**Załącznik numer 4 do SWZ**

**Cześć 1 : Licencja do zapory antyspamowej**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Roczna licencja FortiCare oraz ATP dla Fortimail VM-01SN: FEVM01TM24001326 | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 1 sztuki | Spełnia / nie spełnia |

**Cześć 2 : Licencja do zapory sieciowej**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Roczna licencja UTP Bundle dla dwóch urządzeń FortiGate 121GSN: FG121GTK24000360SN: FG121GTK24000061 | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 2 sztuk ( po jednej dla każdego urządzenia) | Spełnia / nie spełnia |

**Cześć 3 : Licencje wsparcia technicznego dla przełącznika sieciowego**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Poziom usługi oferowanego wsparcia Juniper Networks, musi zapewnić dostęp do kluczowych zasobów niezbędnych do utrzymania sprawności i aktualności infrastruktury sieciowej w terminie od 14.05.2025r. dla przełączników 1-8 oraz w terminie od 13.11.2025r. dla przełączników 9,10. Przedłużenie obecnego wsparcia do dnia 12.11.2026r. W ramach oferowanej usługi musi być zapewnione:* Całodobowy dostęp do Juniper Technical Assistance Center (JTAC): Możliwość kontaktu z inżynierami wsparcia technicznego 24 godziny na dobę, 7 dni w tygodniu.
* Aktualizacje oprogramowania: Nieodpłatny dostęp do najnowszych wersji oprogramowania oraz poprawek w okresie świadczenia usługi.
* Dostęp do portalu wsparcia Juniper: Możliwość korzystania z zasobów online, takich jak bazy wiedzy, dokumentacja techniczna oraz narzędzia diagnostyczne.

1 - NY48233906002 - NY48233905993 - NY48233903664 - NY02203005085 - NY48233906816 - NY48233903177 - NY48233905008 - NY48233905159 - NY482423023210 - NY4824230526 | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 10 sztuk ( po jednej dla każdego urządzenia) | Spełnia / nie spełnia |

**Cześć 4 : Rozszerzenie licencje dla Autentykatora MFA Duo Mobile w wersji Essentials**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Rozszerzenie obecnej licencji o 20 użytkownikówID: 1177-5629-96 | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w postaci licencji wystawionej przez dystrybutora/producenta poświadczającego legalność produktu | Spełnia / nie spełnia |

**Cześć 5 : Rozszerzenie licencje dla Eset Protect w wersji Enterprise**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Rozszerzenie obecnej licencji o 20 urządzeńidentyfikator publiczny: 3BA-2KT-9S3 , do końca trwania obecnej licencji tj: 19.11.’26r.Termin rozpoczęcia licencji: 01.05.2025r. | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w formie odpowiedniego certyfikatu wystawionego przez dystrybutora/producenta poświadczającego legalność produktu (certyfikat w formie PDF).  | Spełnia / nie spełnia |

**Cześć 6 : Licencja Microsoft Office 2024 dla serwera usług terminalowych Windows Server 2025**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Wymagania ogólne | Wieczysta licencja dla 5 użytkowników | Spełnia / nie spełnia |
| Licencje muszą pochodzić od oficjalnego polskiego dystrybutora | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 5 sztuk | Spełnia / nie spełnia |

**Część 7 : Akcesoria sieciowe**

* 1. – Wkładki światłowodowe SFP28

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Rodzaj wkładki | SFP28 | Spełnia / nie spełnia |
| Przepustowość | 25 Gb/s | Spełnia / nie spełnia |
| Długość fali: | Tx 850 nmRx: 850 nm | Spełnia / nie spełnia |
| Minimalny zasięg transmisji | 1m | Spełnia / nie spełnia |
| Maksymalny zasięg transmisji | 100m | Spełnia / nie spełnia |
| Typ Złącza:  | LC (Duplex) | Spełnia / nie spełnia |
| Kompatybilne włókna optyczne | Multimode | Spełnia / nie spełnia |
| Kombatybilność z urządzeniami producenta | Cisco | Spełnia / nie spełnia |
| Gwarancja | 2 lata | Spełnia / nie spełnia |
| Stan | Fabrycznie nowy | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 30 sztuk |  |

7.2 – Patchcord światłowodowy

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| Typ złącza | LC, Duplex | Spełnia / nie spełnia |
| Długość | 3m | Spełnia / nie spełnia |
| Typ złącza | LC / UPC | Spełnia / nie spełnia |
| Kompatybilne włókna optyczne | Multimode OM3 | Spełnia / nie spełnia |
| Gwarancja | 2 rok | Spełnia / nie spełnia |
| Stan | Fabrycznie nowy | Spełnia / nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia ww. produkt w ilości 20 sztuk |  |

**Część 8 : Zestaw Komputerowy**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Wymagania** |  |
| **Procesor** | Architektura x86-64 , minimum 25k w teście wielowątkowym PASSMARK, Minimum 6/12 rdzeni wątków, bazowy zegar procesora minimum 2.5 Ghz.Procesor nie może być starszy niż 2 lata (liczony od daty wydania) | Spełnia / Nie spełnia |
| **Pamięć RAM** | 32 GB DDR5, w trybie Dual Channel | Spełnia / Nie spełnia |
| **Dysk** | Typ M2 SSD, Minimum 500 GB, PCI-e 4 gen | Spełnia / Nie spełnia |
| **Karta Graficzna** | Zintegrowana zapewniająca obsługę rozdzielczości 1920x1080 | Spełnia / Nie spełnia |
| **Karta Dźwiękowa** | Karta zintegrowana z płytą główną | Spełnia / Nie spełnia |
| **Karta sieciowa LAN** | Tak, 100/1000 Mbps | Spełnia / Nie spełnia |
| **Bezpieczeństwo** | TPM 2.0 | Spełnia / Nie spełnia |
| **Bios** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:- wersji BIOS wraz z datą jego produkcji- nr seryjnym komputera- ilości zainstalowanej pamięci RAM- typie procesora - Numerze inwentarzowym urządzenia Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - ustawienia hasła administratora- ustawienia hasła dysku twardego- włączenia/wyłączenia wirtualizacji- włączenia/wyłączenia bootowania z USB oraz PXE- zdefiniowania sekwencji bootowania urządzeń- włączenia/wyłączenia karty sieciowej- włączenia/wyłączenia zintegrowanego systemu audio- włączenia/wyłączenia portów USB | Spełnia / Nie spełnia |
| **System operacyjny** | Windows 11 Pro PL | Spełnia / Nie spełnia |
| **Gwarancja**  | 3 lata typu ON-Site producenta na wszystkie komponenty | Spełnia / Nie spełnia |
| **Interfejsy / Komunikacja** | Minimum 1x Port HDMI, 1x port Display Port  | Spełnia / Nie spełnia |
| Minimum 4x USB A  | Spełnia / Nie spełnia |
| **Obudowa** | Stojąca typu Tower lub mini/midi Tower, zapewniająca odpowiednie chłodzenie podzespołów wewnątrz obudowy komputera. | Spełnia / Nie spełnia |
| **Zasilacz** | 230V 50Hz sprawność zasilacza na poziomie 80% przy 20, 50, i 100% obciążeniu. Zasilacz powinien posiadać, po zainstalowaniu wszystkich podzespołów, dodatkowo co najmniej 25% mocy rezerwowej do obsługi dodatkowego wyposażenia. | Spełnia / Nie spełnia |
| **Klawiatura** | Pełnowymiarowa, czytelny i kontrastowy układ w polskim standardzie QWERTY z wydzielonymi klawiszami nawigacyjnymi i klawiaturą numeryczną, przewodowa USB, długość przewodu 1,8m | Spełnia / Nie spełnia |
| **Urządzenie wskazujące** | Mysz optyczna przewodowa USB, długość przewodu minimum 1,8m | Spełnia / Nie spełnia |
| **Monitor** | Przekątna ekranu 23-24” | Spełnia / Nie spełnia |
| Powłoka matrycy matowa | Spełnia / Nie spełnia |
| Rodzaj matrycy LED IPS | Spełnia / Nie spełnia |
| Rozdzielczość natywna 1920x1080 | Spełnia / Nie spełnia |
| Format obrazu 16:9 | Spełnia / Nie spełnia |
| Częstotliwość odświeżania obrazu minimum 60 Hz | Spełnia / Nie spełnia |
| Czas reakcji nie większy niż 5 ms | Spełnia / Nie spełnia |
| Jasność minimum 250 nit | Spełnia / Nie spełnia |
| Wbudowane głośniki | Spełnia / Nie spełnia |
| VESA 100x100 | Spełnia / Nie spełnia |
| Złącza 1x HDMI, 1xDP, 1xVGA | Spełnia / Nie spełnia |
| **Certyfikaty, oświadczenia i standardy** | Dla producenta sprzętu należy dostarczyć certyfikat:- ISO 9001- ISO 14001- ISO 50001Dla komputera:- ENERGY STAR 8.0- EPEAT Gold dla kraju Polska według danych widocznych na stronie https://epeat.net/search-computers-and-displays- Mil-STD-810H- Deklaracja zgodności CE- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki | Spełnia / Nie spełnia |
| **Stan** | Fabrycznie nowy, pochodzący z polskiej dystrybucji | Spełnia / Nie spełnia |
| **Licencje / Ilość** | Zamawiający wymaga dostarczenia ww. produkt w ilości 30 sztuk |  |

**Część 9 : Laptopy**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Parametr** | **Wymagania** |  |
| **Procesor** | Architektura x86-64, niskonapięciowy, minimum 18k w teście wielowątkowym PASSMARK, Minimum 6/12 rdzeni wątków, zegar bazowy minimum 3.2 GhzProcesor nie może być starszy niż 2 lata (liczony od daty wydania) | Spełnia / Nie spełnia |
| **Pamięć RAM** | ~~32 GB DDR5, w trybie Dual Channel,~~ **~~16 GB DDR5~~**~~, Możliwość rozbudowy pamięci do min. 64GB~~min. 16 GB DDR5, możliwość zainstalowania 32GB  | Spełnia / Nie spełnia |
| **Dysk** | Typ M2 SSD, Minimum 500 GB, PCI-e 4 genDysk samoszyfrujący w technologii OPAL 2.0 | Spełnia / Nie spełnia |
| **Ekran** | Matowy, matryca IPS 14” 16:10 z podświetleniem w technologii LED, rozdzielczość WUXGA 1920x1200, 400 nits, kontrast 800:1, matowa, low powerKąt otwarcia pokrywy ekranu min.180 stopni. | Spełnia / Nie spełnia |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio (Stereo 2x2W), port słuchawek i mikrofonu typu COMBO, kamera video ~~5MP~~ FHD/5MP z mechaniczną zasłoną obiektywu, obsługująca logowanie za pomocą danych biometrycznych z Windows Hello, dwa mikrofony 360 stopni, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). | Spełnia / Nie spełnia |
| **Obudowa** | Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H. | Spełnia / Nie spełnia |
| **Karta Graficzna** | Zintegrowana | Spełnia / Nie spełnia |
| **Bluetooth** | Tak, min 5.3 | Spełnia / Nie spełnia |
| **Karta sieciowa LAN** | Tak, 100/1000 Mbps | Spełnia / Nie spełnia |
| **Karta sieciowa bezprzewodowa** | Tak, obsługa Wifi 6e, obsługa WPA2-Enterprise | Spełnia / Nie spełnia |
| **Klawiatura** | Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w min. 2 stopniowe podświetlanie przycisków (włączone, wyłączone). | Spełnia / Nie spełnia |
| **Czytnik linii papilarnych** | Wbudowany czytnik linii papilarnych w przycisku zasilaniaPrzycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury. | Spełnia / Nie spełnia |
| **Bezpieczeństwo** | - TPM 2.0- Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington.- Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. | Spełnia / Nie spełnia |
| **Bios** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:- wersji BIOS wraz z datą jego produkcji- nr seryjnym komputera- ilości zainstalowanej pamięci RAM- typie procesora - Numerze inwentarzowym urządzenia Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - ustawienia hasła administratora- ustawienia hasła dysku twardego- włączenia/wyłączenia wirtualizacji- włączenia/wyłączenia bootowania z USB oraz PXE- zdefiniowania sekwencji bootowania urządzeń- włączenia/wyłączenia karty sieciowej- włączenia/wyłączenia czytnika linii papilarnych- włączenia/wyłączenia zintegrowanego systemu audio- włączenia/wyłączenia portów USB | Spełnia / Nie spełnia |
| **Bateria** | O pojemności min. 50Wh, obsługujący funkcjonalność szybkiego ładowania od 0 do 80% w czasie 60 minut. | Spełnia / Nie spełnia |
| **System operacyjny** | Windows 11 Pro | Spełnia / Nie spełnia |
| **Gwarancja**  | Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site). W przypadku awarii, dysk twardy pozostaje u Zamawiającego. Firma serwisująca posiadająca certyfikat ISO 9001:2000 na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:- fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach.Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera. | Spełnia / Nie spełnia |
| **Interfejsy / Komunikacja** | 4x USB min. 3.2 z czego minimum 2 złącza USB 4, umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 2.1, RJ-45. Wbudowane w obudowę komputera: czytnik kart inteligentnych oraz slot na kartę nano SIM. | Spełnia / Nie spełnia |
| **Łączność mobilna** | Anteny WWAN zintegrowane z obudową komputera.Dedykowany slot pozwalający na rozbudowę urządzenia o moduł 4G. | Spełnia / Nie spełnia |
| **Waga** | Maximum 1,6 kg | Spełnia / Nie spełnia |
| **Zasilacz** | Maximum 65W USB-C | Spełnia / Nie spełnia |
| **Torba** | Torba na ramię z minimum dwoma przekładkami, na zamek błyskawiczny | Spełnia / Nie spełnia |
| **Certyfikaty, oświadczenia i standardy** | Dla producenta sprzętu należy dostarczyć certyfikat:- ISO 9001- ISO 14001- ISO 50001Dla komputera:- ENERGY STAR 8.0- EPEAT Gold dla kraju Polska według danych widocznych na stronie https://epeat.net/search-computers-and-displays- Mil-STD-810H- Deklaracja zgodności CE- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki | Spełnia / Nie spełnia |
| **Stan** | Komputer przenośny.W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.  Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 7 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2022 poz. 1710 ze zm.), z uwagi na fakt, że treść oferty jest niezgodna z warunkami zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek | Spełnia / Nie spełnia |
| **Licencje / Ilość** | Zamawiający wymaga dostarczenia ww. produkt w ilości 10 sztuk. |  |

**Część 10 : Access Pointy**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|   |   | Spełnienie warunków. |
| **Standardy komunikacyjne** | IEEE 802.11g, IEEE 802.11ax, IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11n | Spełnia / Nie spełnia |
| **Obsługa Wifi 6e** | Tak | Spełnia / Nie spełnia |
| **Obsługa Bluetooth** | Tak | Spełnia / Nie spełnia |
| **Pasmo 6 Ghz** | 4x4 MU-MIMO i OFDMA z szybkością radiową 4,8 Gb/s z przepustowością 160 MHz | Spełnia / Nie spełnia |
| **Pasmo 5 Ghz**  | 4x4 MU-MIMO i OFDMA z szybkością radiową 4,8 Gb/s z przepustowością 160 MHz | Spełnia / Nie spełnia |
| **Pasmo 2,4 GHz** | 2x2 MIMO i OFDMA z szybkością radiową 573,5 Mb/s | Spełnia / Nie spełnia |
| **QOS** | Tak | Spełnia / Nie spełnia |
| **DFS** | Tak | Spełnia / Nie spełnia |
| **Montaż** | Sufit | Spełnia / Nie spełnia |
| **Materiał obudowy** | Aluminium / plastik | Spełnia / Nie spełnia |
| **Kolor** | Biały | Spełnia / Nie spełnia |
| **Obsługa POE** | Tak | Spełnia / Nie spełnia |
| **Rodzaj POE** | 802.3at | Spełnia / Nie spełnia |
| **Waga** | Do 1 kg | Spełnia / Nie spełnia |
| **Obsługa** | WPA,WPA-Enterprise, WPA2, WPA2-Enterprise, WPA3, WPA3-Enterprise | Spełnia / Nie spełnia |
| **Dopuszczalna temperatura pracy** | -30 – 60 °C | Spełnia / Nie spełnia |
| **Dopuszczalny zakres wilgotności pracy** | 5-95% | Spełnia / Nie spełnia |
| **Ilość portów Ethernet LAN (RJ45)** | 1, 2.5 Gbps | Spełnia / Nie spełnia |
| **Typ anten** | wewnętrzne | Spełnia / Nie spełnia |
| **Gwarancja** | 2 lata | Spełnia / Nie spełnia |
| **Stan** | Fabrycznie nowy, pochodzący z polskiej dystrybucji | Spełnia / Nie spełnia |
| **Wymagania dodatkowe** | Sprzęt musi być kompatybilny z bieżącym systemem w jednostce - Unifi Controller | Spełnia / Nie spełnia |
| **Licencje / Ilość** | Zamawiający wymaga dostarczenia ww. produkt w ilości 5 sztuk |  |

**Część 11: System uwierzytelnienia dostępu do sieci LAN/WLAN/VPN**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Podstawowe cechy systemu | 1.1 System umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.1.2 System umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.1.3 System umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń.1.4 System umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym na:1.4.1 VMware wersji 8 dla ESXi 5.1 U21.4.2 VMware wersji 11 dla ESXi 6.x1.4.3 WMware Cloud w AWS1.4.4 Azure VMware Solution1.4.5 hypervisorze KVM na Red Hat Enterprise Linux (RHEL)1.4.6 Microsoft Hyper-V1.4.7 AWS EC21.4.7.1 serwerach fizycznych wspieranych przez producenta1.5 System umożliwia wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:1.5.1 Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie1.5.2 Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:1.5.2.1 przełączników dostępowych1.5.2.1.1 sesji uwierzytelniania 802.1X1.5.2.1.2 zdarzeń kontroli dostępu (autoryzacji)1.5.2.1.3 zdarzeń związanych z błędami1.5.2.1.4 zdarzeń związanych z alarmami systemowymi1.5.2.2 Wydzielenie serwerów usługowych realizujących funkcje:1.5.2.2.1 serwera RADIUS dla infrastruktury sieciowej1.5.2.2.2 serwera polityk uwierzytelniania i kontroli dostępu 802.1X1.5.2.2.3 serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego1.5.2.2.4 serwera profilowania stacji końcowych1.6 System umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym:1.6.1 zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu1.6.2 zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych1.7 System umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS.1.8 System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).1.9 System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).1.10 System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.1.11 System umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0.1.12 System umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni1.13 System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:1.15.1 dostęp do interfejsu konfiguracji usług tożsamości 802.1X1.15.2 dostęp do interfejsu konfiguracji urządzeń sieciowych1.15.3 dostęp do interfejsu konfiguracji polityk 1.15.4 dostęp do interfejsu konfiguracji kontroli dostępu gościnnego1.15.5 dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania1.16 System umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.1.17 System posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.1.18 System wspiera REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych.1.19 System wspiera REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych.1.20 System wspiera REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików.1.21 System umożliwia rozbudowanie funkcjonalności o m.in. profilowanie urządzeń oraz weryfikację stanu stacji końcowej– z ang. posture assessment, bez konieczności rozbudowy sprzętowej.1.22 System umożliwia rozbudowanie funkcjonalności o serwer TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej. | Spełnia / Nie spełnia |
| Mechanizmy uwierzytelniania 802.1x | 2.1 System wspiera następujące protokoły uwierzytelniania i standardy: 2.1.1 RADIUS, zgodnie z dokumentami: 2.1.1.1 RFC 2138 — Remote Authentication Dial In User Service (RADIUS) 2.1.1.2 RFC 2139 — RADIUS Accounting 2.1.1.3 RFC 2865 — Remote Authentication Dial In User Service (RADIUS) 2.1.1.4 RFC 2866 — RADIUS Accounting 2.1.1.5 RFC 2867 — RADIUS Accounting for Tunnel Protocol Support 2.1.1.6 RFC 2868 — RADIUS Attributes for Tunnel Protocol Support 2.1.1.7 RFC 2869 — RADIUS Extensions 2.1 RADIUS Proxy dla zewnętrznego serwera RADIUS 2.2 System wspiera protokół Windows Active Directory, w tym następujące repozytoria AD: 2.2.1 Microsoft Windows Active Directory 2003 32bit 2.2.2 Microsoft Windows Active Directory 2003 R2 32bit i 64bit 2.2.3 Microsoft Windows Active Directory 2008 32bit i 64bit 2.2.4 Microsoft Windows Active Directory 2008 R2 64bit 2.2.5 Microsoft Windows Active Directory 2012 2.2.6 Microsoft Windows Active Directory 2012 R2 2.2.7 Microsoft Windows Active Directory 2016 2.2.8 Microsoft Windows Active Directory 2019 2.3 System wspiera protokół Lightweight Directory Access Protocol (LDAP) 2.4 System wspiera protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO). 2.5 System wspiera integrację z Azure Active Directory z użyciem technologii Oauth ROPC w celu uwierzytelnienia klientów 802.1x. 2.6 System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865 2.7 System wspiera następujące protokoły uwierzytelniania: 2.7.1 PAP/ASCII 2.7.2 CHAP 2.7.3 MS-CHAPv1 2.7.4 MS-CHAPv2 2.7.5 EAP-MD5 2.7.6 LEAP 2.7.7 EAP-TLS 2.7.8 EAP-TTLS 2.7.9 Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi: 2.7.9.1 EAP-MS-CHAPv2 2.7.9.2 EAP-GTC 2.7.9.3 EAP-TLS 2.7.10 Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi: 2.7.10.1 EAP-MS-CHAPv2 2.7.10.2 EAP-TLS 2.8 System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect 2.8.1 wbudowanym klientem 802.1X dla Windows 10 2.8.2 wbudowanym klientem 802.1X dla Windows 7 2.8.3 wbudowanym klientem 802.1X dla Windows 8 i 8.1 2.8.4 Apple Mac OS X Supplicant 2.8.5 Apple iOS Supplicant 2.8.6 Google Android Supplicant 2.9 System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based). 2.10 System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników. 2.11 System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły. 2.12 System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym) 2.13 System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC. 2.14 System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC 2.15 System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym: 2.15.1 tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port 2.10 System wspiera implementację 802.1X z przynajmniej następującymi suplikantami:2.15.2 tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia 2.15.3 tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym 2.15.4 tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym 2.15.5 mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny 2.15.6 mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym. 2.15.7 mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA. 2.15.8 mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X 2.15.9 mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X 2.15.10 obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki 2.15.11 mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych 2.15.12 mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny 2.15.13 przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników 2.15.14 uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego sie w VLANie głosowym 2.15.15 współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN 2.15.16 możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web 2.15.17 możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika 2.16 System wspiera uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X) 2.17 System wspiera m.in. następujące urządzenia sieciowe jako klientów RADIUS (NAD - Network Access Device): 2.17.1 Przełączniki Ethernet. 2.17.2 Kontrolery sieci bezprzewodowej. 2.17.3 Koncentratory VPN.  | Spełnia / Nie spełnia |
| Realizacja dostępu gościnnego | 3.1 System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkęinternetową, w tym, między innymi dla:3.1.1 Microsoft Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7,3.1.2 Apple Mac OS X 10.x oraz 11.x3.1.3 Apple iOS 11.x, 12.x, 13.x i nowszych3.1.4 Google Android dla wersji 7.x i nowszych3.1.5 Linux3.2 System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor).3.3 System zapewnia uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:3.3.1 wewnętrzną bazę użytkowników3.3.2 zewnętrzne repozytorium użytkowników3.4 System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:3.4.1 logowania się do systemu3.4.2 tworzenia pojedynczego konta gościnnego3.4.3 tworzenia wielu kont gościnnych3.4.4 importowania kont gościnnych z pliku CSV3.4.5 wysyłania wiadomości email po utworzeniu konta gościnnego3.4.6 wysyłania wiadomości SMS po utworzeniu konta gościnnego3.4.7 wyświetlenia hasła konta gościnnego3.4.8 wydrukowania danych konta gościnnego3.4.9 wyświetlenia danych stworzonych kont gościnnych3.4.10 zawieszenia (suspend) i reinicjacji kont gościnnych3.5 System umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:3.5.1 zmianę logo strony logowania3.5.2 zmianę obrazu tła strony logowania3.5.3 zmianę logo bannera3.5.4 zmianę obrazu tła bannera3.5.5 zmianę koloru tła strony z treścią3.6 System umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP iportu HTTPS3.7 System umożliwia zmianę adresu URL i FQDN strony sponsora.3.8 System umożliwia automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadanąliczbę dni i o określonej godzinie. System umożliwia wyświetlenie czasu ostatniego kasowania wygasłychkont gościnnych i następnego kasowania wygasłych kont gościnnych3.9 System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, conajmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim3.10 System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w językupolskim.3.11 System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcietworzenia konta przez sponsora:3.11.1 Imienia3.11.2 Nazwiska3.11.3 Firmy3.11.4 adresu e-mail3.11.5 numeru telefonu3.11.6 danych opcjonalnych (nie mniej niż 5 dodatkowych pól)3.12 System umożliwia konfigurację dla użytkowników gościnnych:3.12.1 wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)3.12.2 zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,3.12.3 samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora3.13 System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniegowzorca językowego.3.14 System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.3.15 System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej20 urządzeń per konto gościnne.3.16 System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach.3.17 System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważnościkonta gościnnego z dokładnością do daty i godziny3.18 System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych:3.19 System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniejtworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika3.20 System umożliwia tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwąużytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodudostępu.3.21 System umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsuIP, portu HTTPS i certyfikatu SSL dla FQDN.3.22 System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramySMTP, secure SMTP i poprzez SMS,3.23 System umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych orazsponsora.3.24 System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych. | Spełnia / Nie spełnia |
| Raportowanie | 4.1 System umożliwiać generowanie m.in. następujących raportów: 4.1.1 raportów dla protokołów AAA: 4.1.2 diagnostyki protokołów AAA 4.1.3 trendów uwierzytelnienia 802.1X 4.1.4 accountingu RADIUS 4.1.5 uwierzytelniania RADIUS 4.1.6 raportów dozwolonych protokołów 4.1.7 sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym: 4.1.7.1 uwierzytelnień pomyślnych 4.1.7.2 uwierzytelnień nieudanych 4.1.7.3 „N” największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym: 4.1.7.3.1 uwierzytelnień pomyślnych 4.1.7.3.2 uwierzytelnień nieudanych4.1.8 raportów dla poszczególnych instancji serwerów systemu, w tym: 4.1.8.1 uwierzytelnień RADIUS per serwer 4.1.8.2 Top „N” uwierzytelnień per serwer 4.1.8.3 monitorowania Online Certificate Status Protocol (OCSP) 4.1.8.4 administratorów systemu i ich uprawnień 4.1.8.5 logowania administratorów do systemu 4.1.8.6 zmian konfiguracji serwera dokonanych przez administratorów 4.1.8.7 stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS) 4.1.8.8 zmian operacyjnych serwera dokonanych przez administratorów 4.1.8.9 zmian haseł przez użytkowników 4.1.9 raportów dla stacji końcowych, w tym: 4.1.9.1 uwierzytelnień typu MAC Authentication 4.1.9.2 Top „N” uwierzytelnień per adres MAC stacji 4.1.9.3 Top „N” uwierzytelnień per maszyna 4.1.9.4 Top „N” uwierzytelnień per RADIUS Calling Station ID 4.1.9.5 działań podsystemu profilera per adres MAC 4.1.9.6 czasu wymaganego na sprofilowanie stacji per adres MAC 4.1.10 raportów dla błędów, w tym: 4.1.10.1 błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił 4.1.10.2 sumarycznych przyczyn nieudanych uwierzytelnień 4.1.10.3 Top „N” uwierzytelnień per rodzaj błędu 4.1.11 raportów dla urządzeń sieciowych: 4.1.11.1 sumarycznych uwierzytelnień dla urządzeń sieciowych 4.1.11.2 Top „N” uwierzytelnień per urządzenie sieciowe 4.1.11.3 niedostępności serwera AAA dla urządzenia sieciowego 4.1.11.4 wiadomości logowanych przez urządzenia sieciowe 4.1.11.5 stanu portów i sesji urządzenia sieciowego widocznych przez SNMP 4.1.12 raportów użytkowników: 4.1.12.1 sumarycznych uwierzytelnień użytkowników 4.1.12.2 Top „N”uwierzytelnień per użytkownik 4.1.12.3 sesji użytkowników gościnnych 4.1.12.4 aktywności użytkowników gościnnych 4.1.12.5 sumarycznych uwierzytelnień sponsorów dostępu gościnnego 4.1.12.6 uwierzytelnień per unikalny użytkownik 4.1.13 raportów katalogu sesji 4.1.13.1 aktywnych sesji RADIUS 4.1.13.2 historii sesji RADIUS 4.1.13.3 zaterminowanych sesji RADIUS  | Spełnia / Nie spełnia |
| Alarmy i diagnostyka | 5.1 System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą 5.1.1 wiadomości e-mail 5.1.2 syslog 5.2 Alarmy mogą być generowane w następujących sytuacjach: 5.2.1 ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu 5.2.2 opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego 5.2.3 status krytycznych procesów będzie niepożądany, w tym status: 5.2.3.1 procesu wewnętrznej bazy danych systemu 5.2.3.2 serwera aplikacyjnego systemu 5.2.3.3 bazy danych sesji 5.2.3.4 kolektora i procesora wiadomości log 5.2.3.5 błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej) 5.2.3.6 stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym: 5.2.3.6.1 obciążenie systemu (load) 5.2.3.6.2 zajętość pamięci 5.3 System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: 5.3.1 badanie łączności IP za pomocą ping, nslookup, traceroute 5.3.2 wyszukiwanie zdarzeń RADIUS z uwzględnieniem: 5.3.2.1 nazwy użytkownika 5.3.2.2 adresu MAC 5.3.2.3 statusu uwierzytelnienia (udana lub nieudana) 5.3.2.4 powodu, jeżeli uwierzytelnienie nieudane 5.3.2.5 zakresu czasowego, co do dnia, godziny i minuty 5.3.3 wykonanie zdalnego polecenia na urządzeniu sieciowym 5.3.4 ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: 5.3.4.1 definicji serwerów AAA 5.3.4.2 protokołu RADIUS 5.3.4.3 odkrywania urządzeń 5.3.4.4 logowania 5.3.4.5 uwierzytelniania Web 5.3.4.6 konfiguracji trybu 802.1X 5.3.5 wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu  | Spełnia / Nie spełnia |
| Wsparcie dla protokołu IPv6 | 6.1 System posiada wsparcie dla SSH IPv6 6.2 System pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6 6.3 System pozwala na konfigurację NTP IPv6 6.4 System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6 6.5 System umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6 6.6 System umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6 6.7 System umożliwia integrację z Active Directory w oparciu o IPv6 6.8 System umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6  | Spełnia / Nie spełnia |
| Dobre praktyki realizacji rozwiązania | 7.1 System spełnia następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci 7.2 System może występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów. 7.3 W przypadku zastosowania rozwiązania złożonego z kilku komponentów system zapewnia pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN. 7.4 Niezależnie od tego czy system występuje w formie pojedynczego rozwiązania lub jest złożony z kilku komponentów, może on być serwisowany jako jeden system w ramach pojedynczej usługi wsparcia.  | Spełnia / Nie spełnia |
| Wdrożenie/ dokumentacje/ szkolenie | Przygotowanie infrastruktury i zasobów na potrzeby instalacji oprogramowania. Instalacja oprogramowania na wybranej platformie (sprzętowej lub wirtualnej).Wstępna konfiguracja systemu (adres IP, dostęp, konfiguracja języka).Konfigurowanie połączenia z Active Directory (AD) lub innym źródłem danych użytkowników.Testowanie poprawności integracji z systemem katalogowym.Zdefiniowanie pobieranych list dostępowych (dACL)Utworzenie profili autoryzujących.Definiowanie polityk 802.1X, MAB, i innych metod autentykacji.Konfiguracja ról użytkowników i przypisanie polityk dostępu.Konfiguracja przełączników sieciowych i punktów dostępu do współpracy z zamówionym oprogramowaniem.Testowanie poprawności działania uwierzytelniania i dostępu do sieci.Konfiguracja systemu monitorowania i audytu działań użytkowników.Implementacja generowania raportów zgodnie z wymaganiami.Szkolenie dla administratorów.Przygotowanie procedur operacyjnych.Wsparcie powdrożeniowe w ilości 5 godzin.Dostarczenie dokumentacji- instrukcje procedur SOP (standard operating procedure), opisujące, w jaki sposób wykonywać czynności administracyjne - dokumenty, który precyzyjnie opisują standardowy sposób wykonywania określonych zadań w tym systemie.Dokument obejmuje opis podstawowych czynności administracyjnych, które są wykonywane przez administratorów systemu uwierzytelniającego dostępu do sieci, w tym:• Dodawanie nowych urządzeń do oprogramowania• Tworzenie i zarządzanie politykami dostępu• Monitorowanie stanu systemu• Rozwiązywanie podstawowych problemów z urządzeniami i politykami• Aktualizacja systemuSzkolenie w ramach funkcjonalności zawartych w licencjach jest szacowane na 8 godzin, w trybie zdalnym.Wymagania dla inżyniera wdrażającego:posiadanie certyfikatów CCNP Enterprise oraz CCNP Security lub równoznacznych.Zamawiający wymaga wykonania usługi w terminie 30 dni od dnia podpisania umowy.Cały zakres wdrożenia wraz zamawianymi usługami zostanie wykonany w ilości godzin: nie mniej niż 25, w trybie zdalnym. | Spełnia / Nie spełnia |
| Licencje / Ilość | Zamawiający wymaga dostarczenia oprogramowania z oficjalnego, polskiego kanału dystrybucyjnego.Rozwiązanie musi posiadać konsolę do zarządzania wraz ze wsparciem producenta, na okres 36 miesięcy oraz subskrypcją dla 100 hostów na okres 36 miesięcy.Termin rozpoczęcia trwania licencji: 01.05.2025r. Zamawiający wymaga dostarczenie ww. produktu w formie odpowiedniego klucza licencyjnego.  | Spełnia / Nie spełnia |