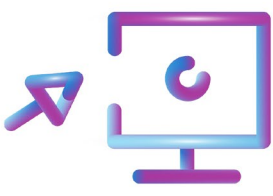
Как сэкономить на обеспечении безопасного доступа в интернет для сотрудников

Современные рабочие процессы трудно представить без использования интернета. Быстрые поиск и коммуникации, совместная и удалённая работа — всё это возможности, без которых не обойтись ни одной организации. Но у каждой медали есть две стороны, и интернет также несёт в себе угрозы для ИТ-инфраструктуры и внутренних сервисов компании, а значит, и для непрерывности бизнеса.

Как противостоять этим вызовам? Какими средствами можно обеспечить защиту? И как эффективно распорядиться бюджетом? На эти вопросы поможет ответить наш гайд.

Свободно распространяемое ПО



Первая идея, как обеспечить безопасный доступ, — это использование бесплатного софта, что представляется наименее затратным способом.

Для обеспечения контроля доступа и защиты от веб-угроз подойдут десятки решений, например, веб-прокси Squid и антивирус ClamAV. При должной настройке, они будут достаточно эффективно решать стоящие перед компанией задачи. Но кроме очевидного плюса — отсутствие платы за само ПО, — у этого варианта есть и свои минусы.

1

Свободное ПО не бесплатное

Использование open-source продуктов требует серьёзных знаний и навыков, так как официальной техподдержки и технической документации для них нет, информацию и помощь приходится искать на специализированных форумах и телеграм-каналах. Таким образом, применение свободного ПО оказывается не бесплатным — за него компании придется платить временем своего специалиста, который будет заниматься поддержкой этого ПО.

2

Сложности обслуживания свободного ПО

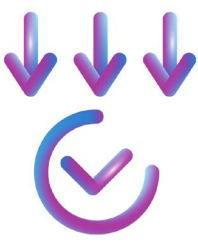
Ввод в эксплуатацию и конфигурирование таких решений — процесс, нередко требующий индивидуального подхода. В связи с этим увольнение сотрудника, который поддерживал свободное ПО, часто оборачивается для компании большой проблемой, поскольку новый сотрудник может не сразу понять, как работать с наследием своего предшественника.

3

Риски из-за свободного ПО

Нельзя забывать и об архитектурных особенностях свободного ПО. Оно способно выдержать небольшие нагрузки и справиться с основными угрозами, но станет критической точкой ИТ-инфраструктуры при развитии бизнеса в условиях роста штата сотрудников и числа целевых атак злоумышленников или конкурентов. Не говоря уже о том, что в случае неисправности свободного ПО или заражения сети никто не гарантирует устранения подобных проблем, так как не несет за это юридической ответственности.

Решения «все в одном»



Другой способ обеспечения безопасного доступа сотрудников в интернет — это покупка универсальных продуктов для сетевой безопасности (Unified Threat Management, UTM) или межсетевых экранов нового поколения (Next Generation Firewall, NGFW). Они могут не только решить проблему с веб-безопасностью, но также защитить от сетевых атак и обеспечить безопасное подключение удаленных пользователей.

UTM и NGFW на рынке уже давно, их достоинства и недостатки до мельчайших подробностей разобраны в публикациях экспертов, он и объединяют тысячи специалистов в профильные комьюнити. Даже если возникли трудности с техподдержкой, всегда можно рассчитывать на помощь сообщества. Эти продукты часто соответствуют требованиям регуляторов и крупных заказчиков, эффективны в решении поставленных задач и стоят приемлемых денег за предлагаемый набор функций. Но, как и свободно распространяемое ПО, имеют свои изъяны.

1

Снижение производительности

Вычислительной мощности устройства-комбайна может не хватить, если резко увеличивается нагрузка или усложняются правила политики безопасности, так как все механизмы защиты используют одни вычислительные мощности. Включение всех функций также может снизить производительность в 10–20 раз, а перегрузка привести к деградации скорости интернета и остановке бизнес-процессов.

2

Переплаты за счет покупки продуктов со схожим функционалом

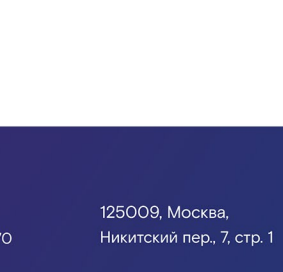
Подход «все в одном» не учитывает имеющиеся в инфраструктуре средства защиты и не предполагает, что можно приобрести только одну базовую функцию для обеспечения безопасного доступа в интернет. Из-за этого компания переплачивает за счет покупки ненужных функций или дублирования продуктов со схожим функционалом.

2022

Ситуация на рынке в 2022 году

В 2022 году на российском рынке NGFW/UTM сложилась ситуация, когда остался всего один зарубежный продукт, который можно полностью отнести к этому классу, а также три-четыре российских решения — и то, с большим количеством оговорок.

Специализированные устройства (SWG)



Для обеспечения безопасного доступа в интернет также существуют отдельные устройства — шлюзы веб-безопасности (Secure Web Gateway, SWG).

В их состав входят веб-прокси, реверс-прокси, категоризатор веб-ресурсов, потоковый антивирус, а также средства контентного анализа веб-трафика для предотвращения возможных утечек конфиденциальной информации. То есть все необходимое для эффективного управления доступом сотрудников к веб-ресурсам и защиты от потенциальных веб-угроз: зараженных, фишинговых или запрещенных сайтов.

Гибкая настройка политики фильтрации веб-трафика

Правила позволяют гибче настраивать политики фильтрации веб-трафика и доступа сотрудников в интернет. Кроме того, интерфейс и внутренняя система отчетов SWG обычно лучше и удобнее, чем у NGFW/UTM, и, конечно, на порядок превосходят соответствующие разделы свободного ПО.

Каким предприятиям не подходит SWG

Узкая специализация SWG может показаться кому-то недостатком. SWG не защищают от сетевых атак, и не могут заменить межсетевые экраны. Также они не подходят для предприятий малого бизнеса — за неимением у них специалиста, который будет администрировать и настраивать SWG.

Сравнение SWG с UTM/NGFW

Использование SWG может компенсировать основной недостаток UTM/NGFW-решений — резкое падение производительности при включении всех функций. Таким образом, эти решения дополняют друг друга: SWG обеспечивает безопасный доступ в интернет, а UTM/NGFW — защиту от сетевых атак и угроз. В результате можно добиться ощутимой экономии, так как SWG стоят существенно дешевле, чем UTM/NGFW.

Solar webProxy от «Ростелеком-Солар»

После начала СВО на российском рынке остался единственный зарубежный SWG. При этом присутствует несколько российских SWG, часть из которых может заместить иностранные решения. Одно из них — Solar webProxy от «Ростелеком-Солар», которое рассчитанное на средний и крупный бизнес. За 2022 год с его помощью были заменены зарубежные SWG в ряде крупнейших компаний России.

Преимущества Solar webProxy

- Категоризатор собственной разработки
- Встроенный антивирус
- Понятный интерфейс
- Досье на персону

Все преимущества Solar webProxy доступны в демоверсии

Скачать

Записи вебинаров по продукту Solar webProxy

Посмотреть

Если вы хотите узнать о возможностях Solar webProxy подробнее, оставьте заявку на консультацию.

Отправить заявку

Ростелеком Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70

125009, Москва,
Никитский пер., 7, стр. 1