ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Шлюз безопасности Ideco ICS — многофункциональное программное и программно-аппаратное UTM-решение для организации защищенного доступа в Интернет в корпоративных и ведомственных сетях.

Компания «Айдеко» - образована в 2005-ом году и является российским производителем программных продуктов для построения сетей и развития сетевых инфраструктур любого уровня сложности.

Наша компания за годы работы на рынке приобрела профессиональную экспертизу в области разработки программного обеспечения для локальных сетей и защиты информации, что позволило на равных соперничать с ведущими иностранными производителями программного обеспечения. Среди успешных примеров импортозамещения замена таких иностранных продуктов как eSafe Web Security Gateway, Microsoft TMG, Kerio Control, Checkpoint UTM и других.

Вы можете обратиться к одному из наших менеджеров и узнать дополнительную информацию по программе импортозамещения и миграции с продуктов других производителей по телефону **8 800 555 3340**.

Документация: руководство администратора.

Регламент работы службы технической поддержки.

Скачать дистрибутив можно по ссылке.

ОБЗОР ВОЗМОЖНОСТЕЙ

Защита от несанкционированного доступа и внешних угроз	
Межсетевой экран Firewall	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.
Защита от атак на обслуживание DoS-атак	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 Application Control	Возможность управлять доступом к сети приложений: Skype, другие мессенджеры, torrent-клиенты и десятки других.
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 brootforce	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 ICS.
Интеграция с внешними решениями	Возможность интеграции по протоколу ICAP со сторонними DLP-системами, антивирусами и решениями для контентной фильтрации.

Контроль доступа	
Active Directory / LDAP	Возможность синхронизации и авторизации пользователей через Active Directory и LDAP сервер.
Авторизация пользователей Identity-Based Control	Авторизация по логину и паролю через VPN, PPPoE или через Ideco Agent, авторизация по IP-адресу и 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.

Удаленные подключения (VPN-сервер)	
Удаленные офисы и филиалы / протоколы **site-to-site VPN**	Возможность объединить все удаленные подразделения в общую сеть на единой платформе. Поддерживаются протоколы: PPTP, OpenVPN, IKEv2 IPsec, L2TP/IPsec с максимально криптостойкими алгоритмами шифрования.
Мобильные сотрудники / протоколы **client-to-site VPN**	До 1000 одновременных сессий. PPTP, L2TP/IPsec (с использованием криптостойкого алгоритма AES-256).

Контентная фильтрация	
Стандартный фильтр URL-фильтрация	34 категории сайтов, включающие более 900 тысяч url.
Расширенный фильтр Ideco Cloud WebFilter	143 категории, более 500 млн url в облачной базе данных, обновляемые в режиме реального времени.
Декодирование и проверка HTTPS-трафика Encrypted Data Control	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» и антивируса ClamAV. Возможна последовательная проверка трафика двумя антивирусами.
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	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.

Управление трафиком	
Управление полосой пропускания	Контроль полосы пропускания и приоритезация трафика. Приоритезация трафика по скорости и типу, резервирование полосы пропускания для важного типа трафика, возможность установки приоритетов. Управление шириной канала для пользователей и групп.
Маршрутизация трафика	Поддержка множества интерфейсов (как локальных, так и внешних). Поддерживаются виртуальные 802.1q VLAN интерфейсы, PPTP, L2TP, PPPoE и OpenVPN интерфейсы. Возможно указание маршрута по источнику.
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.
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. 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 ICS и защитить внутренний почтовый сервер от различного вида атак, вирусов и спама.

Почтовый сервер	
Поддержка протоколов	Поддержка протоколов IMAP, POP3, SMTP. Все они используются только с максимально криптостойкими алгоритмами шифрования (STARTTLS), исключая возможность атаки человек-по-середине.
Веб-интерфейс	Веб-интерфейс почтового сервера доступен на внешних и внутренних сетевых интерфейсах ICS 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.
Антивирусная и антиспам проверка почтового трафика	Антивирусная проверка почтового трафика осуществляется антивирусами Касперского и ClamAV (возможна их совместная работа). Письма также проверяются на спам антиспамом Касперского и с помощью технологии серых списков.

Дополнительные сервисы	
Сервер точного времени	Централизованная синхронизация времени для локальных компьютеров и устройств.
DNS-сервер	Кэширующий DNS сервер для локальной сети, с возможностью поддержки внешних DNS-зон для неограниченного числа доменов. Также возможен перехват сервером запросов к внешним DNS-серверам для предотвращения попыток обхода DNS-фильтрации и фишинга.
DHCP-сервер	DHCP-сервер в составе ICS обеспечивает автоматизированную настройку сети на клиентских устройствах.

Развертывание и управление	
WEB-интерфейс	Полное управление сервером и конфигурирование через WEB-браузер (поддерживаются браузеры Google Chrome, Mozilla Firefox, Microsoft Internet Explorer 11).
Консольный интерфейс	Возможно удаленное подключение к серверу по SSH и выполнение консольных команд (в том числе доступ под root).
Active Directory / LDAP	Интеграция с каталогами пользователей и ресурсов компании.
Система отчетов	Настраиваемые детальные отчеты для Администратора и Руководителя по использованию интернет-трафика сотрудниками и сервисами.

Технические требования	
Поддержка процессоров	X86_64
Минимальное количество оперативной памяти	4 Гб
Поддержка гипервизоров	VMware ESX, Microsoft HyperV, VirtualBox, KVM, Citrix XenServer
Требования к программному обеспечению	Шлюз безопасности Ideco ICS устанавливается и работает на CBT, не требуя наличия операционной системы или другого ПО. Управление и настройка сервером осуществляется через веб-браузер (поддерживаются браузеры Google Chrome, Mozilla Firefox, Microsoft Internet Explorer 11).
Требования к среде работы	Шлюз безопасности Ideco ICS предназначен для работы в TCP/IPv4 сетях ЭВМ.
Требования к персоналу	Для конфигурирования, управления шлюзом безопасности Ideco ICS и осуществления его технической поддержки не требуются специальные знания и навыки, помимо базовых знаний сетевых технологий.

Жизненный цикл программного обеспечения	
Приобретение и поставка программного обеспечения	Права на неисключительное право использования программного продукта Ideco ICS 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 5 лет с даты покупки.
Подписка на обновления и техническую поддержку	Подписка на обновления техническую поддержку включает: получение новых версий продукта, а также обновляемых баз данных: контентного фильтра, сигнатур антивирусов, антиспама и системы предотвращения вторжений. Также пользователи с продленной подпиской получают доступ к технической поддержке. Подписка на обновления и техническую поддержку действует 1 год с момента покупки лицензии. После этого срока возможно продление подписки на коммерческой основе.
Техническая поддержка	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**.
Документация	**Руководство администратора** сервера Ideco ICS. По ссылке доступна документация в формате adobe pdf.