (1 год)	01-SSC-0252
Поддержка 24x7 (1 год)	01-SSC-0246

Нормативные номера моделей

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/ TZ300P	APL28-0B4/APL28-0B5/ APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3

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.

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

Datasheet-TZ Series-RUS-VG-340