**Техническая спецификация по государственной закупке товара**

**«Межсетевой экран в комплекте с лицензиями (подписками)»**

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Структура** | **Примечание** |
| **1.** | **Наименование товара, работы, услуги** | **Межсетевой экран в комплекте с лицензиями (подписками)** |
| **2.** | **Наименование национальных стандартов.** | **ГОСТ 30804.3.2-2013** «Совместимость технических средств электромагнитная. Эмиссия гармонических составляющих тока техническими средствами с потребляемым током не более 16 А (в одной фазе). Нормы и методы испытаний» |
| **3.** | **Год выпуска** | Не ранее 2021г. |
| **4.** | **Гарантийный срок** | Не менее 12 месяцев |
| **5.** | **Описание требуемых функциональных, технических,**  **качественных, эксплуатационных и иных характеристик закупаемого товара** | **Комплектация:**  1. Межсетевой экран – 1 комплект;  2. Кабель питания 220В не менее, чем 1,5 метра;  3. Ушки для монтажа в стойку;  4. Документация.  **Форм фактор:** не более 1U,с поддержкой монтирования в стойку 19 дюймов;  **Технические требования к межсетевому экранированию:**   * минимальная производительность:   Пропускная способность брандмауэра (1518/512/64 байт UDP(протокол пользовательских датаграмм)): не ниже, чем 30/29/23 Гбит\с;  Одновременное количество сессий: не ниже, чем 3.7 Млн;  Скорость установки новых соединений: не ниже, чем 430 000 в сек.;  Пропускная способность IPS Enterprise Mix: не ниже, чем 7.7 Гбит\с;  Пропускная способность управления приложениями (HTTP 64K): не ниже, чем 11 Гбит\с;  Пропускная способность в режиме защиты от угроз (включены все профили безопасности): не ниже, чем 5 Гбит\с;  Количество виртуальных контекстов безопасности в базовой комплектации: не ниже, чем 10;  Количество интерфейсов: не менее, чем 16x GE SFP, 16x GE RJ45;  Количество выделенных менеджмент портов: не менее, чем 1;  Количество USB портов: не менее, чем 1;  Блок питания от 100 до 240В AC  **Управление:** Должен поддерживать SSH, HTTP, HTTPS;  **Электропитание:** от 100 до 240В AC (от 50 до 60HZ).  **Отказоустойчивость**: поддержка резервирования в режимах Active/Active, Active/Passive.  **Интерфейсы**: не менее 16-и 10/100/1000 Base-T RJ-45 c поддержкой следующих режимов работы: L2, L3, Tap, Virtual wire (transparent mode); не менее 16-и SFP модулей, не менее одного последовательного порта консоли RJ-45; не менее одного USB порта; не менее одного порта высокой доступности; не менее одного 10/100/1000 Base-T RJ-45 порта управления (management port).  **Программные требования к межсетевому экрану:**  лицензирование системы должно осуществляться для неограниченного количества пользователей;   * система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; * система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: * с холодным резервом (active/passive); * с горячим резервом (active/active); * кластер балансировки; * система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений; * система должна иметь функциональность балансировки нагрузки; * система должна поддерживать технологию интеллектуального управления трафиком SD-WAN (Software-Defined Wide Area Network, программно-конфигурируемая сеть); * система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); * система должна обеспечивать инспекцию SSL трафика c возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); * система должна обеспечивать возможность реализации концепции ZTNA (Zero Trust Network Access); * система должна обеспечивать анализ Secure Shell (SSH) трафика (ssh inspection); * система должна обеспечивать динамическую маршрутизацию по протоколам не ниже Internet Protocol v4 и Internet Protocol v6; * система должна иметь возможность работы по протоколу не ниже Web Cache Communication Protocol (WCCP) (как в режиме сервера, так и в режиме клиента); * система должна обеспечивать оптимизацию не ниже Wide Area Network (WAN) соединений; * система должна иметь функционал защиты от утечек данных Data Leak Prevention (DLP); * система должна обеспечивать антивирусную защиту с аппаратным ускорением; * система должна обеспечивать защиту от спама (антиспам); * система должна иметь функциональность предотвращения вторжения не ниже Intrusion Prevention System (IPS) с аппаратным ускорением; * система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; * должна обеспечиваться WEB фильтрация трафика по не менее 85 категориям; * принудительное включение режима безопасного поиска в популярных поисковых системах; * система должна иметь функциональность контроля приложений; * система должна иметь функциональность WEB proxy; * система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных межсетевых экранов внутри одного устройства), доступных по умолчанию; * система должна иметь возможность проверки на наличие вирусов внутри не ниже HTTP, SMTP, POP3, IMAP, FTP и IM трафика; * система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; * система должна иметь возможность помещать инфицированные сообщения в карантин; * система должна иметь возможность блокировки передачи файлов в зависимости от размера и типа; * система должна поддерживать соединения множества (Wide Area Network) WAN сетей; * система должна поддерживать протокол не ниже, чем PPPoE и L2TP; * система должна поддерживать не ниже, чем DHCP протокол в конфигурации “Клиент/Сервер”; * система должна поддерживать маршрутизацию на основе политик; * система должна поддерживать динамическую маршрутизацию на основе протоколов не ниже RIP v1 и v2, OSPF, BGP; * система должна поддерживать использование зон безопасности; * система должна поддерживать маршрутизацию между зонами; * система должна поддерживать маршрутизацию между виртуальными сетями; * система должна поддерживать администрирование на основе ролей; * система должна поддерживать несколько уровней администраторов и пользователей; * система должна поддерживать обновление встроенного программного обеспечения через протокол не ниже, чем TFTP и web-интерфейс; * система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного программного обеспечения; * система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; * система должна поддерживать сетевой протокол аутентификации (Kerberos) пользователей; * система должна поддерживать аутентификацию пользователей посредством не ниже Windows Active Directory; при этом аутентификация пользователей операционных систем не ниже Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей; * система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; * система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; * система должна поддерживать аутентификацию на основе групп пользователей; * система должна поддерживать функции не ниже, чем NAT, PAT, «прозрачный» (мост); * система должна поддерживать функции не ниже, чем NAT на основе политик; * система должна поддерживать функции не ниже, чем VLAN Tagging (802.1Q); * система должна поддерживать функции не ниже, чем SIP/H.323 NAT Traversal; * система должна поддерживать настройку профилей безопасности; * система должна иметь возможность блокировки по URL/ключевому слову/фразе; * система должна поддерживать «Белые» списки URL; * система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; * система должна уметь предотвращать не менее 10000 типов сетевых атак; * система должна иметь возможность настройки списка сигнатур атак; * система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; * система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; * система должна поддерживать проверку заголовков MIME; * система должна поддерживать фильтрацию электронной почты по ключевым словам и фразам; * система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; * система должна иметь возможность отсылки логов на удаленный syslog сервер; * система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; * система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; * система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках; * система должна поддерживать протокол не ниже, чем VRRP; * система должна поддерживать интеграцию с SIEM; * система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; * система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; * система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; * система должна поддерживать управление через Web интерфейс; * система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; * система должна поддерживать протоколы не ниже, чем NetFlow, sFlow; * система должна обеспечивать режим обратного прокси-сервера (reverse proxy); * система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); * система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; * система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях; * система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа; * система должна обеспечивать возможность управления беспроводными точками доступа; * система должна обеспечивать возможность управления коммутаторами;   **C межсетевым экраном должны иметься предустановленные подписки:**  1. IPS система обнаружения и предотвращения вторжений должна анализировать трафик и выявлять аномалии в сети на основе базы данных, которая должна ежедневно обновляться в автоматическом режиме. Должна поддерживаться возможность создания собственных сигнатур.  2. Антивирус - в режиме реального времени должен обеспечивать определение и нейтрализацию вирусов и вредоносного кода на традиционных и мобильных платформах. Антивирусные сигнатуры должны обновляться автоматически.  3. Web&Video filtering должен обеспечивать фильтрацию нежелательных URL и видео на основании глобальной базы данных. База должна обновляться ежедневно и быть разделена на категории для быстрой и удобной настройки. Должна быть возможность ограничения использования определенных сайтов и видео каналов.  4. Антиспам должен проверять почтовые службы (SMTP, POP3, IMAP) и нейтрализовать СПАМ на основе IP репутации и собственных сигнатур. Обеспечивать настройки параметров фильтрации и возможность создания белых и черных списков адресов.  5. Подписка на сервис песочницы для изоляции вредоносного кода служба загружает и анализирует на неизвестные угрозы файлы, которые среда эмуляции отмечает, как подозрительные или легитимные.  6. Подписка на службу поддержки 24/7 должна обеспечивать возможность обновления программного обеспечения, обращения в техподдержку производителя для открытия и сопровождения тикетов, технических консультаций по работе с оборудованием, а также опережающей замены оборудования в случае выхода из строя. |
| **5.** | **Сопутствующие услуги** | В стоимость межсетевого экрана должны быть включены: доставка, монтаж, а также обучение ответственного сотрудника заказчика. |
| **6.** | **Требования к поставщику** | В составе конкурса Потенциальный поставщик должен предоставить авторизационное письмо от производителя либо его официального представителя (дилера или дистрибьютора) указанного в технической спецификации Потенциального поставщика. |