Запрос № **14/2024**

на предоставление ценовой информации
по приобретению
комплекса межсетевых экранов

Размещен на сайте Фонда «11» июля 2024 г.

Фонд социальной защиты населения Министерства труда и социальной защиты Республики Беларусь (далее – Фонд) в рамках исследования конъюнктуры рынка товаров (работ, услуг) и определения предельной стоимости на их поставку (выполнение, оказание) просит в срок до **16 июля 2024 года**:

рассмотреть запрос на предоставление ценовой информации на поставку комплекса межсетевых экранов в объеме и в соответствии с Требованиями к поставляемому комплекту оборудованию (Приложение № 1 к настоящему запросу);

предоставить в адрес Фонда ценовую информацию о предельной стоимости по форме, согласно приложению № 2.

Подготовленная ценовая информация о предельной стоимости товаров (работ, услуг) может быть направлена в адрес Фонда:

посредством системы межведомственного документооборота;

по почте или нарочно (220026, г. Минск, пр-т Партизанский, 52а);

по электронной почте (fsp@ssf.gov.by).

Настоящий запрос № 14/2024 от 11.07.2024, в том числе размещен на интернет-сайте Фонда (адрес сайта: http://ssf.gov.by/) в закладке «Закупки» раздела «О Фонде».

Приложения: 1. Требования к поставляемому комплекту оборудованию на 11 л. в 1 экз.;
2. Форма ценовой информации на 1 л. в 1 экз.;

Управляющий Фондом Ю.Н.Бердникова

Жданович 3610558

Приложение 1

Комплект поставки должен включать в себя следующие компоненты:

Наименование	К-во шт.
Программный комплекс для управления межсетевыми экранами	1
Межсетевой экран Тип 1	2
Межсетевой экран Тип 2	2

Допускается только новое, не бывшее ранее в эксплуатации, демонстрационном тестировании и не восстановленное оборудование.

Расчет цены должен содержать все расходы, связанные с приобретением и пуско-наладочными работами предмета закупки, включая транспортировку, разгрузку, страховку, уплату таможенных пошлин, налогов, сборов и другие обязательные платежи в республиканский и (или) местные бюджеты, в том числе государственные целевые бюджетные фонды, государственные внебюджетные и инновационные фонды.

Комплекс работ:

1. Развертывание системы управления на базе виртуальной машины.
2. Развертывание 2-х кластеров межсетевых экранов и подключение их к системе управления.
3. Реализация схемы горячего резервирования модулей межсетевого экрана, обеспечивающей, в случае отказа одного из них, сохранение текущих сетевых соединений.
4. Настройка функциональных модулей Identity Awareness, IPS, Application Control, URL Filtering, Threat Prevention (AntiVirus, AntiBot).
5. Интеграция кластеров в существующую инфраструктуру организации.
6. Ввод в промышленную эксплуатацию.

Комплекс работ по базовому внедрению кластера из 2 межсетевых экранов и программно-аппаратного комплекса для управления межсетевыми экранами должен включать в себя:

6.1. Настройка базовых политик согласно Best Practice от производителя (примерно 7–10 политик контроля доступа и один профиль защиты от угроз). Настройка базовой связности (выход внутренних пользователей через Hide NAT/Proxy + публикация одного внутреннего сервиса через Static NAT наружу + настройка инспекции HTTPS трафика).

6.2. Установка/обновление менеджмента до актуальной версии, все в одном, настройка сети, DNS, NTP

6.3. Установка/обновление 2 шлюзов до актуальной версии, настройка сети, маршрутизации, топологии, объединение в кластер, подключение к менеджменту

6.4. Подключение лицензий и контрактов, включение всего функционала (NGTP/NGTX), интеграция с Active Directory

6.5. Настройка обновлений блейдов (IPS, AV, AB, TE/TEX)

Требования к программному комплексу для управления межсетевыми экранами:

1.1. Решение должно обеспечивать функционал централизованного управления безопасностью.

1.1.1. Все приложения безопасности Брандмауэра следующего поколения должны быть управляемыми с центральной консоли GUI. Доступ к системе управления осуществляется посредством защищённого канала и выделенного приложения, устанавливаемого на АРМ администратора системы.

1.1.2. Должна поддерживаться фильтрация подключений к менеджменту на основе хранящегося в системе списка разрешённых IP-адресов устройств и подсетей доверенных пользователей.

1.1.3. Централизованное управление безопасностью должно обеспечивать управление 5 шлюзами.

1.1.4. Приложение для управления безопасностью должно поддерживать учетные записи администраторов на основе ролей. Например, только роли для управления политикой брандмауэра или только роль для просмотра журнала.

1.1.5. Решение должно обеспечивать возможность обеспечения высокой доступности системы управления, используя резервный сервер управления, который автоматически синхронизируется с активным сервером.

1.1.6. Решение должно включать возможность централизованного распространения и применения новых версий шлюзового программного обеспечения.

1.1.7. Решение должно включать инструмент для централизованного управления лицензиями всех шлюзов, контролируемых станцией управления.

1.2. Решение должно обеспечивать механизм обновления во всех приложениях включая IPS, Управление приложениями, URL-фильтрацию, Anti-Bot и Anti-Virus.

1.3. Решение должно обеспечивать функционал Централизованного Протоколирования & Мониторинга.

1.3.1. Система централизованного протоколирования событий должна быть частью системы управления.

1.3.2. Решение должно протоколировать все правила.

1.3.3. У средства просмотра журналов событий должна быть возможность индексированного поиска.

1.3.4. Решение должно иметь возможность протоколирования событий

во всех интегрированных приложениях безопасности на шлюзе (включая виртуальные шлюзы), включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрацию, Anti-Bot, Anti-Virus, Sandboxing.

1.3.5. У системы протоколирования должен быть безопасный канал для передачи данных для предотвращения подслушивания, канал передачи должен быть зашифрован и проходить проверку подлинности.

1.3.6. Журналы событий должны безопасно передаваться между шлюзом и управлением или выделенным сервером журналов и консолью просмотра журналов в компьютере администратора.

1.3.7. Решение должно включать опцию динамического блокирования активного соединения в графическом интерфейсе системы протоколирования событий без необходимости внесения изменений в базу правил.

1.3.8. Решение должно включать настраиваемую установку пороговых значений параметров для выполнения действий при достижении определенных пороговых значений на шлюзе. Действия должны включать: запись события, оповещение, отправка SNMP trap, отправка электронного письма и выполнение определенного пользователем предупреждения.

1.3.9. Решение должно включать предварительно настроенные графики для мониторинга трафика во времени и системных счетчиков: главные правила безопасности, основные пользователи P2P, VPN туннели, сетевой трафик и другая полезная информация. Решение должно обеспечивать возможность создания новых графиков с различными типами диаграмм.

1.3.10. Решение должно поддерживать сегментирование политики безопасности по слоям с возможностью делегирования полномочий разным администраторам с точностью до блоков правил в общей политике.

1.3.11. Решение должно обеспечивать хранение ревизий политик для файрволов следующего поколения с возможностью возврата изменений к предыдущим версиям ревизий.

1.4. Решение должно обеспечивать функционал Централизованной Корреляции событий и Отчетов.

1.4.1. Решение должно иметь возможность корреляции событий из всех приложений, включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, Управление приложениями,

URL-фильтрация, Anti-Bot, Anti-Virus, Sandboxing.

1.4.2. Решение должно включать инструмент для корреляции событий из всех функций шлюза и сторонних устройств.

1.4.3. Приложение корреляции событий должно обеспечивать графическое представление событий на основе времени.

1.4.4. Решение должно включать возможность поиска внутри списка событий, углубления в детали для изучения и расследования инцидентов.

1.4.5. Решение должно включать предопределенные ежечасные, ежедневные, еженедельные и ежемесячные отчеты, в том числе, как минимум, Основные события, Основные источники, Основные пункты назначения, Основные сервисы, Основные источники и их основные события, Основные пункты назначения и их основные события, и Основные сервисы, и их основные события.

1.4.6. Решение должно поддерживать автоматическое распространение отчетов по электронной почте, загрузку на FTP/Веб-сервер и скрипт рассылки внешних пользовательских отчетов.

1.4.7. Решение должно обеспечивать функционал управления рисками и соответствия требованиям (GRC) – лучших практик безопасности.

1.4.8. Решение должно обеспечивать оценку соблюдения основных регуляторных требований в режиме реального времени (поддержка стандартов ISO 27001/27002, PCI-DSS, HiPPA, SOX и т.д.).

1.4.9. Решение должно предоставлять рекомендации по реализации лучших практик безопасности.

1.4.10. Решение должно переводить регуляторные требования в инструкции для выполнения лучших практик безопасности.

1.4.11. Решение должно постоянно контролировать конфигурацию шлюза при помощи лучших практик безопасности.

1.4.12. Решение должно генерировать автоматические отчеты по оценке для определения рейтинга соответствия регуляторным требованиям.

1.4.13. Решение должно полностью интегрироваться в Архитектуру программного обеспечения и Инфраструктуру управления.

1.4.14. Решение должно обеспечивать мгновенное уведомление об изменениях политики, влияющих на соответствие регуляторным требованиям.

1.5. Технические требования к системе централизованного управления.

1.5.1. Система централизованного управления должна быть выполнена в виде программного комплекса, который может устанавливаться на сервер в качестве основной операционной системы или на

виртуальную машину. Минимальные системные требования для установки:

- Не менее 6 ядер CPU
- Не менее 32 Гб ОЗУ
- Не менее 2 Тб HDD

1.6. Поддержка и подписка.

1.6.1. Поддержка и подписка сроком на 3 года от производителя, 9x5, должны быть включены все необходимые подписки на сервисы безопасности.

1.7. На момент поставки программный комплекс для управления межсетевыми экранами должен соответствовать требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)

Требования к межсетевому экрану Тип 1 (кол-во 2 шт.):

1.1. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.

1.2. Решение должно поддерживать DHCP, сервер и relay.

1.3. Решение должно включать в себя возможность работы в режиме Transparent/Bridge.

1.3.1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).

1.3.2. Решение должно поддерживать Firewall, IPS, URL-фильтрацию, Antibot, Antivirus, Управление приложениями, Identity Awareness

1.3.3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.

1.4. Решение должно поддерживать политику, основанную на QoS.

1.4.1. Решение должно позволять, гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

1.4.2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

1.5. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

1.5.1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

1.6. Решение должно обеспечивать функционал Идентификации пользователей.

1.6.1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

1.6.2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

1.6.3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

1.7. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

1.7.1. База данных управления приложениями должна содержать свыше 9300 известных приложений.

1.7.2. Решение должно обеспечивать детальный контроль безопасности минимум для 255700 Web 2.0 виджетов.

1.7.3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

1.8.Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

1.8.1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.

1.8.2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.

1.8.3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.

1.8.4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик.

1.9.Решение должно обеспечивать функционал IPSEC VPN.

1.9.1. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.

1.9.2. Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.

1.9.3. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5

(1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20

1.9.4. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC

1.9.5. Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:

1.9.5.1. Полносвязная сеть (все-со-всеми),

1.9.5.2. Звездообразная сеть (удаленные офисы к центральному сайту)

1.9.5.3. Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт)

1.10. Удаленный мобильный доступ

1.10.1. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 200 одновременных соединений пользователей.

1.10.2. Решение должно обеспечивать функционал безклиентного VPN: плагин, который обеспечивает удаленный доступ с предоставлением полной возможности сетевого соединения для IP-приложений. Решение должно обеспечивать функционал SSL VPN 3-уровня по запросу для подключения к корпоративным ресурсам. Решение должно поддерживать любое IP-приложение, включая ICMP, TCP и UDP, не требуя сложной конфигурации для поддержки каждого приложения. Он должен работать на удаленных компьютерах, не требуя прав администратора.

1.10.3. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации.

1.10.4. Решение должно реализовать функционал интегрированной системы предотвращение вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг, настраиваемый модуль блокирования HTTP червей, защиту от обхода каталога (directory traversal), защиту от отклонения заголовков (header rejection), защиту от вредоносного HTTP-кода.

1.10.5. В целом, решение должно обеспечивать следующие функции:

1.10.5.1. Безопасный VPN доступ

1.10.5.2. Ассоциирование мобильных устройств с конечными пользователями

1.10.5.3. Обеспечение соответствия конечных точек соединения корпоративной политике

1.11. Аппаратные и рабочие требования к шлюзу:

- 1 x 1GbE copper/fiber DMZ port
- 1x 1GbE WAN port
- 8x 1GbE LAN switch
- 1x USB-C console port
- 1x USB 3.0 port
- xDSL порт
- 1x (12V power connector) External Power supply

1.11.1. Продуктивные сетевые интерфейсы (минимальные требования):

1.11.2. Пропускная способность Firewall: минимум 2.8 Гбит/с.

1.11.3. Пропускная способность IPS: минимум 1050 Мбит/с

1.11.4. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 970 Мбит/с

1.11.5. Одновременные соединения: минимум 500 000.

1.11.6. Новые соединения: минимум 15 750 в секунду.

1.11.7. Поддержка MicroSD карты расширения памяти.

1.12. Поддержка и подписка.

1.12.1. Поддержка и подписка сроком на 3 год от производителя, 9x5, гарантийная замена оборудования, должны быть включены все необходимые подписки на сервисы безопасности.

Требования к межсетевому экрану Тип 2 (кол-во 2 шт.):

1.1. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.

1.2.Решение должно иметь возможность управления им с программно-аппаратного комплекса для управления межсетевыми экранами.

1.3. Решение должно поддерживать DHCP, сервер и relay.

1.4. Решение должно включать в себя возможность работы в режиме Transparent/Bridge.

1.4.1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).

1.4.2. Решение должно поддерживать Firewall, IPS, URL-фильтрацию, Antibot, Antivirus, Управление приложениями, Identity Awareness

1.4.3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.

1.5. Решение должно поддерживать политику, основанную на QoS.

1.5.1. Решение должно позволять, гарантировать или ограничивать

пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

1.5.2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

1.6. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

1.6.1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

1.7. Решение должно обеспечивать функционал Идентификации пользователей.

1.7.1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

1.7.2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

1.7.3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

1.8. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

1.8.1. База данных управления приложениями должна содержать свыше 9800 известных приложений.

1.8.2. Решение должно обеспечивать детальный контроль безопасности минимум для 255700 Web 2.0 виджетов.

1.8.3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

1.9. Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

1.9.1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.

1.9.2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.

1.9.3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.

1.9.4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик.

1.10. Решение должно обеспечивать функционал IPSEC VPN.

1.10.1. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.

1.10.2. Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.

1.10.3. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20

1.10.4. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC

1.10.5. Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:

- Полносвязная сеть (все-со-всеми),
- Звездообразная сеть (удаленные офисы к центральному сайту)
- Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт)

1.11. Удаленный мобильный доступ

1.11.1. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 500 одновременных соединений пользователей.

1.11.2. Решение должно обеспечивать функционал безклиентного VPN: плагин, который обеспечивает удаленный доступ с предоставлением полной возможности сетевого соединения для IP-приложений. Решение должно обеспечивать функционал SSL VPN 3-уровня по запросу для подключения к корпоративным ресурсам. Решение должно поддерживать любое IP-приложение, включая ICMP, TCP и UDP, не требуя сложной конфигурации для поддержки каждого приложения. Он должен работать на удаленных компьютерах, не требуя прав администратора.

1.11.3. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации.

1.11.4. Решение должно реализовать функционал интегрированной системы предотвращение вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг,

настраиваемый модуль блокирования HTTP червей, защиту от обхода каталога (directory traversal), защиту от отклонения заголовков (header rejection), защиту от вредоносного HTTP-кода.

1.11.5. В целом, решение должно обеспечивать следующие функции:

- Безопасный VPN доступ
- Ассоциирование мобильных устройств с конечными пользователями
- Обеспечение соответствия конечных точек соединения корпоративной политике

1.12. Аппаратные и рабочие требования к шлюзу.

1.12.1. Интерфейсы (минимальные требования):

- 2x 2.5GbE LAN ports
- 16x 1GbE LAN switch
- 2x 10GbE SFP+ LAN ports
- 1x 1GbE copper/fiber WAN port
- 1x 1GbE copper/fiber DMZ port
- 1x SD card slot
- 1x Console port (USB-C or RJ45)
- 2x USB ports
- 2x Power supplies

1.12.2. Пропускная способность Firewall: минимум 20 Гбит/с.

1.12.3. Пропускная способность IPS: минимум 9 Гбит/с.

1.12.4. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 8 Гбит/с.

1.12.5. Одновременные соединения: минимум 4.2 миллиона.

1.12.6. Новые соединения: минимум 90 000 в секунду.

1.13. Поддержка и подписка сроком на 3 года от производителя, 9x5, гарантийная замена оборудования, должны быть включены все необходимые подписки на сервисы безопасности.

1.14. На момент поставки межсетевой экран должен соответствовать требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)

Приложение 2

Реквизиты бланка
(угловой штамп)

Ценовая информация на запрос от 11.07.2024 № 14/2024
(дата и номер исх. письма Фонда)
по приобретению
комплекса межсетевых экранов

_____
(наименование организации)

сообщает, что предельная цена товаров (работ, услуг), в случае поставки их Фонду нашей организацией, соответствующих качественным, техническим и функциональным требованиям, составит:

_____ _____
(сумма цифрами) (сумма прописью)

белорусских рублей (BYN)

в том числе НДС: _____ _____
(сумма цифрами) (сумма прописью)

белорусских рублей (BYN);

Ориентировочный срок поставки с даты заключения логовора:_____дней.

_____ _____ _____
(должность) (подпись) (инициалы, фамилия)
М.П.