Техническая спецификация
на приобретение программно-аппаратного комплекса защиты сетевой инфраструктуры

1. Межсетевой экран (программно-аппаратный комплекс защиты сетевой инфраструктуры).

1.1. Общее требования .

- К участию в конкурсе допускаются UTM решения, имеющие положительные оценки и заключения ведущей мировой исследовательской компании и независимой тестовой лаборатории (Gartner /gartner.com/, ICSA Labs /icsalabs.com/).
- В частности, к конкурсу допускаются Системы (производители Систем), удовлетворяющие одному (любому) из следующих критериев:
    - Отнесенные исследовательской компанией Gartner к сегменту лидеров (Leaders), в соответствии с последней редакцией “магического квадранта” (Magic Quadrant for Unified Threat Management).
    - Отнесенные исследовательской компанией Gartner к любому из сегментов “магического квадранта” (Magic Quadrant for Network Intrusion Prevention System) и вместе с этим имеющие сертификаты ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL, VPN.
- Межсетевые экраны должны полностью интегрироваться с системой централизованного управления.
- Все предлагаемые решения, должны быть **одного производителя** и собираться в полностью интегрируемый программно-аппаратный комплекс обеспечения безопасности.

1.2. Общие описание.

Межсетевой экран с функциями:

- Маршрутизации (статической, динамической, на основе политик (PBR));
- Фильтрации и квотирования web-контента;
- Антивирусной защиты;
- Защиты от спама и нежелательной корреспонденции;
- Предотвращения вторжений (IDS/IPS);
- Предотвращения утечки конфиденциальной информации (DLP);
- Контроля приложений;
- Оптимизации траффика (QoS, кэширование, Traffic Shaping);
- Поддержка SSL/IPSec VPN;
- Балансировки 2-ух и более WAN каналов;
- Контроллера коммутаторов.

Комплекс должен иметь функцию отказоустойчивости и собираться в кластер до четырёх устройств.

2. Технические требования к межсетевым экранам.

2.1. Общие требования к функционалу межсетевых экранов.

Требования к функционалу	
Модуль антивирусной защиты / обнаружения и уничтожения червей и зловредного ПО.	• Наличие функции проверки HTTP, SMTP, POP3, IMAP, FTP-протоколов и IM-служб • Наличие функции проверки зашифрованных VPN-туннелей. • Наличие функции проверки автоматической “оперативной доставки” обновлений антивирусных баз. • Наличие функции помещения инфицированных сообщений в карантин. • Наличие функции блокирования в зависимости от размера файла. • Наличие функции блокирования в зависимости от типа файла.
Сетевые функции	• Наличие поддержки соединений множества WAN-сетей. • Наличие поддержки PPPoE-протокола • Наличие поддержки DHCP-протокола в конфигурации “Клиент/Сервер” • Наличие функции маршрутизации на основе политик.

	• Наличие функции динамической маршрутизации (RIP v1 и v2, OSPF, BGP, Multicast). • Наличие поддержки множества зон. • Наличие функции маршрутизации между зонами. • Наличие функции маршрутизации между виртуальными сетями.
Администрирование/управление	• Наличие функции управления на основе ролей. • Поддержка нескольких уровней администраторов и пользователей. • Наличие функции обновления через TFTP-протокол и web-интерфейс пользователя. • Наличие функции возврата к предыдущему состоянию в системном программном обеспечении.
Аутентификация пользователей	• Наличие встроенной базы локальных пользователей и групп. • Поддержка интеграции и автоматического обновления базы пользователей и групп посредством интеграции службы Windows Active Directory • Поддержка внешней базы данных RADIUS/LDAP • Поддержка привязки по IP/MAC-адресу. • Поддержка Xauth через RADIUS для IPSEC VPN-протокола • Поддержка двухфакторной аутентификации • Поддержка Single Sign-on
Межсетевой экран	• Поддержка NAT, PAT, «прозрачный» • Наличие режима маршрутизатора (RIP v1 и v2, OSPF, BGP, Multicast). • Поддержка функции NAT на основе политик. • Поддержка функции виртуальных устройств (NAT / «прозрачный режим»). • Поддержка функции VLAN Tagging (802.1Q) • Наличие функции аутентификации на основе групп пользователей. • Поддержка функции SIP/H.323 NAT Traversal • Поддержка WINS. • Наличие настраиваемых профилей защиты.
VPN	• Поддержка функции PPTP, IPSec и SSL • Поддержка функции шифрования (DES, 3DES, AES256) • Наличие функции аутентификации SHA-512 / MD5 • Наличие сквозного VPN-клиента PPTP, L2TP • Поддержка иерархических (hub and spoke) VPN-соединений. • Наличие функции аутентификации по IKE сертификату • Поддержка IPSec NAT • Наличие механизма Dead Peer • Поддержка двухфакторной аутентификации.
Фильтрация web-содержимого	• Наличие функции блокирования URL по ключевому слову/фразе. • Наличие функции контроля доступа по категориям узлов. • Наличие функции «Белые/Черные» списки URL. • Поддержка опции Профили содержимого. • Наличие функции Блокирование аплетов Java, Cookies, элементов управления ActiveX. • Поддержка репутационного анализа. • Наличие возможности квотирования трафика по объёму на определённый период.
Система предотвращения вторжений (IPS/IDS)	• Наличие возможности предотвращения не менее чем 11 000 видов сигнатурных атак. • Возможность настройки списка сигнатур динамического обнаружения.

	• Поддержка автоматического обновления базы сигнатур.
Модуль антиспам защиты	• Поддержка «черных» списков в режиме реального времени / Сервер базы данных «открытых ретрансляторов». • Наличие функции проверки заголовков MIME. • Наличие функции фильтрации по ключевым словам / фразам. • Поддержка «черных» / «белых» списков IP-адресов. • Наличие функции автоматического, получения обновлений в режиме реального времени из сети служб обновлений.
Протоколирование / мониторинг	• Наличие функции внутреннего протоколирования. • Наличие функции отсылки протоколов на удаленный Syslog. • Наличие графических средств для мониторинга в реальном времени и просмотра истории. • Наличие функции уведомления о вирусах и атаках по электронной почте. • Наличие функции мониторинга VPN-туннелей. • Поддержка опционального протоколирования с использованием дополнительного аппаратного решения. • Наличие возможности хранения и обработки событий в облаке.
Формирование трафика	• Возможность формирования трафика на основе политик. • Наличие функции настройки различных видов обслуживания разнотипного трафика. • Наличие режимов гарантированной / максимальной / приоритетной пропускной способности.
Обязательная поддержка перечисленных служб мгновенных сообщений – контроль доступа	• AOL-IM. • Yahoo. • MSN. • ICQ.
Proxy-server и Web-cache	• Наличие функции локального хранения Web-контента, запрашиваемого пользователями для оптимизации работы полосы пропускания. • Наличие режима работы межсетевого экрана в роли Proxy-сервера.
Обязательное наличие перечисленных выполняемых функций	• Межсетевое экранирование. • Маршрутизация трафика. • Механизм виртуальных устройств (разделение физического устройства на 2 и более логических устройств не менее 10). • Аутентификация пользователей. • Антивирус. • Антиспам. • IPS. • Web-filter. • Application control.

2.2. Требования к техническим характеристикам программно-аппаратного комплекса.

Наименование	**Технические характеристики**
Количество	2 шт.
Технические требования	
Форм фактор	Desktop
Пропускная способность с контролем состояния соединений	Не менее 4 Гбит/с.

Задержка при обработке пакетов	Не более 3 Мкр сек.
Пропускная способность по количеству пакетов	Не менее 6 000 000 пакетов/сек.
Производительность IPsec VPN	Не менее 2,5 Гбит/с.
Количество VPN-тунелей (точка-точка)	Не менее 200.
Количество VPN-тунелей (клиент-точка)	Не менее 2500.
Производительность IPS	Не менее 450 Мбит/с
Производительность контроля приложений	Не менее 900 Мбит/с.
Производительность SSL VPN	Не менее 200 Мбит/с.
Количество SSL VPN пользователей	Не менее 200.
Количество новых сессий в секунду	Не менее 30000.
Количество одновременных сессий	Не менее 1300000.
Производительность в режиме инспекции SSL-трафика	Не менее 135 Мбит/с.
Количество политик безопасности	Не менее 5000.
Количество жестких дисков	**1**
Объем хранилища	**Не менее 128GB SSD**
Встроенные средства ввода/вывода	Не менее 2 портов GE DMZ/HA Ports; Не менее 12 портов GE RJ45; Не менее 2 портов RJ45/SFP Shared Media Pairs; Не менее 1 разъема USB 2.0 для управления; Не менее 1 консольного порта RJ-45.
Количество виртуальных устройств	Не менее 10.
Возможность поддержки отказоустойчивости	Active-Active / Active-Standby.
Обновления	Обновление сигнатур систем антивируса и предотвращение вторжений, доступ онлайн web-фильтрации и антиспама не менее 3 года. **Возможность централизованного обновления с единой системой управления**
Рабочее напряжение	От 100В до 240В.
Рабочая температура	От 0 до 40 С.
Влажность	От 10% до 90% без конденсации.
Гарантия	Не менее 3 года, включая техническую поддержку от производителя в режиме 24х7 по телефону и через интернет

3. Технические требования к оборудованию централизованного управления

Наименование	**Технические характеристики**
Количество	1 шт.
Архитектура и форм-фактор	Не более 1RU
Сетевые интерфейсы	Не менее 2 портов GE RJ45 Не менее 2 портов GE SFP не менее 1 порта DB9
Количество управляемых устройств	Не менее 30
Количество жестких дисков	Не менее 2
Объем хранилища	8 TB
Объем журналов обрабатываемых за день:	Не менее 2 GB / Day logs
Административные домены и глобальные политики	• Обязательное наличие перечисленных функциональных возможностей, которые позволяют администратору создавать группы устройств для других администраторов с целью мониторинга и управления:

	- Администраторы должны управлять устройствами в их географической локации или бизнес-подразделении. - Несколько виртуальных доменов должны иметь возможность быть разделены между несколькими административными доменами - Гранулированные политики доступа должны позволять назначать административным доменам и политики конкретным пользователям. - Пользователи должны иметь доступ к устройствам и виртуальных доменов, которые им назначены. - Наличие возможности создания шаблонов конфигурации устройств для быстрой настройки новых устройств безопасности. - Каждый административный домен должен иметь общую базу объектов для всех устройств и пакетов политик, должен позволять пользователям использовать подобные настройки в необходимой группе. - Наличие возможности настройки глобальных политик.
Локальный хостинг контента безопасности	• Обязательное наличие функции сохранения контента безопасности локально, которая должна позволять администраторам контролировать обновления и обеспечивать улучшения времени ответа для рейтинговых баз данных. Должен включать в себя поддержку: - Обновление баз антивируса. - Обновления сигнатур IPS. - Обновления настроек уязвимостей. - Веб-фильтрация. - Анти-спам.
Мониторинг, анализ и отчет	• Наличие функции управления устройствами и конечными агентами индивидуально или на основе групп. • Наличие возможности обновления прошивок устройств. • Наличие функции выявления новых устройств. • Наличие функции создания, развертывания и мониторинга VPN. • Наличие возможности делегирования контроля другим пользователям с распределенными функциями администрирования. • Наличие возможности проведения аудита изменений конфигурации для обеспечения соблюдения согласия. • Наличие функции мониторинга политик безопасности и сетевой статистики. • Мониторинг в реальном времени и интегрированная система базовой отчетности позволяет наблюдать за сетевой и пользовательской активностью. • Поиск по устройству, ADOM или в совокупности. • Фильтрация логов и функции поиска. • Гранулированный обзор с панелью детализации • Интуитивно понятный интерфейс.
Наличие возможности управлять устройствами с помощью утилит, поддерживающих следующие инструменты	• JSON, XML, API
Гарантия и сервисная поддержка	• Оборудование должно обеспечиваться гарантией от производителя сроком не меньше 3 года. • Обязательное получение всех обновлений. • Обязательное получение основных и промежуточных релизов программного

	обеспечения через сайт, поддержка программных кодов в актуальном состоянии в соответствии с рекомендациями производителя, в том числе микрокодов устройств. • Предоставление консультаций по телефону, электронной почте и на сайте поддержки производителя с понедельника по пятницу с 00.00 до 24.00 часов круглосуточно; • Постоянный (не менее 8 часа х 5 дней) авторизованный доступ к сайту производителя.

4. Общие требования к функционалу сбору и анализу событий.

Требования к функционалу	Описание
Общие требования.	• В комплекте с оборудованием должен присутствовать набор не менее чем из 30 настраиваемых графических отчетов для упрощенного мониторинга и управления политиками безопасности, определения шаблонов атак, и обеспечения соответствия нормативным и международным стандартам защиты данных, по которым можно отфильтровать и оценить события по различным параметрам, включая трафик, события, вирус, атаку, web-контент, и содержимое почтовых сообщений – с целью определения состояния безопасности системы и ее соответствие нормативным актам и стандартам, а также должна быть возможность создания и редактирования собственных шаблонов. • Оборудование должно иметь функции архивирования файлов, находящихся в карантине, корреляции событий, оценки уязвимости сети, анализа трафика в сети, архивации таких событий, как почтовые сообщения, доступ в Интернет, IM-сообщения, содержимое пересланных файлов. • Корреляция событий, расследование аномальных событий, и оценка уязвимостей.
Инструменты отчетности и визуализации	• Оборудование должно уметь генерировать графики для конкретного случая с возможностью фильтрации по топ пользователям, приложениям, направлениям, веб-сайтам, угрозам, использованию VPN и другим. • Встроенные шаблоны отчетов. Использование или модификация PDF-шаблонов для отображения цветных, комплексных, графических отчетов по использованию и функциям безопасности сети. • Регулярный анализ профилей безопасности и характера трафика/ пропускной способности в отчетах. • Контроль важных событий для отчетности перед администратором о потенциально аномальном поведении устройств
Отображение журналов	• Отображение исторических логов или в реальном времени. • Выборка из логов трафика, логов событий и логов безопасности. • Поиск по устройству, административному домену или в совокупности. • Фильтрация логов и функции поиска. • Гранулированный обзор с панелью детализации
Управление событиями	• Конфигуратор комплексных предупреждений.

	• Триггеры для всех уровней "severity" журналов, конкретных событий, действий и направлений. • Установка порогов по количеству событий для конкретного промежутка времени. • Просмотр или поиск исторических предупреждений. • Сообщение по электронной почте / SNMP или syslog.

4.1 Требования к техническим характеристикам к сбору и анализу событий.

Наименование	**Технические характеристики**
Количество	1 шт.
Архитектура и форм-фактор	Не более 1RU
Интерфейсы	Не менее 2 портов GE RJ45
Количество жестких дисков	Не менее 1
Объем хранилища	Не менее 4 TB
Производительность журналирования (GB/day of logs):	Не менее 100
Стабильная скорость в режиме аналитики (логов/сек)	Не менее 3000
Стабильная скорость в режиме коллектора (логов/сек)	Не менее 4500
Устройства/Виртуальные/ Административные (максимум)	Не менее 150
Рабочее напряжение	От 100В до 240В
Рабочее температура	От 0 до 40 С
Влажность	От 20% до 90% без конденсации
Гарантия и сервисная поддержка	Оборудование должно обеспечиваться гарантией от производителя сроком не меньше 3 года. Получение всех необходимых обновлений. Получение основных и промежуточных релизов. программного обеспечения через сайт или поддержка программных кодов в актуальном состоянии в соответствии с рекомендациями производителя, в том числе микрокодов операционной системы. Постоянный (не менее 8 часов х 5 дней) авторизованный доступ к сайту производителя.

5. Техническая спецификация точек доступа

Наименование	**Технические характеристики**
Количество	3 шт.
Тип оборудования	Внутренние
Сетевые интерфейсы	Не менее 1x GE RJ45 порта
Поддержка беспроводных стандартов	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3az
Количество радиомодулей	Не менее 2
Количество внутренних антенн	Не менее 4
Пиковое усиление антенны	Не менее 4 dBi for 2.4 GHz Не менее 5 dBi for 5 GHz
Диапазоны частот (GHz)	От 2.400 До 2.4835 От 5.150 До 5.250 От 5.250 До 5.350 От 5.470 До 5.725 От 5.725 До 5.850
Диапазон Radio 1	Не менее 2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz (256 QAM)
Диапазон Radio 2	Не менее 5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)

Максимальная скорость передачи данных	Radio 1: Не менее 400 Mbps Radio 2: Не менее 867 Mbps
Количество одновременных SSID	Не менее 16
Типы EAP	Не менее EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Аутентификация	WPA™ и WPA2™ совместно с 802.1x или Preshared key, WEP и Web Captive Portal, чёрные / белые списки MAC
Максимальная Tx мощность	Не менее 23 dBm (200 mW) @ 2.4 GHz Не менее 24 dBm (251 mW) @ 5 GHz
Управление	**Точки доступа и ПАК должны быть полностью интегрированными и должны быть одного производителя.**
Гарантия	Не менее 3 года, включая техническую поддержку от производителя в режиме 8x5 по телефону и через интернет

6. Техническая спецификация безопасной аутентификации

7. Наименование	**Технические характеристики**
Количество	1 шт.
Технические требования	
Форм фактор	Не менее 1RU
Всего пользователей (локальных + удаленных)	Не менее 500
Количество клиентов RADIUS (устройства NAS)	Не менее 166
Количество групп пользователей	Не менее 50
CA сертификаты	Не менее 10
Пользовательские сертификаты	Не менее 2500
Количество жестких дисков	Не менее 1
Встроенные средства ввода/вывода	Не менее 4 портов GE RJ45; Не менее 1 порта DB9
Объем хранилища	Не менее 1 TB
Дополнительные функции и преимущества	Аутентификация пользователя RADIUS и LDAP Широкий спектр методов строгой аутентификации Самостоятельная регистрация пользователя и восстановление пароля Интеграция с Active Directory и LDAP Управление сертификатами Аутентификация 802.1X
Поддерживаемые стандарты	10/100/1000 Base-TX (GbE), 1000, IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Certificate Revocation (RFC3280), PKCS#12 Certificate Import, PKCS#10 CSR Import (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP)
Потребляемая мощность (в среднем)	Не менее 60W
Рабочее напряжение	От 90В до 240В.
Рабочая температура	От 0 до 40 С.
Влажность	От 5% до 90% без конденсации.
Гарантия	Не менее 3 года, включая техническую поддержку от производителя в режиме 24x7 по телефону и через интернет