ОБЗОР ВОЗМОЖНОСТЕЙ IDECO UTM 17 ФСТЭК

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ	
Сертификация ФСТЭК: Межсетевой экран, Система обнаружения вторжений	Номер сертификата 4503, срок действия 28.12.2026. Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ).
Импортозамещение	44-ФЗ. Запись в реестре №329 от 08.04.2016 в едином реестре российских программ для электронных вычислительных машин и баз данных.
Тип и класс ИС (для защиты которых подходит)	ГИС: до 1 К3 (включительно), ИСПДн: до 1 У3 (включительно), АСУ: до К1 (включительно), Значимые объекты КИИ: до 1 класса (включительно), ИС ОП: II класс.
Законы, регламентирующие применение	187-ФЗ «О безопасности КИИ РФ», 152-ФЗ «О персональных данных», 139-ФЗ и 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

ИНТЕГРАЦИЯ В ИС	
На периметре сети	Тип МЭ А (сертифицированный ПАК).
Между сегментами локальной сети	Тип МЭ Б (ПО) Возможно использование собственного железа или виртуальной машины.
Прокси-сервер	Тип МЭ Б (ПО) Возможно использование собственного железа или виртуальной машины.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ	
Межсетевой экран	Zone Based Firewall (зоны в правилах файрвола, включая IPSec и клиентские VPN-подключения); Защищает корпоративную сеть от атак извне. Правила можно применять как для всей сети и отдельных подсетей, так и для отдельных пользователей или групп. Возможность использования в правилах страны (GeoIP).
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), список блокировки НКЦКИ. Ведет журналирование инцидентов информационной безопасности.
Расширенная база правил предотвращения вторжений от Лаборатории Касперского (платный доп. модуль)	Сигнатуры системы предотвращения вторжений от "Лаборатории Касперского". Эти сигнатуры создаются и обновляются большой командой аналитиков, с использованием данных Kaspersky Security Network (KSN). Для подготовки правил на ВПО во внутренних системах автообработки с помощью ML производится поиск подозрительного трафика, затем его анализируют эксперты и вручную составляют правила. Подозрительные сетевые взаимодействия отслеживаются на всем потоке ВПО, поступающего в ЛК (~400К вредоносных файлов в день); Содержат правила на выявление попыток эксплуатации сетевых уязвимостей (CVE) составляются по результатам регулярного мониторинга публикаций с аналитикой,

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ	
	GitHub репозиториев, Telegram каналов, Twitter и пр.; База содержит более 4600 правил
Контроль приложений	Возможность управлять доступом к различным популярным приложениям: Skype, мессенджерам, torrent-клиентам, программам удаленного доступа и другим (более 400 приложений).
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 сетевыми песочницами. Интеграция с SIEM (по протоколу syslog, в т.ч. в формате CEF), 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 пользователей доверенных доменов Active Directory.
ALD Pro	Возможность интеграции, синхронизации и авторизации пользователей с ALD Pro.
BaseALT и Samba DC	Возможность интеграции, синхронизации и авторизации пользователей с BaseALT и Samba DC
Авторизация пользователей Identity-Based Control	Авторизация по логину и паролю через VPN, PPPoE, авторизация по IP-адресу и по MAC-адресу, через веб-браузер, прозрачная Single Sign-On аутентификация по Kerberos/NTLM, по логам безопасности контроллеров домена через Active Directory, авторизация пользователей WiFi через авторизацию по подсети. Возможность включения автосоздания пользователей при их выходе в интернет. Возможность авторизации пользователей терминальных серверов на прокси-сервере. Авторизация VPN-пользователей с помощью RADIUS и др. способами.
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.
Аудит действий администраторов	Ideco UTM логирует действия администраторов, которые вносят изменения в конфигурацию UTM из веб-интерфейса, локального интерфейса и терминала.
Двухфакторная аутентификация	Позволяет авторизовать пользователей, использующих VPN-подключение с сервиса SMS Aero или интеграции с Мультифактор.

УДАЛЕННЫЕ ПОДКЛЮЧЕНИЯ (VPN-СЕРВЕР)	
Удаленные офисы и филиалы \ протоколы site-to-site VPN	Возможность объединить все удаленные подразделения в общую сеть на единой платформе. Возможность создания маршрутов для IPSec-подключений. Возможность настройки BGP соседства в IPSec-подключениях; Используется протокол IKEv2 IPSec с максимально криптостойкими алгоритмами шифрования.
Мобильные	Поддержка split tunneling. Возможность использовать различные протоколы: IKEv2

УДАЛЕННЫЕ ПОДКЛЮЧЕНИЯ (VPN-СЕРВЕР)	
сотрудники \ протоколы client-to-site VPN	IPSec, L2TP/IPSec, SSTP, PPTP. Поддерживается возможность создания профилей для подключения определенных пользователей и групп.

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. Гибкие способы блокировки: возможность заблокировать только загрузку файлов на файлообменники или ограничить активность в социальных сетях.
Расшифровка и проверка HTTPS-трафика	Все службы: контентная фильтрация, антивирусы, веб-отчетность — поддерживают проверку шифрованного HTTPS-трафика (методом MITM (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.
Перенаправление трафика	С включенной расшифровкой HTTPS трафика можно настроить перенаправление запросов к определенному ресурсу или категории на необходимый URL адрес.

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 и BGP.
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	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).Есть возможность настроить балансировку трафика на несколько серверов обратным прокси-сервером. Поддерживается публикация Outlook Web Access через обратный прокси-сервер. Также возможна публикация ресурсов с помощью переадресации портов (DNAT).
IGMP Proxy	Позволяет принимать мультикаст-трафик от провайдера.
WCCP	Используется для перенаправления веб-трафика на прокси-сервера. Работает на

УПРАВЛЕНИЕ ТРАФИКОМ	
	уровне L2/GRE.

РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ	
Роли администраторов	Администратор, Только просмотр, Просмотр отчётов, Создание отчётов.
Отказоустойчивая конфигурация	Кластер отказоустойчивости с синхронизацией сессий (Active-Passive).
Веб-интерфейс	Полное управление сервером и конфигурирование через веб-браузер.
Консольный интерфейс	Возможно удаленное подключение к серверу по SSH и выполнение консольных команд.
Центральная консоль	Позволяет централизовано управлять вашими серверами Ideco NGFW. Входит в состав лицензии.
Резервное копирование	Возможность резервного копирования конфигурации Ideo UTM в ручном и автоматическом режиме по расписанию, а также отправки копий на FTP и общую папку CIFS.

ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	
Приобретение и поставка программного обеспечения	Неисключительное право на использование программного продукта Ideco UTM приобретаются у правообладателя – ООО "Айдеко Софтвер" 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. Стоимость приобретения модуля Security Update составляет 45% от текущих цен на продукт без учета модуля Лаборатории Касперского. 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. Позднее приобретение Security Update: если прошло больше двух месяцев после окончания подписки модуля Security Update вы можете приобрести его за 75% текущих цен на продукт без учета модуля Лаборатории Касперского. 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.

ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	
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 Софтвер". Поддержка осуществляется в соответствии с утвержденным регламентом. Поддержка доступна в тикетной системе обращений, по телефону, в встроенном в веб-интерфейс чате, в Telegram, с 04:00 до 21:00 по Московскому времени в рабочие дни и с 9:00 до 16:00 по субботам.
Документация	Руководство администратора сервера Ideco UTM на русском языке.