620137, Россия, г. Екатеринбург, ул. Кулибина 2, оф. 500
тел.: +7 (495) 987-32-70
e-mail: sales@ideco.ru
ideco.ru

Обзор возможностей Ideco UTM 14

Защита от несанкционированного доступа, от внешних и внутренних угроз	
Межсетевой экран	Защищает корпоративную сеть от атак извне. Правила можно применять как для всей сети и отдельных подсетей, так и для отдельных пользователей или групп, даже если у них используются динамические IP-адреса. Предустановленные правила позволяют обеспечить высокий уровень защиты, даже без специальной настройки. Возможность использования в правилах стран по GeoIP.
Защита от атак на обслуживание DoS	Предустановленные правила по умолчанию настроены на защиту всех сетевых интерфейсов сервера от DoS-атак, MIT-атак, агрессивного, нелегитимного, неавторизованного и явно вирусного трафика, с учетом его характерных особенностей.
Система предотвращения вторжений IDS/IPS	Система обнаружения и предотвращения вторжений блокирует попытки несанкционированного доступа, эксплойты, ботнеты, DoS-атаки, вирусную активность в сети, spyware, TOR, анонимайзеры, телеметрию Windows и скомпрометированные IP-адреса (с помощью обновляемой базы IP Reputation). Ведет журналирование инцидентов информационной безопасности и оповещает о них администратора сети.
Контроль приложений	Возможность управлять доступом к различным приложениям: Skype, мессенджерам, torrent-клиентам и другим (более 250 приложений).
Межсетевой экран уровня веб-приложений	Web Application Firewall – Защита опубликованных веб-приложений от сканирования на уязвимости, SQLi, XSS, DoS и других атак с помощью анализа запросов к сайту.
Защита от подбора паролей к сервисам brute force	Специальная служба блокирует brute force атаки (попытки подбора паролей и многократные подключения к сервисам) на сервисы SSH, SMTP, IMAP, POP3, веб-почту, VPN-сервер и доступ в административный веб-интерфейс UTM.
Интеграция с внешними решениями	Возможность интеграции по протоколу ICAP со сторонними DLP-системами, антивирусами и решениями для контентной фильтрации. Интеграция с SIEM (по протоколу syslog), с системами мониторинга (SNMP, Zabbix-агент).

Контроль доступа	
Active Directory / LDAP	Возможность синхронизации и авторизации пользователей через Active Directory и LDAP сервер. Поддержка интеграции с несколькими доменами Active Directory. Авторизация по логам безопасности домена и протоколу Kerberos.
Авторизация пользователей Identity-Based Control	Авторизация по логину и паролю через VPN, PPPoE или через Ideco Agent, авторизация по IP-адресу и/или по MAC-адресу, через веб-браузер, прозрачная Single Sign-On аутентификация по безопасному протоколу Kerberos через Active Directory. Доступ к Интернету неавторизованных устройств блокируется сервером.
Отчеты	Модуль формирования отчетов для руководителей и IT-менеджеров, позволяющий визуально оценивать степень использования Интернет-ресурсов сотрудниками и подразделениями компании. Отчетность по пользователям и категориям сайтов в графическом виде. Гибкая настройка отчетов на основе виджетов, регулярные автоматические рассылки на выбранные Email'ы
Двухфакторная аутентификация	Позволяет авторизовать пользователей, использующих VPN-подключение через сервис Sms Aero, повышает общую безопасность.

Удаленные подключения (VPN-сервер)	
Удаленные офисы и филиалы \ протоколы	Возможность объединить все удаленные подразделения в общую сеть на единой платформе. Поддерживаются протоколы: IKEv2 IPSec, L2TP/IPSec с максимально криптостойкими

620137, Россия, г. Екатеринбург, ул. Кулибина 2, оф. 500
тел.: +7 (495) 987-32-70
e-mail: sales@ideco.ru
ideco.ru

Удаленные подключения (VPN-сервер)	
site-to-site VPN	алгоритмами шифрования.
Мобильные сотрудники \ протоколы client-to-site VPN	До 1000 одновременных сессий. Wireguard (VPN-агент под Windows), IKEv2 IPSec, L2TP/IPSec, SSTP, PPTP. С возможностью отдавать маршруты по всем протоколам кроме VPN-агента.

Контентная фильтрация	
Расширенный контент-фильтр	146 категорий, более 500 млн url в обновляемой базе данных. Используются базы российского производителя баз фильтрации с высокой степенью релевантности для русскоязычного интернет-сегмента.
Декодирование и проверка HTTPS-трафика	Все службы: контентная фильтрация, антивирусы, веб-отчетность — поддерживают проверку шифрованного HTTPS-трафика (методом ssl bump либо без подмены сертификата с помощью SNI и анализа данных сертификата).
Блокировка файлов по MIME-типу и расширению	Контент-фильтр позволяет блокировать трафик по типу (MIME-type) и расширению файлов.

Антивирусная проверка трафика	
Применяемые технологии	Антивирусная проверка почтового и веб-трафика с помощью технологий «Лаборатории Касперского» (платный доп. модуль) и антивируса ClamAV.
Проверка web-трафика	Позволяет блокировать зараженные файлы, эксплойты, вредоносные скрипты, не допуская их проникновения в локальную сеть.
Проверка почтового трафика	Позволяет выполнять антивирусную проверку всех почтовых сообщений. Поддерживается проверка архивных файлов и многократно упакованных объектов.

Антиспам	
Антиспам Касперского (платный доп. модуль)	Обеспечивает высокий уровень детектирования спама при низких значениях ложных срабатываний (0,003-0,005% от общего количества сообщений). Для защиты пользователей используется большой набор технологий распознавания спама с использованием внешних облачных сервисов (DNSBL, SPF и SURBL) и собственных алгоритмов: сигнатурный анализ текста и графики, лингвистический эвристик, использование UDS-запросов в режиме реального времени. В зависимости от настроек спам-сообщения могут автоматически удаляться, перемещаться в спам-контейнер или доставляться конечному пользователю с пометкой spam. Также проверяются все ссылки в почтовых сообщениях, письма со ссылками на фишинговые ресурсы блокируются.
Серые списки greylisting	Поведенческий способ автоматического блокирования спама. Преднастроенная служба позволяет блокировать спам без получения текста письма, снижая нагрузку на сервер.
DNSBL	Фильтрация спама с помощью сервисов DNS blacklist.
Предварительный спам-фильтр и защита от DoS	Предварительный спам-фильтр защищает почтовый сервер от подключений ботов, спама и DoS-атак. Проверяет соответствие SPF-записи и корректность DKIM-подписи сервера.

620137, Россия, г. Екатеринбург, ул. Кулибина 2, оф. 500
тел.: +7 (495) 987-32-70
e-mail: sales@ideco.ru
ideco.ru

Управление трафиком	
Маршрутизация трафика	Поддержка множества интерфейсов (как локальных, так и внешних). Поддерживаются виртуальные 802.1q VLAN интерфейсы, PPTP, L2TP, PPPoE интерфейсы. Возможность указать маршруты по источнику. Динамическая маршрутизация OSPF.
Подключение к провайдерам, резервирование и балансировка каналов	Поддержка нескольких каналов провайдеров и нескольких внешних сетей; Перенаправление трафика в разные подсети; Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров; Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера, в случае необходимости. Подключение к провайдеру по протоколам PPTP (VPN), L2TP и PPPoE. Балансировка трафика между каналами. Агрегирование каналов (LACP).
Управление полосой пропускания	Интернет-канала для пользователей и групп.
Кэширование трафика и DNS-запросов	Встроенный прокси-сервер кэширует трафик популярных ресурсов для ускорения доступа к ним. DNS-сервер кэширует DNS-запросы, что также позволяет ускорить доступ к Интернет-ресурсам.
Публикация ресурсов Reverse Proxy, DNAT, SMTP relay	Возможна публикация веб-ресурсов с помощью обратного прокси (Reverse Proxy) с защитой веб-серверов от различных типов атак. Поддерживается публикация Outlook Web Access через обратный прокси-сервер. Применимы правила WAF и перенаправления с http на https Также возможна публикация ресурсов с помощью переадресации портов (DNAT). Публикация почтового сервера с помощью почтового релея позволяет использовать все возможности фильтрации почтового трафика на Ideco UTM и защитить внутренний почтовый сервер от различного вида атак, вирусов и спама.

Почтовый сервер	
Поддержка протоколов	Поддержка протоколов IMAP, POP3, SMTP. Шифрованных протоколов POP3S, IMAPS, STARTTLS - все они используются только с максимально криптостойкими алгоритмами шифрования, исключая возможность атаки человек-по-середине.
Веб-интерфейс	Веб-интерфейс почтового сервера доступен на внешних и внутренних сетевых интерфейсах UTM и обеспечивает удаленный доступ пользователей к почте по защищенному протоколу HTTPS. В пользовательском интерфейсе также присутствует общая и пользовательская адресные книги, и календари событий и задач.
Антиспам проверка почтового трафика	Письма проверяются на спам антиспамом Касперского (опционально) и с помощью технологии серых списков.
Защита внутренних серверов электронной почты	Все возможности фильтрации почты также доступны для внутренних почтовых серверов, при использовании почтового сервера UTM в качестве почтового релея.

Развертывание и управление	
Отказоустойчивая конфигурация	Кластер отказоустойчивости (Master-Slave).
WEB-интерфейс	Полное управление сервером и конфигурирование через WEB-браузер.

620137, Россия, г. Екатеринбург, ул. Кулибина 2, оф. 500
тел.: +7 (495) 987-32-70
e-mail: sales@ideco.ru
ideco.ru

Развертывание и управление	
Консольный интерфейс	Возможно удаленное подключение к серверу по SSH и выполнение консольных команд.
Active Directory / LDAP	Интеграция с каталогами пользователей и ресурсов компании.
Центральная консоль	Позволяет централизовано управлять вашими серверами Ideco UTM

Жизненный цикл программного обеспечения	
Приобретение и поставка программного обеспечения	Неисключительное право на использование программного продукта Ideco UTM приобретаются у правообладателя - ООО "Айдеко" и включают в себя доступ к обновлениям ПО и технической поддержке сроком на 1 год.
Срок действия лицензии на ПО	Лицензия на неисключительные права доступа действует бессрочно с даты покупки.
Подписка на обновления и техническую поддержку (Security Update)	Security Update включает в себя: - Получение новых версий продукта (обновлений Ideco UTM). - Расширенный контент-фильтр (обновления модуля и возможность его работы). - Систему предотвращения вторжений (обновления модуля и возможность его работы). - Контроль приложений (обновления модуля и возможность его работы). - Техническую поддержку. Модули системы предотвращения вторжений, контент-фильтр, контроль приложений - работают только при активной подписке. Стандартная покупка Security Update. Стоимость покупки модуля составляет 45% от текущих прайсовых цен на продукт без учета модулей Лаборатории Касперского. Ежегодная стоимость модулей антивируса и антиспама Касперского фиксированная. Вы можете приобрести Security Update на этих условиях в течение двух месяцев с момента завершения срока активности обновлений и технической поддержки. Срок активности Security Update продлевается ровно на один год с момента завершения предыдущего периода. Поздняя покупка Security Update. Независимо от даты окончания активности Security Update (если прошло больше двух месяцев) вы можете приобрести его за 75% базовой цены вашей редакции. Ежегодная стоимость модулей антивируса и антиспама Касперского фиксированная. Срок активности Security Update продлевается с момента оплаты ровно на один год. Вы получаете возможность загрузить и установить все изменения и обновления, которые вышли за весь предыдущий период, пока вы не пользовались обновлениями и еще в течение полного года с момента покупки пользоваться поддержкой, обновлениями продукта и UTM-модулями.
Прямая техническая поддержка от вендора	Техническая поддержка ПО, включающая помощь пользователям в настройки и эксплуатации системы, а также устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, осуществляется службой технической поддержки ООО "Айдеко". Поддержка осуществляется в соответствии с утвержденным регламентом. Экспликация обращений происходит до уровня разработчиков ПО. Поддержка доступна в тикетной системе обращений и по телефону, с 7 до 19 часов по Московскому времени в рабочие дни и с 9 до 16 по субботам.
Документация	Руководство администратора сервера Ideco UTM.

620137, Россия, г. Екатеринбург, ул. Кулибина 2, оф. 500
тел.: +7 (495) 987-32-70
e-mail: sales@ideco.ru
ideco.ru

О компании «Айдеко»

Наша компания за годы работы на рынке приобрела профессиональную репутацию в области разработки программного обеспечения для локальных сетей и защиты информации, что позволяет на равных соперничать с ведущими иностранными производителями программного обеспечения.

Пользователями Ideco UTM являются более 10 000 коммерческих компаний и государственных учреждений России и стран СНГ, в том числе Федеральная таможенная служба Российской Федерации, Министерство юстиции Российской Федерации, Федеральная служба по военно-техническому сотрудничеству России, Федеральная служба по надзору в сфере транспорта (Ространснадзор), Федеральное агентство лесного хозяйства России (Рослесхоз), Федеральное агентство по недропользованию (Роснедра) и другие.

Ideco UTM входит в единый реестр российских программ для электронных вычислительных машин и баз данных.

Наше решение разрабатывается в России и использует отечественные базы контентной фильтрации, антивирусов, системы предотвращения вторжений.

Сервера обновлений продукта и сигнатур расположены на территории Российской Федерации и не подвержены геополитическим и санкционным рискам.

Простота настройки нашего продукта обеспечивает высокую безопасность сети (уже при настройках «по умолчанию»), быстрое внедрение и низкую стоимость владения.

security.ideco.ru - сервис проверки:

- фильтрации трафика;
- возможности проникновения тестовых вирусов и эксплойтов в сеть;
- ответов портов и сервисов на внешнем сетевом интерфейсе;
- нахождение IP-адреса в черных списках спам-листов;
- наличие пароля почты в известных базах хакеров.