**Приложение №2**

**к Договору № \_\_\_**

**от «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_г.**

**Техническая спецификация**

Настоящая техническая спецификация составлена на закуп межсетевого экрана.

1. **Общие требования**

Поставщик должен произвести поставку товара, с удалённой настройкой межсетевых экранов.

1. **Комплект поставки должен включать в себя следующие компоненты:**

|  |  |
| --- | --- |
| **Наименование** | **К-во шт.** |
| Межсетевой экран (Checkpoint 1595) (CPAP-SG1595-SNBT-SS-PREM-1Y 1595 appliance.) | 2 |

1. **Требования к межсетевому экрану.** 
   1. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.
   2. Решение должно поддерживать DHCP, сервер и relay.
   3. Решение должно включать в себя возможность работы в режиме Transparent/Bridge.
      1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).
      2. Решение должно поддерживать Firewall, IPS, URL-фильтрацию, Antibot, Antivirus, Управление приложениями, Identity Awareness
      3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.
   4. Решение должно поддерживать политику, основанную на QoS.
      1. Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.
      2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.
   5. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).
      1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.
   6. Решение должно обеспечивать функционал Идентификации пользователей.
      1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.
      2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.
      3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.
   7. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.
      1. База данных управления приложениями должна содержать свыше 10000 известных приложений.
      2. Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.
      3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.
   8. Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.
      1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.
      2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.
      3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.
      4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик.
   9. Решение должно обеспечивать функционал «песочницы» Sandboxing (инспекция – в облаке или на выделенном локальном устройстве).
      1. Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня.
      2. Топология внедрения песочницы:
         * Поддержка режима сетевой песочницы (network based);
         * Поддержка режима инлайн (bridge mode);
         * Поддержка режима почтового агента (mail transfer agent).
         * Поддержка режима зеркального порта (TAP/SPAN порт).
      3. Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.
      4. Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе специально настроенные образы (customized images).
      5. Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.
      6. Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Mбайт.
      7. Решение должно детектировать атаки на стадии выполнения экслойта (exploitation) – т.е. до того как запускается шелл-код (shell code) и осуществляется загрузка/исполнение самого кода зловредного ПО.
      8. Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.
      9. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.
      10. Решение должно содержать средства борьбы с методиками детектирования исполнения в песочнице.
      11. Решение должно обеспечивать возможность управления им с централизованного менеджмента.
      12. Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.
   10. Решение должно обеспечивать функционал IPSEC VPN.
   11. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.
   12. 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. 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
       2. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC
   13. Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:
       1. Полносвязная сеть (все-со-всеми),
       2. Звездообразная сеть (удаленные офисы к центральному сайту)
       3. Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт)
   14. Удаленный мобильный доступ
       1. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 200 одновременных соединений пользователей.
       2. 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.
       3. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации.
       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 обход каталога (directory traversal), защиту от отклонения заголовков (header rejection),защиту от вредоносного HTTP-кода.
   15. Аппаратные и рабочие требования к шлюзу.
       1. Продуктивные сетевые интерфейсы (минимальные требования):
          1. 1х1 Гбит/с медный WAN порт
          2. 1х1 Гбит/с медных/оптических DMZ порт
          3. 8x1 Гбит медных LAN портов
          4. 1 слот для SD карты
          5. 1 консольный порт
          6. 1 USB порт
   16. Пропускная способность Firewall: минимум 2.8 Гбит/с.
   17. Пропускная способность IPS: минимум 1.4 Гбит/с.
   18. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 1300 Мбит/с.
   19. Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): минимум 660 Мбит/с.
   20. Одновременные соединения: минимум 1 000 000.
   21. Новые соединения: минимум 21 000 в секунду.
   22. Поддержка и подписка.
       1. Поддержка и подписка сроком на 1 год от производителя, 24x7, гарантийная замена оборудования, должны быть включены все необходимые подписки на сервисы безопасности.
2. **Требования к поставщику**
   1. После поставки товара произвести удалённую настройку межсетевых экранов на виртуальном сервере управления Checkpoint SmartConsole, совместно с заказчиком.
3. **Место и условия поставки:**

Условия поставки DDP г. Актобе, пр. Абилкайыр хана 10.