**Основно училище „Васил Евстатиев Априлов“,с. Хърлец, общ. Козлодуй, обл. Враца**
село Хърлец, ул.”Антим I” № 2
email: v.aprilov@abv.bg

**ПОКАНА ЗА ПРЕДОСТАВЯНЕ НА ОФЕРТА**
**От Любимка Василева Ламбова –**
**Директор на ОУ”Васил Априлов” с.Хърлец**

Относно: Предоставяне на оферта от доставчици за изграждане на безжична мрежа в училището, съобразено с изискванията за изграждане на безжични мрежи, публикувани на сайта на МОН , в рубрика „Програми и проекти”- „Изграждане на безжични мрежи за нуждите на държавните и общински училища за 2019г.-начални и основни училища”. Предложените варианти от доставчиците на услугата, трябва да покриват изискванията за изграждане на безжични тип WI-FI мрежи. Офертите да отговарят на задължителни минимални изисквания към компонентите на архитектурата приложени в програмата. Офертите могат да бъдат изпращани по пощата на адрес: с.Хърлец, ул.”Антим 1 „ №2 ОУ”Васил Априлов”, по електронната поща: v.aprilov@abv.bg и лично в сградата на училището – кабинет „Счетоводство”, всеки делничен ден от 08:00 часа до 17:00 часа, считано от 14.03.2019г. до 22.03.2019г.

**Приложение:**

1.Изисквания към компонентите на архитектурата

**С УВАЖЕНИЕ:**
**ЛЮБИМКА ЛАМБОВА**
**ДИРЕКТОР**
**ОУ”ВАСИЛ АПРИЛОВ”**
**С.ХЪРЛЕЦ**

## Задължителни минимални изисквания към компонентите на архитектурата

| № | Наименование | Минимални технически характеристики |
|---|---|---|
| 1. | **Защитна стена (NGFW)- тип 1**<br><br>***(за училища, в които покритието на стаите, може да се осигури с до 6 точки за достъп)** | • *Минимум 4 LAN и 2 WAN порта*<br>• *Всички портове да са RJ45,10/100/1000T*<br>• *Пропускателна способност на защитната стена - минимум - 1 Gbit/s съгласно RFC 2544 (1 518 байтови UDP пакети)*<br>• *IDP пропускателна способност (с контрол на приложенията) - минимум 150 Mbps*<br>• *Антивирусна пропускателна способност - минимум 90 Mbit/s*<br>• *VPN пропускателна способност - минимум 180 Mbit/s*<br>• *Конкурентни сесии -100 000*<br>• *Възможност за управление на безжични точки за достъп (AP) - минимум 6 AP*<br>• *Методи за удостоверяване - local, RADIUS, AD, LDAP, TACACS+, Captive portal, двуфакторна автентикация (SSL VPN, Потребителски портал, Администраторски портал)*<br>• *Защита от проникване - поддръжка на дефинирани от потребител IDP сигнатури, блокиране на опити за свързване към Command&Control сървъри, DNS, AFC и firewall*<br>• *Уеб сигурност:*<br>- *възможност за гъвкави политики чрез предупреждение, забрани, разрешения по протоколи, различни действия за HTTP и HTTPs, базирани на потребители, групи, времеви интервали и квоти*<br>- *антивирусна защита - посещаване на заразени сайтове, изтегляне на заразени файлове, блокиране на файлове, които не могат да бъдат сканирани*<br>• *Сигурност на електронната поща - антиспам и анти фишинг защита, филтриране на мейли на база проверка на съдържание, проверка на ключови думи, проверка на прикачени файлове, сканиране за вируси в прикачени файлове за SMTP, POP3, IMAP*<br>• *Защита и контрол на приложения*<br>• *Защита на web сървъри (WAF)*<br>• *Мрежова възможности:*<br>- *инспектиране на пакети - „дълбоко" инспектиране на пакетите*<br>- *маршрутизация - Статични, Dynamic - BPG, OSPF, RIP,*<br>- *възможност за работа в различни режими - Bridge - трансперантен (STP, ARP и VLAN forwarding), Router - gateway*<br>- *Virtual Private Networks - VLAN*<br>- *поддръжка на DHCP - Server и Relay*<br>- *превенция на атаки за отказ от услуги - DoS, DDoS и portscan*<br>- *управление на множество WAN връзки - Failover/ Loadbalance с различна тежест,*<br>- *възможност за автоматично превключване*<br>- *приоритизация на трафика - Quality of Service (QoS), квоти*<br>- *Voice over IP (VoIP) оптимизация - Real-Time*<br><br>• Виртуални мрежи VPN Отдалечени потребители -SSL, IPsec, L2TP, TLS, DES, AES<br><br>• Виртуални мрежи VPN Site to Site:<br>- *SSL - RDP, HTTP, HTTPS, SSH, SMB, VNC*<br>- *IPsec - IKEv1 и IKEv2 - X.509 cert. и PSK*<br>- *GRE*<br>- *TLS*<br>- *DES*<br>- *AES* |

| | | |
|---|---|---|
| | | • *Управление и администрация*<br>- *:Уеб интерфейс, command line (CLI), конзолен порт*<br>- *Инструменти за диагностика - Packet Capture, графики*<br>- *Възможност за централизирано управление - Облачно базирано*<br>- *Възможност за интеграция с други услуги - API*<br><br>• ***В случаите, когато защитната стена изисква абонамент за определени функционалности, изисквани като минимални, абонамента трябва да покрива минимум 3 годишен период!*** |
| 2. | **Защитна стена (NGFW)- тип 2**<br><br>***(за училища, в които за осигуряване покритието на стаите са необходими над 6 точки за достъп)** | • Минимум 4 LAN/DMZ порта, 2 WAN порта, 1 LAN/WAN/DMZ конфигурируем порт<br>• Всички портове да са RJ45, 10/100/1000T<br>• Пропускателна способност на защитната стена - минимум - 1,9 Gbit/s съгласно RFC 2544 (1 518 байтови UDP пакети)<br>• IDP пропускателна способност (с контрол на приложенията) - минимум 650 Mbps<br>• Антивирусна пропускателна способност - минимум 500 Mbit/s<br>• VPN пропускателна способност - минимум 500 Mbit/s<br>• Конкурентни сесии - 200 000<br>• Възможност за управление на безжични точки за достъп (AP) - минимум 20 AP<br>• Методи за удостоверяване - local, RADIUS, AD, eDirectory, LDAP, TACACS+, Captive portal, двуфакторна автентикация (SSL VPN, Потребителски портал, Администраторски портал)<br>• Защита от проникване - поддръжка на дефинирани от потребител IDP сигнатури, блокиране на опити за свързване към Command&Control сървъри, DNS, AFC и firewall<br>• Уеб сигурност:<br>- *възможност за гъвкави политики чрез предупреждение, забрани, разрешения по протоколи, различни действия за HTTP и HTTPs, базирани на потребители, групи, времеви интервали и квоти*<br>- *антивирусна защита - посещаване на заразени сайтове, изтегляне на заразени файлове, блокиране на файлове, които не могат да бъдат сканирани*<br>• Сигурност на електронната поща - антиспам и анти фишинг защита, филтриране на мейли на база проверка на съдържание, проверка на ключови думи, проверка на прикачени файлове, сканиране за вируси в прикачени файлове за SMTP, POP3, IMAP<br>• Защита и контрол на приложения<br>• Защита на web сървъри (WAF)<br>• Мрежова възможности:<br>- *инспектиране на пакети - „дълбоко" инспектиране на пакетите*<br>- *маршрутизация - Статични, Dynamic - BPG, OSPF, RIP,*<br>- *възможност за работа в различни режими - Bridge - трансперантен (STP, ARP и VLAN forwarding), Router - gateway*<br>- *Virtual Private Networks - VLAN*<br>- *поддръжка на DHCP - Server и Relay*<br>- *превенция на атаки за отказ от услуги - DoS, DDoS и portscan*<br>- *управление на множество WAN връзки - Failover / Loadbalance с различна тежест,*<br>- *възможност за автоматично превключване*<br>- *приоритизация на трафика - Quality of Service (QoS), квоти*<br>- *Voice over IP (VoIP) оптимизация - Real-Time*<br><br>• Виртуални мрежи VPN Отдалечени потребители -SSL, IPsec, L2TP, TLS, DES, AES<br>• Виртуални мрежи VPN Site to Site:<br>- *SSL - RDP, HTTP, HTTPS, SSH, SMB, VNC*<br>- *IPsec - IKEvl и IKEv2 - X.509 cert. и PSK*<br>- *GRE* |

| | | |
|---|---|---|
| | | - *TLS*<br>- *DES*<br>- *AES*<br><br>• Управление и администрация:<br>- *Уеб интерфейс, command line (CLI), конзолен порт*<br>- *Инструменти за диагностика - Packet Capture, графики*<br>- *Възможност за работа в клъстър - High Availability (Active - Active, Active - Passive)*<br>- *Възможност за централизирано управление - Облачно базирано*<br>- *Възможност за интеграция с други услуги - API*<br><br>***• В случаите, когато защитната стена изисква абонамент за определени функционалности, изисквани като минимални, абонамента трябва да покрива минимум 3 годишен период!*** |
| 3. | **Точка за достъп** | • Минимум 1 порт 1 Gbit(PoE)<br>• Скорост на трансфер на данни - минимум 300 Mbit/s на 2.4 GHz + 800 Mbit/s на 5 GHz<br>• Поддържани протоколи IEEE 802.11a/b/g/n/ac<br>• Поддръжка на минимум 2x2 MIMO<br>• Поддръжка на честотите 2.4 GHz и 5 GHz,<br>• Поддръжка на множество SSID - минимум 8<br>• Поддръжка на 802.1x и RADIUS автентикация<br>• Поддръжка на управление от контролер с автоматично откриване, автоматично задаване на IP адрес, ограничение на брой клиенти, ограничение на трафика<br>• Поддръжка на интелигентен роуминг 802.11k, 802.11v и 802.11r<br>• Работа при температури от 0 до +40 градуса<br>• Възможности за удостоверяване и криптиране на базата на WPA/WPA2-PSK/WEP<br>• Възможност за удостоверяване по MAC адрес и удостоверяване през портал |
| 4. | **Управляем PoE комутатор** | • Минимум 8 порта (10/100/1000 GbE, 802.3at/af PoE+)<br>• Производителност - минимум 10 Mpps<br>• Поддръжка на Jumbo Frame - минимум 9 K<br>• MAC адреси - минимум 8 K<br>• PoE бюджет, общо - минимум 70W<br>• Поддръжка на VLAN |
| 5. | **Комуникационен шкаф** | • Минимални размери на комуникационния шкаф - мин. 9U с дълбочина 450мм |

**<u>Правила за изпълнение:</u>**

- **Решението трябва да включва доставка, монтаж, инсталиране и първоначално конфигуриране на оборудването.**
- **При възможност защитната хардуерна стена да бъде така инсталирана и конфигурирана, че да защитава и съществуващата локална мрежа в училищата, с оглед целесъобразното и пълноценно използване на разходите за лицензи и оборудване.**
- **Първоначалната конфигурация следва да включва като минимум създадени 4 типа потребители - (Примерно - административно управление, учители, ученици и гости),**