ПРИЛОЖЕНИЕ 5

Изисквания към изграждане на безжични (тип WiFi) мрежи в училища, финансирани по НП „Информационни и комуникационни технологии (ИКТ) в системата на предучилищното и училищно образование“ 2017

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.

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.

Трябва да има възможност 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. Заради 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.

Изискванията за покритие на безжичната мрежа

Мрежата трябва да предлага покритие във всички учебни стаи.

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. Решението трябва да позволява възможности за приоритизиране на ресурси.

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.

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
- Създаване на виртуални частни мрежи с повече от една точка (други училища, регионални центрове и т.н.)

Качество на услугата

Трябва да се подсигури 99% достъпност на безжичната услуга, отговор от поддръжката при наличие на проблем в рамките на 4 часа(в работно време) и време за възстановяване на услугата до 1 работен ден. Поддръжката трябва да е достъпна от понеделник до петък от 8:00 до 18:00

Допълнителни изисквания

Референции с реализирани проекти за безжична мрежа от сходен или по-голям мащаб.

Проект за покриване на конкретното училище с безжична мрежа, изработен с професионален деклариран инструмент, базиран на противопожарния план на училището.

Изисквания към компонентите на архитектурата

Защитна стена

- Минимум 8 порта (GE)
- Пропускателна способност на защитната стена - над 1,5 Gbit/s
- IPS пропускателна способност - минимум 700 Mbit/s
- Латентност – под 40 микросекунди
- SSL VPN пропускателна способност – минимум 30 Mbit/s
- Едновременни сесии – 300 000
- Политики за сигурност – минимум 2500
- Методи за удостоверяване – local, RADIUS, AD, CA, LDAP, Endpoint Security
- Защита от проникване – поддръжка на дефинирани от потребител IPS сигнатури, защита от минимум 2500 сигнатури идентифициращи атаки
- Уеб сигурност – филтриране на URL адреси, чрез проверка в база данни. Да предоставя защита срещу атаки базирани на уеб приложения, Cross Site Scripting, SQL инжекции
- Сигурност на електронната поща – Антиспам 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
- Мрежова сигурност – защита срещу DDoS атаки, SYN Flood, SYN ACK Flood, TCP Flood, UDP Flood. Да се поддържа SSL VPN, IPSec VPN,

Контролер

- Минимум 8 порта (GE)
- Поддръжка на ACL
- Поддръжка за виртуални мрежи
- Поддържани стандарти - IEEE 802.11a/b/g/ac/n
- Роуминг – поддръжка на роуминг Pairwise Master Key(PMK) с буфериране и rapid key negotiation
- Точките за Достъп трябва да могат да бъдат директно свързани към контролера
- Контролерът трябва да предлага графичен/уеб интерфейс за управление, мониторинг и диагностика на безжичната мрежа
- Идентификация на трафика от и към различните приложения

- Контролерът трябва да поддържа архитектурните сценарии за bridge, bypass и inline архитектури
- Контролерът трябва да поддържа автентикация на потребителите през портал
- Трябва да има възможност за ребалансиране на потребителите между няколко точки за достъп.
- Възможност за калибриране и рекалибриране на сигнала на ТД с цел да се постигне най-добър сигнал спрямо външни съобщения и съседните ТД.
- Възможност за WDS свързаност на места, където не може да бъде постигната твърда свързаност.

Точка за достъп

- Минимум 2 порта (GE)
- Скорост на трансфер на данни над 1 Gbit/s
- Поддържани протоколи IEEE 802.11a/b/g/ac/n
- Поддръжка на честотите 2.4 GHz и 5 GHz,
- Поддръжка на 2x2 MIMO
- Поддръжка на 802.11 DFS
- Поддръжка на WDS
- Поддръжка на интелигентен роуминг 802.11k и 802.11v
- Поддръжка на WIDS/WIPS
- Възможност за избягване на смущения и интерференции
- Работа при температури от -10 до +40 градуса
- Дефиниране на приоритети на база на потребителски роли
- Възможност за дефиниране на приоритети на база съдържание
- Динамично регулиране на широколентовия трафик
- Възможности за удостоверяване и криптиране на базата на WPA/WPA2-PSK/WEP
- Възможност за удостоверяване по MAC адрес и удостоверяване на портал
- Възможност за разпределяне на потребителите между точките за достъп на база на броя на потребителите.
- Сертификация от WIFI Alliance акредитирана от интернационална институция като Гартнер или подобна.
- Сертификация за безопасност (RoHS)