Barracuda
Your journey, secured.

Barracuda SecureEdge

Обеспечение безопасности пользователей, рабочих площадок и «вещей», а также подключение к любому приложению независимо от места его размещения

SecureEdge обеспечивает безопасный доступ к приложениям, облачную защиту конечных устройств и автоматизированное подключение к сети SD-WAN для предприятий и промышленных объектов любого типа и размера. Удаленные пользователи получают доступ непосредственно к приложениям с любого типа устройств. Обеспечение исполнения политики нулевого доверия, фильтрация URL-адресов и оптимизация трафика на последней миле — все это гарантирует, что доступ к приложениям всегда будет безопасным и оптимизированным, чтобы максимально эффективно использовать общие линии Интернета.

Обеспечение безопасности пользователей, площадок и «вещей»

Гибридный состав сотрудников, архитектуры прямого доступа к приложениям и миграция в облако в значительной степени сделали традиционные архитектуры безопасности неактуальными. Появились новые облачные решения для обеспечения безопасности, но их подход «только облако», ориентированный на крупные предприятия, часто приводит к нестабильной защите или плохой работе пользователей, особенно при доступе к гибридным приложениям. Barracuda SecureEdge была создана с нуля как платформа безопасности, управляемая из облака, предоставляемая из облака и доступная в виде автоматически управляемых пограничных сервисов для любого типа устройств, развертывания или платформы.

Благодаря обширной сети Barracuda Threat Intelligence Network интеллектуальные средства обеспечения безопасности, основанные на технологиях искусственного интеллекта, выходят за рамки обычного развертывания площадки или облачного сервиса, обеспечивая расширенную защиту любого пользователя на любом устройстве и всех «вещей».

Подключение любых устройств, приложений и облачных/гибридных сред

Традиционные VPN-решения оказались небезопасными по своей сути, не имеют возможностей масштабирования и не отвечают требованиям кибербезопасности, предъявляемым многими регулирующими органами. Появляющиеся решения с нулевым уровнем доверия предназначены только для обеспечения безопасного доступа к облачным ресурсам и зачастую сложны в настройке, управлении и использовании в реальных условиях. Сегодня пользователи любых устройств ожидают безопасного и надежного доступа к любым приложениям, независимо от того, размещены ли они в облаке или на локальном компьютере. Кроме того, решение должно быть простым в использовании и расширять доступ к приложениям для оптимальной работы пользователей. Barracuda SecureEdge Access обеспечивает все перечисленное. Доступный для любого типа устройств, любой платформы, облака или локальной сети, он использует возможности SD-WAN на локальных устройствах и оптимизирует поток приложений для обеспечения непревзойденного качества работы удаленных пользователей.

Простота приобретения, развертывания и управления

Платформа Barracuda SecureEdge — это SASE-решение от одного поставщика, в котором грамотно интегрированы и автоматизированы все компоненты. Основные сервисы доступны в виде SaaS, в виртуальной глобальной сети Azure и даже в виде частных экземпляров. Подключение осуществляется путем развертывания устройства на площадке с автоматической оптимизацией SD-WAN до сервиса. Удаленные пользователи на любой операционной системе самостоятельно регистрируются с помощью SecureEdge Access Agent, который доступен в любом магазине приложений и включает до 5 устройств для ZTNA и Secure Internet Access (SIA).
Все это централизованно управляется и контролируется с помощью облачного SecureEdge Manager. Сети на основе намерений и политики безопасности на основе намерений обеспечивают наиболее быстрый и интуитивно понятный способ централизованного управления решением SASE, включая ZTNA и безопасную SD-WAN для подключения.

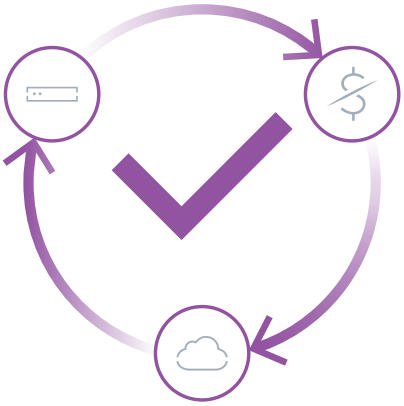
Преимущества Barracuda SecureEdge для бизнеса

Последовательное обеспечение безопасности площадок, пользователей и «вещей»

Политики безопасности сначала определяются на облачном портале управления, а затем распространяются на каждого пользователя, площадку, IoT-устройство или оборудование в цеху. Благодаря обширной сети Barracuda Threat Intelligence Network наши интеллектуальные средства обеспечения безопасности выходят за рамки обычного развертывания площадок или облачных сервисов и обеспечивают расширенную защиту любого пользователя на любом устройстве и всех «вещей».

Безопасное подключение к любому приложению в любое время и в любом месте

Сегодня многие организации нуждаются в том, чтобы их пользователи получали доступ к приложениям в виде SaaS, размещенным в облачной среде и на локальных площадках. Мало того, зачастую организации также должны поддерживать модель, при которой большинство сотрудников могут работать в разных офисах компании, филиалах, дома и в дороге. Barracuda SecureEdge Access обеспечивает безопасный доступ с нулевым уровнем доверия к любому приложению, независимо от места его размещения и с любого типа устройства.



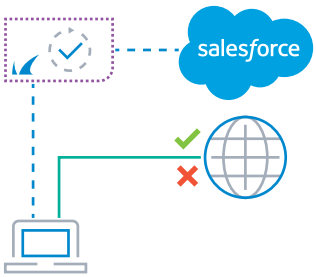
Экономия затрат при переходе на облачные технологии

Устройства SecureEdge для рабочих площадок, полностью интегрированные в концепцию SASE компании SecureEdge, включают в себя защищенные возможности SD-WAN для обеспечения быстрого доступа к приложениям, размещенным в облаке. Устройства SecureEdge для площадок быстро развертываются в автоматическом режиме и самостоятельно подключаются к облачным сервисам. Они оптимизируют трафик облачных каналов связи за счет снижения потерь пакетов и других современных функций оптимизации SD-WAN, что позволяет предприятиям отказаться от дорогостоящих выделенных линий.

Операционная эффективность благодаря консолидации с одним поставщиком

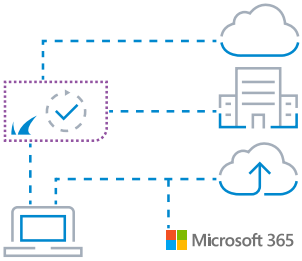
Благодаря тесной интеграции различных компонентов предприятия могут объединить решения нескольких поставщиков в одно целое, сократить штат ИТ-специалистов, консолидировать и уменьшить количество подписок и при этом получить более высокий уровень безопасности, ускорить доступ к приложениям, улучшить связь с площадкой и повысить гибкость ИТ-функций своего бизнеса.

Примеры использования SASE-платформы Barracuda SecureEdge



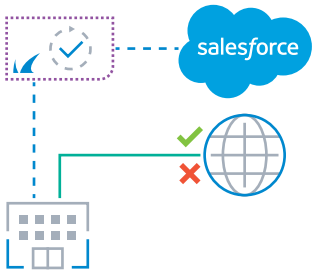
Защищенный доступ в Интернет (SIA) для мобильных пользователей

Сегодня многие сотрудники работают в разных офисах компании, филиалах, дома и в дороге. И при этом уровень корпоративных политик безопасности, например, по допустимому доступу в Интернет, должен быть одинаковым. Опираясь на обширную сеть Barracuda Threat Intelligence Network и интеллектуальную систему безопасности, SecureEdge Access Agent обеспечивает безопасность и соблюдение политик на любом устройстве на любой платформе.



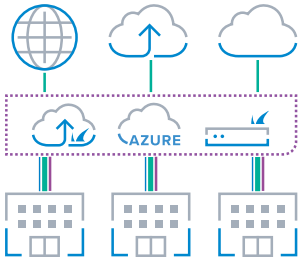
Защищенный доступ к частным и SaaS-приложениям (ZTNA)

Обеспечение прямого защищенного доступа ко всем санкционированным приложениям с непрерывной оценкой безопасности и соответствия требованиям, независимо от места размещения приложений и для любого пользователя на любом устройстве. Оптимизация сетевого трафика «последней мили» для наиболее эффективного использования общих каналов передачи данных в Интернет.



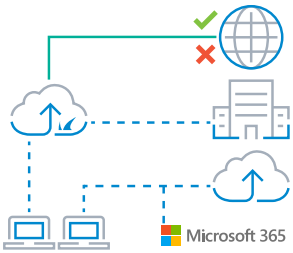
Защищенный веб-шлюз (SWG) для офисов и филиалов

Устройства SecureEdge для рабочих площадок защищают периметр офиса и любые устройства внутри от вредоносных программ, шпионских программ и другого нежелательного содержимого, распространяемого через Интернет. Помимо обнаружения вредоносного кода, это фильтрация URL-адресов и контроль приложений для тысяч популярных приложений (даже не веб-ориентированных). Обеспечение может осуществляться как на устройстве, так и на сервисном уровне SecureEdge.



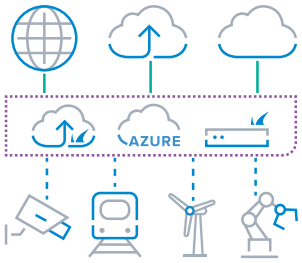
Подключение и безопасность офисов с помощью облачных технологий

Безопасное подключение любого филиала к облаку и обеспечение его защиты от таких интернет-угроз, как вредоносные программы, программы-вымогатели и шпионские программы. Безопасная сеть SD-WAN обеспечивает переход к облаку для оптимальной работы приложений.



Брандмауэр как услуга (FWaaS)

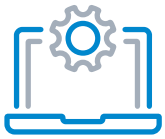
Обеспечение безопасности нового поколения в облаке, безопасного доступа в Интернет и управления приложениями для любого удаленного пользователя на любом устройстве.



Безопасность и возможности подключения «вещей» (IoT/ICS)

Простое и быстрое подключение практически любого IoT-устройства или тяжелой техники на производстве к выбранному вами облаку или необходимому офису. Централизованное обеспечение необходимой безопасности.

Основные характеристики решения Barracuda SecureEdge



Автоматическая инициализация агента

Удаленные пользователи легко самостоятельно регистрируются на своих устройствах (до 5 устройств на пользователя). SecureEdge Access Agent доступен для бесплатной загрузки в любом магазине приложений и даже для Linux. Для начала работы достаточно щелкнуть на ссылке, присланной в письме о регистрации.

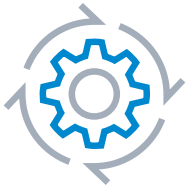
Оптимизация на последней миле

Встроенная оптимизация интернет-трафика от сервиса до SASE-агента позволяет конечным точкам использовать большую часть доступной полосы пропускания на общих интернет-линиях для повышения производительности приложений. В основе технологии устранения потерь пакетов лежат случайные линейные сетевые коды (RLNC) — мощная схема кодирования. Алгоритмы, основанные на кодах RLNC, гораздо быстрее реагируют на потери и быстрее устраняют их на лету, тем самым требуя меньшего количества повторных передач пакетов и снижая накладные расходы устройств.

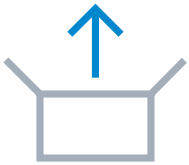
Управление сетями и политиками на основе намерений

В прошлом решения по обеспечению безопасности либо были сложны в использовании, либо не обладали достаточными возможностями. Брандмауэры и другие решения по обеспечению безопасности основывались на назначении сетей, диапазонов IP-адресов и защитных возможностей специализированных продуктов для этих сетей. Операции, основанные на намерениях, строятся с нуля в рамках концепции SecureEdge Manager для нашей единой платформы SASE. SASE-платформа Barracuda SecureEdge строго привязана к конкретным пользователям, группам и приложениям. Таким образом, удаленные пользователи могут гораздо быстрее получать доступ к частным и публичным облачным приложениям, а также к Интернету.

«Одноразовое» управление на основе намерений



Помимо тысяч предопределенных приложений, платформа SecureEdge SASE позволяет создавать частные приложения, которые могут быть размещены в любом месте. Это быстро, легко и нужно сделать только один раз, чтобы затем совместно использовать в определениях политик безопасности, SD-WAN и ZTNA. Все необходимые действия по оптимизации сети и маршрутизации выполняются абсолютно прозрачно в фоновом режиме и автоматически применяются к каждой площадке, каждому пользователю или экземпляру сервиса.

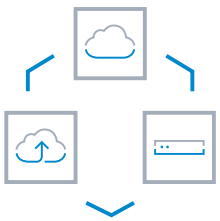


Автоматическое подключение для любой площадки

Внедрение площадок и «вещей»на платформу Barracuda SecureEdge SASE выполняется максимально простым способом. Всего пара щелчков мышью — и конфигурация в облачном менеджере завершена, а устройства площадки отправлены на удаленный объект. Автоматическое развертывание без участия пользователя подключает площадки и IoT-устройства к ближайшей точке входа SecureEdge.

Авто-SD-WAN

После подключения к питанию и включения каждое устройство площадки автоматически использует все доступные восходящие каналы для подключения к сервису SASE. Благодаря настройкам политики SD-WAN, предопределенным для тысяч распространенных бизнес-приложений, устройствам обеспечивается постоянное использование наилучшего маршрута восходящей линии связи для данного приложения.



Гибкая граница обслуживания

Сервис SASE Barracuda SecureEdge доступен как услуга SaaS, управляемая непосредственно компанией Barracuda Networks, как SecureEdge for Virtual WAN в Microsoft Azure и управляемая Microsoft, либо в виде виртуальных и аппаратных устройств, управление и размещение которых осуществляется заказчиком или доверенным партнером. Независимо от типа развертывания, все управление конфигурацией на основе намерений осуществляется с облачного портала SecureEdge Manager. Затем сервис берет на себя заботу о распространении и внедрении изменений для каждой границы сервиса, площадки, пользователя или «вещи».

Один поставщик

Платформа Barracuda SecureEdge — это единственное решение, обеспечивающее безопасность и подключение пользователей, площадок и «вещей» в удобном облачном формате, объединяющее в единую платформу разрозненные технологии — SD-WAN для доступа к площадкам, безопасность и подключение для «вещей» и промышленную безопасность.

Технические характеристики

SecureEdge Access Agent

ОС	Windows	macOS [1]	Android	iOS / iPadOS	Linux
Поддерживаемые версии ОС	Windows 10 Windows 11	macOS 11 (Big Sur) macOS 12 (Monterey) macOS 13 (Ventura)	Android 10 и выше	iOS/iPadOS 15 iOS/iPadOS 16	Текущие дистрибутивы Ubuntu и Fedora
Самоинициализация	✓	✓	✓	✓	✓
Обеспечение исправного состояния клиента	✓	✓	✓	✓	✓
Поддержка приложений	HTTP/HTTPS и TCP/UDP	HTTP/HTTPS и TCP/UDP	HTTP/HTTPS и TCP/UDP	HTTP/HTTPS и TCP/UDP	HTTP/HTTPS и TCP/UDP
Оптимизация на последней миле	✓	✓	✓	✓	✓
Фильтрация по URL	✓	✓	✓	✓	✓
Выборочный контроль безопасности	✓	✓	✓	✓	✓
Макс. количество одновременных устройств/пользователей	5 устройств на пользователя (на всех платформах)				

Коннектор SD-WAN

ОС	Windows	Linux
Поддерживаемые версии ОС	Windows 10 (Pro, Server, архитектура Intel) Windows 11 (Pro, Server, архитектура Intel)	Текущие дистрибутивы Ubuntu и Fedora (редакции Desktop, Server, Cloud) Generic x86_64 Linux
Самостоятельная инициализация в один клик [2]	✓	✓
Шифрование к сервису	Проприетарное (шифрование TINA)	Проприетарное (шифрование TINA)
Максимальная пропускная способность [3]	100 Мбит/с – 1 Гбит/с (в зависимости от серверного оборудования)	100 Мбит/с – 1 Гбит/с (в зависимости от серверного оборудования)
Поддерживаемая облачная платформа	Любой облачный провайдер, предлагающий услуги IaaS или контейнерные сервисы для Windows и Linux	

SecureEdge Service под управлением Barracuda

	Северная и Южная Америка	EMEA	APAC
Доступно для следующих регионов	Бразилия, Канада Центральная, Канада Восточная, центр США, восток США, запад США	Северная Европа, Западная Европа, Франция, Германия, Норвегия, Южная Африка, ОАЭ, Южная Великобритания, Западная Великобритания	Азия Восточная, Азия Юго-Восточная, Австралия Центральная, Австралия Восточная, Австралия Юго-Восточная, Индия Центральная, Индия Южная, Япония Восточная, Япония Западная, Корея

SecureEdge Service для Microsoft Azure Virtual WAN

	MICROSOFT AZURE VIRTUAL WAN SCALE UNIT							
	2	4	10	20	30	40	60	80
Доступная пропускная способность	1 Гбит/с	2 Гбит/с	5 Гбит/с	10 Гбит/с	15 Гбит/с	20 Гбит/с	30 Гбит/с	40 Гбит/с

Устройства SecureEdge для площадок

	ОБОРУДОВАНИЕ для площадок									ВИРТУАЛЬНЫЕ УСТРОЙСТВА для площадок				
	НАСТОЛЬНОЕ ИСПОЛНЕНИЕ		МОНТИРУЕМОЕ В СТОЙКЕ 1U			СОВМЕСТИМОЕ С DIN-РЕЙКОЙ								
	T100B	T200C	T400C	T600D	T900B	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
ПРОИЗВОДИТЕЛЬНОСТЬ (см. Брошюру с характеристиками для получения более подробной информации о производительности)														
Рекомендованное количество пользователей	50–100	150–300	300–1 000	1 000–4 000	6 000–9 000	н/д	н/д	50–100	150–300	50–100	150–300	300–1 000	1 000–4 000	6 000–9 000
Параллельные сессии	80 000	300 000	500 000	2 100 000	4 000 000	н/д	н/д	80 000	250 000	80 000	250 000	500 000	2 100 000	4 000 000
Новые сессии/сеансы	8 000	12 000	20 000	115 000	190 000	н/д	н/д	8 000	12 000	8 000	12 000	20 000	115 000	190 000
Возможности граничных сервисов	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓
ОБОРУДОВАНИЕ (см. Брошюру с характеристиками для получения более подробной информации про оборудование)														
Более прочная версия оборудования							✓ 4	✓ 5	✓ 5					
Лицензированные vCPU (виртуальные)										2	4	8	10	до 32
Медные сетевые карты (1 Гбит/с)	5x	12x	8x	10x	8x	4x	4x	2x	5x					
Оптоволоконные сетевые карты (SFP) (1 Гбит/с)		4x		8x	8x			1x	2x					
Оптоволоконные сетевые карты (SFP+) (10 Гбит/с)			2x	2x	4x									
Оптоволоконные сетевые карты (QSFP+) (40 Гбит/с)					2x									
Виртуальные сетевые карты										5-16x	5-16x	5-16x	5-16x	5-16x

1— SecureEdge Access Agent поддерживается на официально поддерживаемых и обслуживаемых операционных системах Apple Inc. На момент создания данного документа в него входила упомянутая выше версия ОС. Старые версии или устройства, которые определяются как «старинные» или «устаревшие» в соответствии с https://support.apple.com/en-us/HT201624 могут работать, но официально не поддерживаются с Barracuda SecureEdge Access Agent.

2— Для этого достаточно подключиться к Интернету и ввести токен, сгенерированный с помощью SecureEdge Manager.

3— В зависимости от установленного оборудования и распределения памяти; использует один поток процессора.

4— Безвентиляторные локальные устройства с расширенным диапазоном рабочих температур (от -20 до +70 °C), предназначенные для работы в жестких условиях эксплуатации.

5— Безвентиляторные локальные устройства с расширенным диапазоном рабочих температур (от -40 до +75 °C), предназначенные для работы в жестких условиях эксплуатации.

Barracuda
Your journey, secured.