Общие требования к оборудованию и поставщику оборудования.

Все поставляемое оборудование должно быть новым, не восстановленным и не бывшим в употреблении, а также не имеющем объявления о снятии с продаж и поддержки или не снятым с производства, и должно иметь возможность обеспечиваться запасными модулями и элементами в течение минимум 3 лет с момента ввода в эксплуатацию при наличии действующей гарантийной поддержки.

Поставщик должен обладать статусом сертифицированного партнера;

Основным видом деятельности Поставщика должно являться предоставление услуг в сфере телекоммуникаций и/или строительства дата-центров;

Поставщик должен иметь разрешения на продажу товара на территории Республики Узбекистан (требуется официальное письмо компании-производителя об авторизации поставщика);

Необходимо наличие в г. Ташкенте сервисного центра от производителя, выполняющего гарантийное обслуживание товара и замену вышедшего из строя оборудования;

Поставщик обязан обеспечить выполнение работ по запуску и внедрению поставляемого оборудования силами своих квалифицированных инженеров, сертифицированных производителем оборудования.

Технические требования к поставщику и оборудованию

Документ предназначен для включения в конкурсную документацию/договор поставки и внедрения межсетевых экранов (NGFW), системы контроля доступа к сети и сопутствующей инфраструктуры для модернизации существующего комплекса «Удаленного доступа к сети» Заказчика.

Область применения и цели

- Предмет: поставка, внедрение, обучение и гарантийно-сервисная поддержка межсетевых экранов и с системы контроля доступа к сети (далее — «Оборудование»).
- Цель: обеспечить информационную безопасность и бесперебойную работу сетевой инфраструктуры Заказчика.

Определения и сокращения

- **Вендор** — производитель оборудования.
- **Поставщик** — участник закупки, официальный партнёр Вендора.
- **ПМИ** – программа и методика испытания
- **ПСИ** – приемосдаточные испытания
- **TAC** — служба технической поддержки Вендора (Technical Assistance Center).
- **RMA** — процесс замены неисправного оборудования.
- **NBD** — следующий рабочий день.

Требования к поставляемому оборудованию

Состояние и жизненный цикл

- Оборудование должно быть **новым**, не восстановленным, не бывшим в употреблении.
- На дату подачи заявки оборудование **не должно иметь объявлений** End-of-Sale (EoS) или End-of-Support (EoL) в горизонте **не менее 60 месяцев** с даты ввода в эксплуатацию.
- Вендор обязуется обеспечивать наличие запасных частей и модулей **минимум 36 месяцев** с даты ввода в эксплуатацию.

Комплектность и лицензирование

- Поставка включает все необходимые лицензии на заявленный функционал (L3/L7 FW, IPS/IDS, AppControl, SSL/TLS инспекция, User-ID, Threat Intelligence, URL-фильтрация) на **срок не менее 36 месяцев**.
- Указать модель лицензирования (perpetual/subscription) и ограничения (сквозная производительность, количество сессий, VPN-туннели, интерфейсы).

Документация

- В комплекте:
- паспорт/сертификат соответствия,
- руководства по установке/эксплуатации,
- схема коммутации,
- план адресации/прав доступа (по итогам ПНР),
- ПМИ и акт прохождения ПСИ,
- акт приёмки.

Качество и сертификация

- Подтверждение происхождения (Country of Origin), сертификация по ISO 9001/14001 у Вендора либо эквивалент.

Требования к Поставщику (квалификация)

Статус партнёра

- Наличие действующего статуса **официального сертифицированного партнёра** Вендора (не ниже уровня Gold/Advanced, либо эквивалент).
- Предоставить: партнёрский сертификат/скрин с портала Вендора, действительный на дату подачи заявки.

Профиль деятельности

- Основной вид деятельности: услуги в сфере **телекоммуникаций и/или строительства дата-центров**.
- Предоставить: выписку из реестра/устава, портфолио реализованных DC/Network/NGFW-проектов (минимум 3 проекта за последние 3 года).

Авторизация на продажу в Республике Узбекистан

- Письмо-авторизация от Вендора на имя Поставщика с правом поставки и пост-продажной поддержки на территории РУз.

Локальная сервисная инфраструктура

- Наличие **официального сервисного центра в г. Ташкенте** (с указанием адреса, контактных лиц, часов работы) для гарантийного обслуживания и замены оборудования.
- Склад оперативных ЗИП (минимально: блок питания, вентилятор, интерфейсные модули, SFP/SFP+, SSD/Flash если применимо) с гарантированным запасом на **не менее 3%** от поставленного парка или **не менее 1 комплекта** на модель — что больше.

Кадровая компетентность

- Команда внедрения: не менее **2 инженеров уровня Professional/Expert** по продуктам Вендора (сертификаты действующие).
- Подтвердить: сертификаты.

Гарантии и сервисная поддержка

Гарантия Вендора

- Минимум **36 месяцев** с даты ввода в эксплуатацию.
- Включает: замену неисправного оборудования (RMA), открытие сервисных кейсов в TAC, доступ к обновлениям ПО (major/minor/patch), к базе знаний и документации.

SLA TAC (реакция/эскалация)

- Каналы обращения: веб-портал, e-mail (обязательно), телефон (желательно).
- Времена реакции (Response Time) и плана действий (Workaround/Resolution):
  - **Severity 1 (P1, авария, простой сервиса)**: первичный ответ ≤ **4 часа**, активная работа 24×7, эскалация до L3 ≤ **8 часов**.
  - **Severity 2 (P2, деградация, риск отказа)**: первичный ответ ≤ **8 часов**, работа в режимах вендора, эскалация ≤ **24 часа**.
  - **Severity 3 (P3, функциональные вопросы/настройки)**: первичный ответ ≤ **12 часов**.

RMA/замена

- Тип: **Advanced replacement** (замена вперёд) при подтверждённой неисправности.
- Срок поставки заменяемого узла в г. Ташкент: **NBD** для критичных модулей, **до 5 рабочих дней** для прочих.
- Логистика и таможня — ответственность Поставщика.

Онсайт-поддержка

- При P1 — выезд инженера в пределах г. Ташкента **в течение 4 часов** с момента запроса, при P2 — **в течение 1 рабочего дня**.

Порядок работы с инцидентами

1. Открытие кейса в TAC Вендора через e-mail/портал с указанием серийных номеров, версии ПО, логов/tech-support.
2. Классификация по критичности (P1/P2/P3), назначение ответственного инженера.
3. Верификация неисправности, при необходимости — RMA, статус: «Подлежит замене/Repair».
4. Трекинг до полного восстановления сервиса. Еженедельный отчёт по открытым кейсам до закрытия.

Обучение и передача знаний

Доступ к материалам

- Заказчику предоставляется доступ к порталу обучения/базе знаний Вендора на **весь период использования решения** (включая обновления курсов).

Курсы Поставщика

- Обязателен **обучающий курс** (онлайн или офлайн) среднего/углублённого уровня по эксплуатации NGFW в дата-центрах: минимум **16 академических часов** (2 дня) + **лабораторные работы**.
- Содержание: архитектура DC, сегментация/VRF, HA-кластеры, BGP/ECMP/Failover, зоны безопасности, политики L7, SSL-инспекция, IPS/IDS, DDoS basic, логирование/SIEM, обновления/патчи, резервное копирование конфигураций, best practices.
- Количество потоков/слушателей — по заявке Заказчика (не менее **1 потока** по **4 человек**) с предоставлением материалов и записи (для онлайн) либо печатных конспектов (для офлайн).
- По итогам — тест и **сертификат о прохождении**.
- Обязателен обучающий курс (онлайн или офлайн) среднего/углублённого уровня по эксплуатации CISCO ISE, включая создание политик 802.1x: минимум 16 академических часов (2 дня) + лабораторные работы.
- Количество потоков/слушателей — по заявке Заказчика (не менее **1 потока** по **4 человек**) с предоставлением материалов и записи (для онлайн) либо печатных конспектов (для офлайн).
- По итогам — тест и **сертификат о прохождении**.

Внедрение (ПНР) и приёмка

Проектные работы

- Проведение ПНР: монтаж/коммутация, базовая и продвинутая конфигурация, интеграция с AAA/AD/IdP, NTP.

Тесты приёмочные (минимум):

- Проверка производительности (сквозная пропускная способность с включёнными IPS/App-ID/SSL-инспекцией) — достижение не ниже заявленного в ТКП.
- Функциональные сценарии: отказ одного узла HA, отказ/восстановление линка, изменение политики, генерация инцидента IPS, проверка URL-фильтрации.
- Резервное копирование/восстановление конфигурации.
- Итог: акт приёмки-передачи с протоколами тестов.

Сроки, поставка и логистика

- Срок поставки комплекта: **до 90 календарных дней** с даты подписания договора.
- ПНР: **до 25 рабочих дней** после поставки и готовности площадки.
- Поставщик обеспечивает упаковку, доставку, разгрузку, подъем и ответственность за сохранность до передачи Заказчику.

Информационная безопасность и соответствие

- Обязательные практики: безопасная конфигурация по CIS Benchmarks/Best Practices Вендора, отключение неиспользуемых сервисов, ротация паролей, разграничение ролей (RBAC), журналирование и экспорт логов.
- Передача исходных конфигураций, админ-доступов и паролей — по акту, в запечатанном виде/через защищённый канал.

Отчётность и KPI

- Ежемесячный отчёт Поставщика в период гарантии: открытые/закрытые кейсы, среднее время реакции/восстановления, статус обновлений ПО, потребление ресурсов, инциденты безопасности.
- Целевые KPI в гарантии: соблюдение SLA реакции ≥ **95%** случаев; доступность сервис-центра ≥ **99%** рабочих часов.

Ответственность и штрафные санкции

- Нарушение сроков поставки/замены: **0,1%** от стоимости просроченной части за каждый календарный день, но не более 10%.
- Несоблюдение SLA реакции (по P1/P2) более 2 раз в месяц — **штраф 1%** от стоимости договора за месяц.

Перечень подтверждающих документов в составе заявки

1. Партнёрский статус и письмо-авторизация на РУз.
2. Сертификаты инженеров.
3. Перечень реализованных проектов (референсы с контактами).
4. Гарантийное письмо о сроках EoS/EoL и доступности ЗИП.
5. Описание сервис-центра в Ташкенте и склад ЗИП.
6. Шаблон SLA и регламент RMA/TAC.
7. Учебная программа курса и формат проведения.

Состав выполняемых работ.

В рамках реализации проекта Поставщик должен выполнить полный комплекс работ по, поставке, внедрению и интеграции поставляемого оборудования, включая интеграцию с существующими системами Заказчика (NGFW, Cisco ACI, Border routers / switches, балансировщики и т.д.). *Полный список существующих систем, требующих интеграции можно получить по запросу.*

Монтаж, коммутация и базовая настройка.

Исполнитель должен:

- Выполнить поставку нового оборудования в полном объеме согласно требуемым техническим параметрам.
- Выполнить физическую установку и обеспечить корректную коммутацию с устройствами существующей сетевой инфраструктуры Заказчика.
- Произвести маркирование коммутационных линий связи в соответствии с требованиями Заказчика.
- Произвести обновление поставляемого оборудования до рекомендуемых версий от производителя и интеграцию устройств с порталом производителя для получения необходимых сервисов лицензирования, если таковые требуются.
- Произвести интеграции поставляемых МСЭ пользовательского сегмента сети с существующей централизованной системой управления.
- Произвести настройки по формированию двух отказоустойчивых пар МСЭ пользовательского сегмента сети для каждого ЦОД и развёртывание систем контроля удаленного доступа на каждой из площадок ЦОД в режиме 1+1.

Настройка сетевого взаимодействия МСЭ пользовательского сегмента сети с существующими системами и устройствами инфраструктуры.

Исполнитель должен:

- Выполнить построение схемы взаимодействия МСЭ пользовательского сегмента сети с маршрутизаторами границы сети и коммутаторами ядра.
- Выполнить перенос правил доступа с существующих МСЭ на поставляемые МСЭ пользовательского сегмента сети.

- Выполнить интеграцию системы контроля доступа к сети с поставляемыми МСЭ пользовательского сегмента сети и службой каталогов Active Directory для организации контроля удаленного доступа к сети.

Настройка сервисов безопасности МСЭ и политик доступа к сети заказчика.

Исполнитель должен:

- Настроить функции IPS/IDS, функционал URL фильтрации на МСЭ пользовательского сегмента сети, согласно правилам инспекции трафика.
- Настроить соответствующие политики аутентификации и авторизации на системе контроля доступа для обеспечения безопасного доступа пользователей к сети посредством защищенного канала связи (Remote Access VPN) для следующих сценариев:

  - корпоративные компьютеры с операционной системой Windows с возможностью менять истекший пароль (процедура Change password);
  - корпоративные компьютеры с операционной системой MAC OS с возможностью менять истекший пароль (процедура Change password);
  - любые недоверенные устройства (не являющиеся частью MS AD/LDAP) к гостевой подсети с возможностью менять истекший пароль (процедура Change password)"

- Настроить профили безопасности и политики аутентификации для проводных и беспроводных пользователей и устройств согласно следующим разделениям:

  - проводные и беспроводные устройства (IP телефоны, принтеры, МФУ и т.д.) на основе MAC-адресов устройств по методу аутентификации MAB;
  - проводные и беспроводные пользователи, подключающиеся к сети с устройств (ПК, ноутбук) с операционной системой Windows с оценкой состояния устройств на наличие актуальных патчей, антивирусов и т.д. по методу аутентификации AD + TEAP.
  - проводные и беспроводные пользователи, подключающиеся к сети с устройств (ПК, ноутбук) с операционной системой MAC OS по методу аутентификации на базе сертификатов;
  - беспроводные пользователи с возможностью прохождения само-аутентификации через портал системы контроля доступа, при необходимости с интеграцией через SMS шлюз.

- Выполнить настройку политик аутентификации и авторизации для проводных, беспроводных и VPN-подключений с использованием механизмов оценки состояния конечных устройств (posture assessment), обеспечивающих проверку соответствия требованиям безопасности, включая актуальность обновлений ОС, наличие и работоспособность антивирусного ПО и иных средств защиты информации.
- Настроить динамические листы контроля доступа с возможностью трансляции их на МСЭ пользовательского сегмента сети.
- Обеспечить требуемые доступы к необходимым сегментам сети для удаленных пользователей согласно политикам доступа заказчика.
- Выполнить валидацию корректности настроенных политик доступа, тестирование связности и корректности передачи трафика между удаленными пользователями и внутренними сегментами сети заказчика.
- Работы по настройке 802.1x на сетевом оборудовании выполняются:

  - один существующий коммутатор,

  - один существующий Wi-Fi контроллер доступа,

- межсетевые экраны, поставляемые в рамках данного конкурса, и применяются для аутентификации 2-3 конечных устройств, выбранных для демонстрации.

Массовое внедрение, тиражирование и адаптация политик аутентификации на иные устройства Заказчика в объём настоящих работ не входят. Поиск неисправностей и диагностика сторонних устройств (включая существующее сетевое оборудование, персональные компьютеры, устройства с MAC OS, SMS шлюзы и иные устройства Заказчика) в рамках данной реализации в объём работ не входят.

-

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ОБОРУДОВАНИЮ ДЛЯ РЕАЛИЗАЦИИ ДАННОГО ПРОЕКТА

1.1 Краткая информация по оборудованию и количеству.

№.	Описание	Ед. Изм	Количество
1.	Система контроля доступа к сети.	Шт.	2
2.	Межсетевой экран следующего поколения пользовательского сегмента сети для ЦОД1 и ЦОД2.	Шт.	4
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

1.2 Система контроля доступа к сети.

Наименование требований	Технические требования
Кол-во	2 комплекта.
Тип продукта	Система контроля доступа к сети
Реализация	Система должна быть реализована в виде виртуальной машины на базе платформы виртуализации VMware ESXi
Управление	Управление системой должно осуществляться через встроенную WEB консоль администрирования, без необходимости установки отдельных агентов и ПО для управления, мониторинга и отчетности
Количество одновременных сессий	Система должна быть рассчитана на 1000 одновременных пользовательских сессий/подключений;
Отказоустойчивость	Система должна предусматривать отказоустойчивую схему развертывания 1+1
Общее описание системы	• Система должна реализовывать функции контроля доступа к сети. Контроль доступа к сети должен обеспечиваться для проводного и беспроводного сегментов сети, а также для удаленных пользователей, подключающихся по технологии Remote Access VPN; • Наличие поддержки работы системы согласно стандарту 802.1x. Система в данном случае выступает как сервер AAA (Аутентификация, авторизация и учет); • Наличие поддержки протокола Radius для обеспечения функций аутентификации и авторизации пользователей и конечных устройств, подключающихся к проводному и беспроводному сегментам сети, а также к удаленным подключениям VPN; • Наличие поддержки механизма Radius CoA (Change of Authorization) для возможности назначения и изменения уровня пользовательского доступа к сети в зависимости от условий подключения; • Наличие поддержки протокола EAP (EAP-TLS, EAP MS-CHAP, PEAP); • Обеспечение одновременной пользовательской и машинной аутентификации с использованием доменных учетных данных и сертификатов в рамках одной пользовательской сессии; • Наличие поддержки использования различных полей пользовательского сертификата, таких как Common Name, Subject Alternative Name, Serial Number, SAN-Email и SAN-DNS, для идентификации пользователя в процессе аутентификации; • Наличие поддержки локальной базы пользователей; • Наличие поддержки локальной базы устройств на основе MAC адресов; • Наличие поддержки интеграции с корпоративным каталогом Active Directory. Должна обеспечиваться возможность осуществления авторизации на основе принадлежности пользователей к группам в Active Directory; • Наличие возможности определения последовательности проверки баз данных пользователей;

Наименование требований	Технические требования
	• Обеспечивать мониторинг путем обнаружения и управления подключающихся к сети оконечных устройств для предоставления соответствующих сервисов и уровней доступа; • Обеспечивать предотвращение несанкционированного доступа к сети для защиты корпоративных активов; • Наличие поддержки встроенной консоли мониторинга и устранения неполадок для упрощения работы специалистов службы поддержки и администраторов; • Наличие поддержки применения листа контроля доступа или соответствующего идентификатора VLAN для пользователя в результате процесса авторизации; • Наличие поддержки функции проверки операционной системы пользовательского устройства на предмет наличия соответствующих версий операционной системы, установленных приложений, антивирусного программного обеспечения, параметров в системном регистре, статус активности программных компонентов. Система должна быть рассчитана на одновременную проверку не менее 1000 пользовательских устройств. Поддержка возможности применения политики доступа в зависимости от статуса соответствия заданным параметрам; • Наличие встроенной службы центра сертификации; • Наличие поддержки функции автоматического определения типа и версии программного обеспечения подключаемого пользовательского устройства. Система должна быть рассчитана на одновременное подключение не менее 1000 пользовательских устройств; • Система должна быть совместима с существующим активным оборудованием (коммутаторами, устройствами безопасности, контроллерами беспроводной сети) сетевой инфраструктуры; • Наличие поддержки аутентификации и авторизации для административного доступа к оборудованию сети с возможностью авторизации вводимых команд на сетевом оборудовании и ведением журнала по ним;
Лицензирование	36 месяцев
Сервисная поддержка	36 месяцев

1.4 Межсетевой экран следующего поколения пользовательского сегмента сети для ЦОД1 и ЦОД2.

Наименование требований	Технические требования
Кол-во	4 комплекта
Тип продукта	Межсетевой экран
Форм-фактор	Установка в стандартные 19" монтажные шкафы, должен занимать не более 1U.
Количество встроенных интерфейсов	Не менее 8 медных портов 1 Гбит/с RJ45, не менее 4 оптических портов 1/10 Гбит/с SFP+
Порты управления	Serial console port - RJ45 - не менее 1 шт, Management port 1Гбит/с RJ45– не менее 1шт.
Наличие USB 3.0 портов	Не менее 1 порта
Дисковый накопитель	Наличие SSD накопителя ёмкостью не менее 400 ГБ U.2 NVME
Требования к производительности межсетевого экрана.	o Пропускная способность межсетевого экрана в режиме инспекции трафика не менее 13 Гбит/с o Пропускная способность межсетевого экрана в режиме инспекции трафика, контроля приложений и системы предотвращения вторжений не менее 9 Гбит/с o Пропускная способность межсетевого экрана в режиме IPSec VPN не менее 13 Гбит/с o Количество одновременных сессий не менее 400 000. o Кол-во создания новых сессий в секунду не менее 50 000 o Дешифрация TLS трафика не менее 2.5 Гбит/с
Требования к функционалу межсетевого экрана.	o Оборудование межсетевого экрана должно содержать компонент, поддерживающий процедуру безопасной загрузки устройства, для предотвращения запуска неоригинального программного обеспечения или несанкционированной модификации оригинального программного обеспечения o Межсетевой экран следующего поколения должен поддерживать возможность использования сервисов управления работой приложений, предотвращения вторжений, фильтрации запросов пользователей по URL, предотвращения проникновения вредоносного кода (допускается активация различного функционала с помощью отдельных дополнительных подписок). o Поддержка развертывания как в «прозрачном» режиме, так и в режиме маршрутизации. o Поддержка протоколов IPv4 и IPv6. o В частности, для протокола IPv6 поддержка в рамках правил межсетевого экрана, управления работой приложений, системы предотвращения вторжений, фильтрации веб-запросов пользователей по URL. o Поддержка протоколов маршрутизации OSPF и BGP (версии 4 и версии 6). o Поддержка протоколов маршрутизации BGP (версии 4 и версии 6) и механизма bidirectional forwarding detection (BFD) для BGP.

Наименование требований	Технические требования
	○ Поддержка динамического и статического механизма трансляции сетевых адресов NAT. ○ Поддержка распознавания более 4 000 приложений с возможностью гранулярного управления функциональностью ряда приложений. ○ Возможность управления использованием приложений на уровне отдельных пользователей или групп пользователей, возможность интеграции с внешними каталогами пользователей. ○ Возможность описания приложений администратором системы с использованием стандартного для отрасли языка OpenAppID. ○ Поддержка классификации приложений по уровню риска и по уровню соответствия требованиям бизнеса. ○ Поддержка механизмов ограничения скорости передачи и обеспечения качества обслуживания. ○ Поддержка локального управления на уровне устройства и централизованного управления системой управления. Доступный функционал может различаться в зависимости от выбранного варианта управления. ○ Поддержка механизмов обеспечения высокой доступности в режимах Активный/Резервный. ○ Возможность настройки правил изменения маршрута передачи пакетов по критериям, отличным от адреса назначения (Policy Based Routing, PBR) с отслеживанием доступности пути. ○ Поддержка не менее 10 независимых таблиц маршрутизации (Virtual Routing and Forwarding, VRF). ○ Поддержка интерфейсов наложенных сетей с инкапсуляцией VXLAN и GENEVE. ○ Поддержка подключения виртуальных частных сетей не менее 500 VPN peer. ○ Поддержка топологий виртуальных частных сетей точка-точка, звезда и полносвязной. ○ Поддержка виртуальных частных сетей в режиме без выделенных интерфейсов (Policy-based). ○ Поддержка удаленных узлов виртуальных частных сетей с динамическими адресами. ○ Поддержка виртуальных частных сетей с использованием статических и динамических туннельных интерфейсов (Route-based).
Требования к построению виртуальных частных сетей удаленного доступа	○ Наличие клиента виртуальных частных сетей удаленного доступа с поддержкой операционных систем Windows, MacOS, Linux, Android и iOS. ○ Поддержка передачи данных удаленных клиентов виртуальных частных сетей по протоколам IPSec-IKEv2, TLS и DTLS. ○ Поддержка ограничения списка приложений, которым разрешен доступ к VPN на мобильных устройствах Android и iOS.

Наименование требований	Технические требования
	○ Поддержка централизованной аутентификации пользователей с помощью имени и пароля по протоколам AD, LDAP, и RADIUS. ○ Поддержка использования в политике контроля доступа межсетевого экрана полученного идентификатора и группы пользователя. ○ Поддержка смены пользовательского пароля с истекшим сроком действия в процессе подключения. ○ Поддержка аутентификации пользователей в режиме Single Sign-On по протоколу SAML 2.0. ○ Поддержка аутентификации пользователей с помощью сертификатов. ○ Поддержка одновременной аутентификации пользователей по паролю и с помощью сертификата. ○ Поддержка одновременной аутентификации пользователей через SAML SSO и с помощью сертификата. ○ Поддержка одновременной аутентификации пользователей и устройств по нескольким сертификатам. ○ Поддержка многофакторной аутентификации пользователей. ○ Поддержка балансировки нагрузки между несколькими узлами виртуальной частной сети удаленного доступа. ○ Поддержка режима Split Tunneling для обеспечения локального доступа к сети Интернет одновременно с защитой взаимодействия с внутренними сервисами организации. ○ Поддержка динамического механизма разделения трафика Split Tunneling на основе имен DNS. ○ Поддержка профиля удаленного управления клиентскими устройствами. ○ Поддержка гибкой настройки атрибутов LDAP для авторизации пользователей. ○ Поддержка назначения клиентского адреса сервером RADIUS. ○ Поддержка динамического назначения профиля доступа по атрибуту от сервера RADIUS. ○ Поддержка назначения пользователю, загружаемого с сервера RADIUS списка контроля доступа. ○ Поддержка динамического изменения авторизации пользователя и механизма RADIUS Change of Authorization (RADIUS CoA). ○ Поддержка динамических политик контроля доступа по результатам проверки рабочей станции на соответствие политике информационной безопасности. ○ Если данный функционал требует приобретения отдельной лицензии, то требуется заложить лицензии на 500 уникальных пользователей удалённого доступа сроком на три года.
Требования к системе централизованного управления.	○ Возможность получать доступ к содержимому сетевого пакета при анализе события безопасности.

Наименование требований	Технические требования
	○ Встроенные механизмы создания пользовательских отчетов произвольного содержания по событиям, содержащимся в базе данных. ○ Возможность создания отчета одним щелчком с настраиваемой информационной панели. ○ Поддержка различных форматов выгрузки отчетов (PDF, HTML, CSV). ○ Возможность произвольного поиска по базе данных событий. ○ Возможность создания и сохранения пользовательских шаблонов поиска. ○ Поддержка ролевой модели управления доступом к системе централизованного управления. ○ Возможность интеграции с внешними системами аутентификации (RADIUS, LDAP, AD). ○ Поддержка открытых API для взаимодействия внешних систем с системой централизованного управления. ○ Единая платформа централизованного управления сервисами межсетевого экрана, системы предотвращения вторжений, контроля приложений, фильтрации веб-запросов пользователей по URL, платформы для предотвращения проникновения вредоносного кода. ○ Поддержка взаимодействия со сторонними системами в результате корреляции различных условий (возможность инициировать действие в сторонней системе как результата корреляции различных условий). ○ Поддержка SQL-доступа к базе данных событий со стороны внешних систем.
Дополнительные требования к сервисам обеспечения информационной безопасности.	Требования к сервису предотвращения вторжений: ○ Сервис предотвращения вторжений должен непрерывно оценивать состояние сети и параметры оконечных устройств. Он должен использовать результаты оценки при принятии решений. ○ В процессе оценки сети сервис предотвращения вторжений должен автоматически формировать профиль оконечного устройства, регистрируя операционную систему, используемые сервисы и приложения, а также определяя возможные уязвимости оконечного устройства. ○ Сервис предотвращений вторжений должен автоматически определять приоритет событий безопасности в соответствии со сведениями о защищаемой среде (с учетом профиля оконечного устройства и сведений о возможных уязвимостях). ○ Сервис предотвращения вторжений должен автоматически формировать рекомендации по политике предотвращения вторжений на основании результатов оценки сети. ○ Сервис предотвращения вторжений должен поддерживать задание белых списков

Наименование требований	Технические требования
	устройств/операционных систем/приложений/сервисов. o Сервис предотвращения вторжений должен поддерживать возможность задания правил корреляции событий. o Сервис предотвращения вторжений должен поддерживать возможность инициирования действий внешними системами на основании правил корреляции. o Сервис предотвращения вторжений должен поддерживать обнаружение признаков компрометации оконечных устройств на основании нескольких событий безопасности. o Сервис предотвращения вторжений должен поддерживать API для дополнения данных об оконечных устройствах из других источников. o Сервис предотвращения вторжений должен поддерживать возможность просмотра правил/фильтров/сигнатур. o Сервис предотвращения вторжений должен поддерживать возможность редактирования существующих правил. o Сервис предотвращения вторжений должен поддерживать возможность создания пользовательских правил с использованием синтаксиса системы с открытым исходным кодом Snort версии 3 o Система должна поддерживать автоматическую регулярную загрузку черных и белых списков IP-адресов, URL-адресов и DNS-имен как из источников, определяемых производителем, так и из пользовательских источников. o Система должна поддерживать механизм «DNS sinkholing» на основании динамических списков DNS-имен. Требования к сервису предотвращения проникновения вредоносного кода: o Поддержка ретроспективного уведомления о пропуске своевременно не обнаруженного вредоносного кода в защищаемую инфраструктуру. o Возможность формирования политик на уровне типов файлов. o Использование нескольких алгоритмов для обнаружения вредоносного кода, использование специализированной облачной системы для обнаружения вредоносного кода, возможность динамического анализа файла. o Возможность формирования траектории перемещения файла между оконечными устройствами защищаемой инфраструктуры. o Возможность регистрации (и сохранения) заведомо вредоносных файлов, заведомо безвредных файлов и

Наименование требований	Технические требования
	файлов, вердикт о вредоносности которых пока не вынесен. o Возможность обнаружения первоначальной точки проникновения вредоносного ПО. Требования к сервису контроля приложений и фильтрации веб-запросов пользователей по URL: o Сервис контроля приложений должен выполнять глубокую инспекцию пакетов и позволять фильтровать трафик на основе конкретных приложений. Должно быть доступно более 4000 различных приложений, включая TeamViewer, голосовые/видео приложения, почтовые приложения, file sharing, peer-to-peer торренты (P2P), игры и т.д o Сервис фильтрации должен поддерживать автоматическую регулярную загрузку черных и белых списков IP-адресов, URL-адресов и DNS-имен как из источников, определяемых производителем, так и из пользовательских источников. o Сервис фильтрации должен поддерживать возможность категоризации URL и фильтрации на уровне категорий URL. o Сведения о различных категориях URL должны автоматически обновляться в режиме реального времени. o Сервис фильтрации запросов по URL должен обеспечивать фильтрацию HTTPS-запросов без расшифровки SSL-трафика. o Сервис фильтрации запросов должен поддерживать возможность разрешения определенным группам пользователей или пользователям «осознанно обходить» установленные правила фильтрации без вмешательства ИТ-администратора.
Подписка на обновление сигнатур сервиса предотвращения вторжений, сервис предотвращения проникновения вредоносного кода и сервиса фильтрации URL	36 месяцев
Сервисная поддержка	36 месяцев