Изисквания към изграждане на безжични (тип WiFi) мрежи в начални и основни училища

Архитектура

Предложеното решение трябва да покрива изискванията за професионално решение. Причина за това е нуждата от едновременен достъп на голям брой ученици и учители, голямото количество възможни конкурентни връзки към точките за достъп на малка площ и с висока плътност, наличието на пикове в достъпа към мрежата, нуждата от бърз и надежден достъп, за да се позволи безпроблемното функциониране на учебния процес.

За тази цел предложените архитектури трябва да предлагат стандартните компоненти, налични в професионалните мрежи - защитна стена, контролер и точки за достъп(ТД).

Конфигурация и мениджмънт

Конфигурацията на безжичната мрежа трябва да е лесна. В училището се предполага да има множество точки за достъп , които трябва да могат да бъдат конфигурирани и менажирани централизирано, без да се налага индивидуална настройка на всяка от тях.

При възможност и при наличие на два и повече доставчика на интернет при първоначално конфигуриране на оборудването да бъдат свързани в резервиран режим (Failover или Load balancing).

Сигурност и защитеност

Решението трябва да позволява употребата на интернет филтри за съдържание, за да се предпазят децата от опасно такова. Други важни аспекти са блокирането на различни видове атаки, възможностите за криптиране на връзката, защита от спам. Всички тези защити не трябва да пречат на нормалното функциониране на мрежата при скорост позволяваща безпроблемното протичане на учебния процес. Информационната инфраструктура на училището трябва да бъде защитена от външни атаки чрез използване на „умни“ филтри и списъци за контрол на достъпа.

Задължително следва да бъдат активирани филтри за неподходящо съдържание (насилие, порнография, залагания, торенти и други) при първоначално конфигуриране на оборудването. По преценка на училищната общност, както и за удовлетворяване на образователните потребности на учениците могат да бъдат налагани рестрикции за достъп до социални мрежи, стрийминг, игри и други.

При възможност защитната хардуерна стена да бъде така конфигурирана, че да защитава и съществуващата локална мрежа в училищата, които я имат изградена, с оглед целесъобразното и пълноценно използване на разходите за лицензи и оборудването

Трябва да има възможност за защита на съществуващи в училищата web и пощенски сървъри, за криптиране на комуникацията и тунелна свързаност към регионална или централна точка.

Автентикация

За учениците и учителите трябва да е улеснено връзването към училищната мрежа със

собствени мобилни устройства, посредством логин страница, сертификати, автоматична идентификация на устройства.

Капацитет на мрежата

Мобилните устройства са все по-достъпни и с това концепцията за носене и употреба на собствени устройства в училище и ползването им в учебния процес става все по-актуална. Поради това ключово изискване към мрежата е възможността да се справя с много потребители свързани към мрежата, намиращи се на сравнително малка площ, справяйки се с проблеми свързани с интерференция на каналите. Решението трябва да предлага няколко конфигурации за канали и покрития, за да се опрости инсталацията колкото е възможно повече, но запазвайки сегментирането на трафика, безжичните възможности и производителност.

Изискванията за покритие на безжичната мрежа

Мрежата трябва да предлага покритие **във всички стаи**, в които се провежда учебен процес.

Качество на услугите

Учебният процес не трябва да се накъсва от ненадеждна мрежа. Трябва да се осигури нужната скорост и стабилност, за да може учебният процес да върви гладко.

Решението да позволява дефинирането на групи от потребители и правила за техния достъп.

Също така решението трябва да разрешава определянето на политики спрямо устройството, което се е свързало и апликациите, които създават мрежов трафик, а така също и възможности за приоритизиране на ресурси.

Решението трябва да бъде максимално гъвкаво при методите за удостоверяване, за да може да се интегрира във всякакъв тип мрежови среди без да се усложнява процедурата по добавяне на потребителските профили, дефиниране на политики и тяхното управление.

За да се осигури цялостна защита от неоторизиран достъп до локалната мрежа, е необходимо да се поддържат дефинирани от потребителя сигнатури и блокиране на опити за свързване от страна на сървъри за управление и контрол (C & C сървъри).

Необходимо е решението да предлага Quality of Service (QoS) политики, гарантиращи приоритизирането на трафика. Например апликации с тестове и задачи, матури, образователни видеа, уебинари, конферентни разговори, трябва да могат да се приоритизират.

Мрежа

Мрежата трябва да предлага възможност за създаване на отделни виртуални мрежи за преподавателите и учениците.

Трябва да има възможност за безжично свързване на точки за достъп при липса на кабелно трасе (ако училището разполага с няколко сгради, между които такова трасе е невъзможно).

Подготовка оборудването за изграждане на виртуална частна мрежа (VPN) между учебното заведение и централна точка. Това ще е необходимо за свързване с централният център от данни на МОН.

За да се осигури безпроблемното свързване с локалния доставчик на Интернет и имплементацията на устройството, решението трябва да поддържа различни протоколи за маршрутизация и да осигурява работа в различни режими.

За да се осигури непрекъснатата работа на връзката и в синхрон с плана за изграждане на свързаност до училищата, следва да се предвиди възможност за използване и баланс на няколко външни връзки. Мрежовата свързаност да бъде реализиран с медни кабели, като се спазват максимално допустимите дължини за съответната категория. Кабела за изграждане трябва да има фабрична, неизтриваема маркировка на всеки метър с указан производител, метраж, тип и категория, за която е сертифициран. Минималните изисквания за кабелът са да покрива Cat.5e, AWG24 (number of pairs 4)

Всички кабелни трасета да бъдат изведени в комуникационен шкаф. Същия да осигурява всички възможности (площ, захранване, управление на средата и др.) за пасивните елементи, разположени в него. В шкафа да се предвиди свободно място за монтиране на активно оборудване и бъдещо разширение.

Мрежата да бъде обезпечена с комутатор(и), осигуряващ свързаността на безжичните точки за достъп, както и тяхното захранване(PoE).

Възможности за разширение

Да се предвиди възможност за разширяване на изграденото решение:

- Добавяне на нови ТД
- Добавяне на нови потребители/устройства
- Увеличаване на броя логически мрежи
- Възможност за използване на VoIP телефони
- Създаване на виртуални частни мрежи с повече от една точка

(други училища, регионални центрове и т.н.)

Гаранция

Гарантирана от производителя на оборудването минимум 3 години на хардуерните компоненти.

Обучение

Доставчиците на услугата да предоставят на лицата в училище, които имат задължението да обучат, в писмен вид ръководство/инструкция за управление на мрежата, в което да са указани стъпките за основните дейности – смяна на пароли, добавяне или забраняване на функционалности, добавяне или изключване на потребители, въвеждане на рестрикции за достъп до сайтове с неподходящо съдържание и др.

Задължителни минимални изисквания към компонентите на архитектурата

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

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

		- *TLS* - *DES* - *AES* • Управление и администрация: - *Уеб интерфейс, command line (CLI), конзолен порт* - *Инструменти за диагностика - Packet Capture, графики* - *Възможност за работа в клъстър - High Availability (Active - Active, Active - Passive)* - *Възможност за централизирано управление - Облачно базирано* - *Възможност за интеграция с други услуги - API* ***• 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) • Скорост на трансфер на данни - минимум 300 Mbit/s на 2.4 GHz + 800 Mbit/s на 5 GHz • Поддържани протоколи IEEE 802.11a/b/g/n/ac • Поддръжка на минимум 2x2 MIMO • Поддръжка на честотите 2.4 GHz и 5 GHz, • Поддръжка на множество SSID - минимум 8 • Поддръжка на 802.1x и RADIUS автентикация • Поддръжка на управление от контролер с автоматично откриване, автоматично задаване на IP адрес, ограничение на брой клиенти, ограничение на трафика • Поддръжка на интелигентен роуминг 802.11k, 802.11v и 802.11r • Работа при температури от 0 до +40 градуса • Възможности за удостоверяване и криптиране на базата на WPA/WPA2-PSK/WEP • 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+) • Производителност - минимум 10 Mpps • Поддръжка на Jumbo Frame - минимум 9 K • MAC адреси - минимум 8 K • PoE бюджет, общо - минимум 70W • 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),**

с различни права.

- **Задължително да бъдат активирани филтри за неподходящо съдържание (насилие, порнография, залагания, торенти и други). По преценка на училищната общност, както и за удовлетворяване на образователните потребности на учениците могат да бъдат налагани рестрикции за достъп до социални мрежи, стрийминг, игри и други.филтри за съдържание и приоритизиране на трафика в зависимост от конкретните нужди.**
- **На място следва да се извърши обучение на минимум един служител на възложителя.**
- **Доставчиците на услугата предоставят на лицата в училище, които имат задължението да обучат и на директора ръководство/инструкция за управление на мрежата, в което да са указани стъпките за основните дейности (смяна на пароли, добавяне или изключване на потребители, въвеждане на рестрикции за достъп до сайтове с неподходящо съдържание, приоритизиране на трафика и др.).**

Училищата, определени и утвърдени от МОН следва да изискат по конкурентна процедура оферти от доставчици, които **да съответстват на задължителните минимални изисквания** за изграждане на безжични мрежи.

Изпълнителя, под контрола на възложителя, следва да осигури **оптималното** разходване на полученото финансиране.

На онлайн платформата на МОН за национални програми за развитие на образованието (https://np2018.mon.bg) – „Изграждане и развитие на безжични мрежи за нуждите на държавните и общински училища за 2019 г. – НАЧАЛНИ И ОСНОВНИ УЧИЛИЩА“ директорите на училища подават заявка за проверка на съответствието на оферираното оборудване с минималните технически изисквания.

След приключване на дейностите по изграждане на WiFi, но не по-късно от 31.07.2019 г., директорите на училищата прикачат в платформата разходооправдателен документ и приемо-предавателен протокол. В протокола изрично трябва да е упоменато името на поне един служител от училището, който да е обучен за работа с предложеното решение и да бъдат вписани серийните номера на доставената техника.