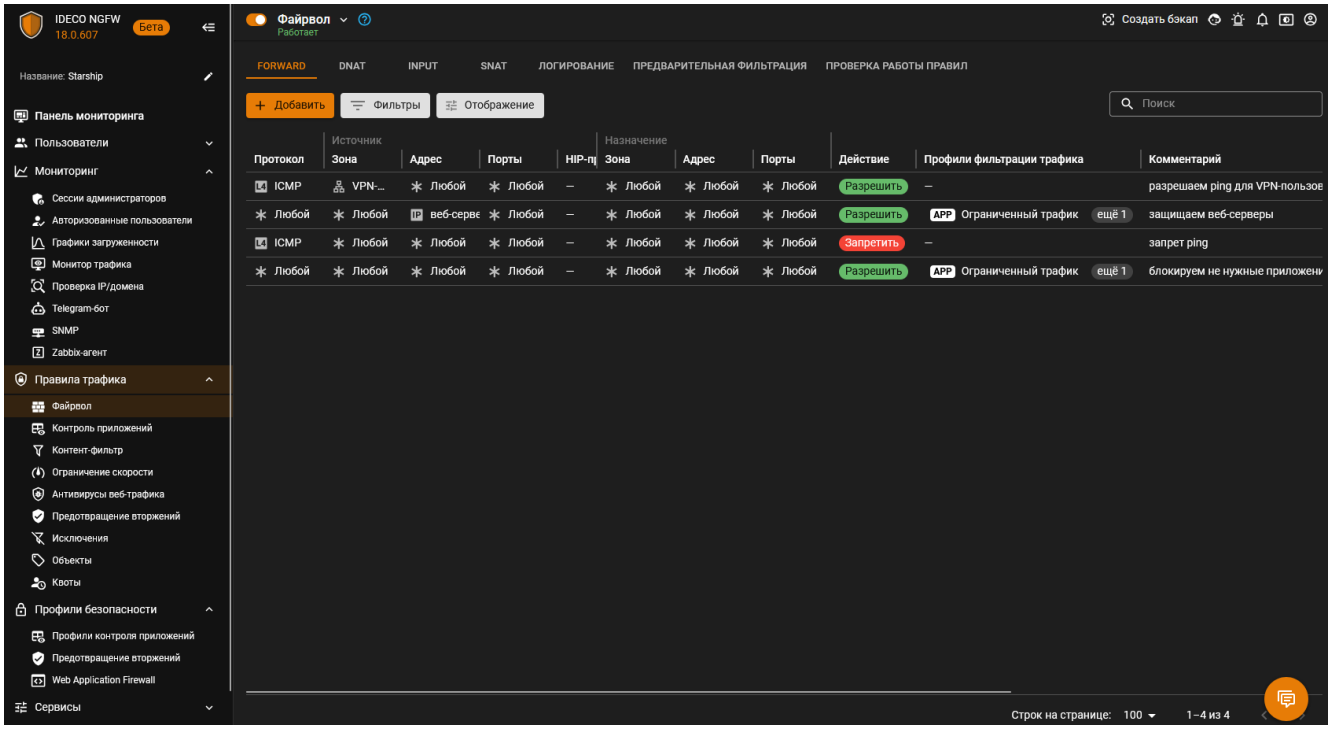
ОБЗОР ВОЗМОЖНОСТЕЙ IDECO NGFW 18



СИСТЕМНЫЕ ТРЕБОВАНИЯ К ПО	
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, включая отечественные аналоги гипервизоров.
Процессор	Intel i3/i5/i7/i9/Xeon с поддержкой SSE 4.2. Минимум 2 ядра.
Оперативная память	16 ГБ (16-64 ГБ в зависимости от количества пользователей).
Дисковая подсистема	SSD, объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe. Дополнительный SSD при использовании почтового сервера.
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel. Поддерживаются Realtek, D-Link и другие.
Дополнительно	Обязательна поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ	
Межсетевой экран	Zone Based Firewall (зоны в правилах файрвола, включая IPSec и клиентские VPN-подключения); Правила можно применять как для всей сети и отдельных подсетей, так и для отдельных пользователей или групп. Возможность использования в правилах страны (GeoIP). Профили приложений Layer7 («Контроль приложений») и IPS в правилах файрвола. Предварительная фильтрация трафика с возможностью проверки TCP-флагов и размера пакетов для защиты от DoS-атак.
Межсетевой экран уровня веб-	Web Application Firewall – Защита опубликованных веб-приложений от сканирования на уязвимости, SQLi, XSS, DoS и других атак с помощью анализа

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ	
приложений	запросов к сайту. Профили безопасности WAF: включая группы сигнатур WAF, исключения, ограничения по источнику подключений (включая GeoIP и сети). Защита опубликованных веб-сервисов от DoS-атак.
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 всём 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, GitHub репозиториев, Telegram каналов, Twitter и пр.; База содержит более 4600 правил.
Контроль приложений	Возможность управлять доступом к различным популярным приложениям: мессенджерам, играм, криптомайнерам, файлообменникам, программам удаленного доступа и другим (более 417 приложений в 28 группах).
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 NGFW.
Интеграция с внешними решениями	Возможность интеграции по протоколу ICAP со сторонними DLP-системами, антивирусами и сетевыми песочницами. Интеграция с SIEM (по протоколу syslog, с возможностью отправки 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, 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 через авторизацию по подсети (для Wi-Fi и др.). Возможность включения автосоздания пользователей при их выходе в интернет. Возможность авторизации пользователей терминальных серверов на прокси-сервере. Доступ к Интернету неавторизованных устройств блокируется сервером.
Ideco Client	Собственный клиент для подключения по VPN и авторизации пользователей Ideco

КОНТРОЛЬ ДОСТУПА	
	Client поддерживающий различные профили и прозрачную Single Sign-On аутентификацию. Клиент поддерживается для Windows 10, 11, MacOS и всех версий Linux, включая отечественные.
Концепция ZTNA	Возможна проверка клиентом домена, антивируса, версии ОС, наличия пакетов обновлений и др. Использование профилей устройств в политиках файрвола.
Отчеты	Отчётность по пользователям, категориям сайтов и по трафику приложений в графическом виде. Дашборды и отчётность по событиям безопасности (IPS, WAF, антивирус). Гибкая настройка отчётов на основе виджетов, регулярные автоматические рассылки на выбранные Email'ы.
Авторизация администраторов	Локальная база данных администраторов, авторизация через RADIUS, Microsoft Active Directory и ALD Pro.
Аудит действий администраторов	Ideco NGFW логирует действия администраторов, которые вносят изменения в конфигурацию NGFW из веб-интерфейса, локального интерфейса и терминала.
Двухфакторная аутентификация	Позволяет авторизовать пользователей, использующих VPN-подключение с помощью TOTP-токена, сервиса SMS Aero или интеграции с Мультифактор.
Интеграция с RADIUS-сервером	Позволяет аутентифицировать пользователей, данные о которых хранятся только на RADIUS-сервере или в базах/каталогах, к которым имеет доступ RADIUS-сервер.
Время окончания действий правил	Возможность создания правил с определенным временем действия, например, для предоставления доступа до определенных ресурсов при подключении по VPN.
Личный кабинет пользователя	Возможность управления доступом группам пользователей в личный кабинет для скачивания Ideco Client, смены пароля, конфигурации двухфакторной аутентификации.

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.
GRE \GRE over IPsec	Возможность создания GRE туннеля для объединения удаленных подразделений в общую сеть. Возможно создать подключение как без шифрования, так и зашифрованного канала связи между устройствами с использованием IPsec.
Мобильные сотрудники\ протоколы client-to-site VPN	Поддержка split tunneling. Возможность использовать различные протоколы: IKEv2 IPSec, L2TP/IPsec, SSTP, PPTP. Собственный клиент для подключения по VPN и авторизации пользователей Ideco Client работающий на WireGuard. Поддерживается возможность создания профилей для подключения определенных пользователей и групп. Поддерживается возможность выдавать IP-адреса из разных подсетей разным группам VPN-пользователей. Передача DNS-суффикса подключения.

КОНТЕНТНАЯ ФИЛЬТРАЦИЯ	
Расширенный контент-фильтр	146 категорий, более 500 млн url в обновляемой базе данных. Используются базы российского производителя баз фильтрации с высокой

КОНТЕНТНАЯ ФИЛЬТРАЦИЯ	
	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, более 600 типов), расширению файлов, HTTP-методу.
Морфологический анализ	Блокировка веб-страниц по словарям с заданным весом «плохих» слов.
Перенаправление трафика	С включенной расшифровкой HTTPS трафика можно настроить перенаправление запросов к определенному ресурсу или категории на необходимый URL адрес.
Безопасный поиск	Принудительное включение безопасного поиска в поисковых системах с помощью изменения URL или перенаправления DNS-запросов.
QUIC и HTTP/3	Возможность блокировки протоколов для предотвращения обхода фильтрации.

Антивирусная проверка трафика	
Применяемые технологии	Антивирусная проверка почтового и веб-трафика с помощью технологий «Лаборатории Касперского» (платный доп.модуль) и антивируса Dr.Web.
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. Проверка почты на вирусы, спам и фишинг с помощью технологий Лаборатории Касперского.
Журнал работы веб-антивируса	Возможность просматривать события срабатывания веб-антивируса.

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.

Антиспам	
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.

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. Loopback-интерфейсы.
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). Зеркалирование портов SPAN.
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) с защитой веб-серверов от различных типов атак. Есть возможность настроить балансировку трафика на несколько серверов обратным прокси-сервером. 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 NGFW и защитить внутренний почтовый сервер от различного вида атак, вирусов и спама.
IGMP Proxy	Позволяет принимать мультикаст-трафик от провайдера.
WCCP	Используется для перенаправления веб-трафика на прокси-сервера. Работает на уровне L2/GRE.
Проверка прохождения трафика	Инструмент в веб-интерфейсе позволяет проверить возможность доступа с IP на IP с настроенной политикой правил файрвола.

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 (MITM).

ПОЧТОВЫЙ СЕРВЕР	
Веб-интерфейс	Веб-интерфейс почтового сервера доступен на внешних и внутренних сетевых интерфейсах Ideco NGFW 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 и антивирусная проверка почтового трафика	Веб-интерфейс почтового сервера обеспечивает безопасный удаленный доступ пользователей к почте.
Антиспам	Фильтрация спама с помощью сервисов DNS blacklist. Предварительный спам-фильтр защищает почтовый сервер от подключений ботов, спама и DoS-атак. Проверяет соответствие SPF-записи и корректность DKIM-подписи сервера.
Защита внутренних серверов электронной почты	Все возможности фильтрации почты также доступны для внутренних почтовых серверов, при использовании почтового сервера NGFW в качестве почтового релея.

РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ	
Роли администраторов	Администратор, Только просмотр, Администратор информационной безопасности, Администратор файрвола, Администратор настройки доступов, Просмотр отчётов, Создание отчётов.
Авторизация администраторов	Через локальную базу NGFW, Microsoft Active Directory, ALD Pro, RADIUS.
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.
Резервное копирование	Возможность резервного копирования конфигурации Ideco NGFW в ручном и автоматическом режиме по расписанию, а также отправки копий на FTP и общую папку CIFS. Возможность восстановления бекапа конфигурации без перезагрузки сервера.
Центральная консоль	Позволяет централизовано управлять вашими серверами Ideco NGFW. Входит в состав лицензии.
Виртуальные контексты VCE (аналог VSX, VDOM)	Virtual Context Engine позволяет виртуализировать несколько Ideco NGFW внутри одной физической инсталляции, предоставляя клиентам возможность создавать и управлять различными сегментами с независимыми друг от друга сетью, управлением и политиками, с высоким уровнем безопасности.

ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	
Приобретение и поставка программного обеспечения	Неисключительное право на использование программного продукта Ideco NGFW приобретаются у правообладателя – ООО "Айдеко" и включают в себя доступ к обновлениям ПО и технической поддержке сроком на 1 год.

ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	
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 NGFW). - 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 модулей Лаборатории Касперского. 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. 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 модулей Лаборатории Касперского. 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 NGFW-модулями.
Прямая техническая поддержка от вендора	Техническая поддержка ПО, включающая помощь пользователям в настройке и эксплуатации системы, а также устранении неисправностей, выявленных в ходе эксплуатации программного обеспечения, осуществляется службой технической поддержки ООО "Айдеко". Поддержка осуществляется в соответствии с утвержденным регламентом. Поддержка доступна в тикетной системе обращений, по телефону, во 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 NGFW на русском языке.

ROADMAP 2024	
Декабрь 2024	Ideco NGFW 19. Отчетность со всех нод в Центральной Консоли. Active-Active балансировка VPN-соединений. SSL VPN-портал. Отправка статистики по NetFlow. Выбор логов и серверов для отправки в SIEM. Ввод кода MFA в интерфейсе Ideco Client.