**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

# **Zakup przełączników sieciowych warstwy szkieletowej, dostępowej oraz systemu kontroli dostępu do sieci.**

# **Przełącznik szkieletowy Liczba urządzeń : 4 sztuki**

**2 zestawy redundantnych przełączników**

**Oferowany model \* …………………….. Producent \* …………………..**

| **Identyfikator wymagania** | **Opis wymagań minimalnych** |
| --- | --- |
| PRZEŁĄCZNIK - 01 | Minimum 40 portów 1/10GBase-X SFP+. Wszystkie porty muszą być dostępne od przodu urządzenia. |
| PRZEŁĄCZNIK - 01 | Urządzenie musi posiadać min. jeden slot modułów rozszerzeń z możliwością wymiany na gorąco ( ang. hot swap). Wśród dostępnych modułów rozszerzeń musza być dostępne co najmniej następujące moduły:   1. Min. 8 portowy moduł 10Gigabit Ethernet SFP+, 2. Min. 2 portowy moduł 40Gigabit Ethernet QSFP+. |
| PRZEŁĄCZNIK – 02 | Urządzenie musi zostać wyposażone w następujące rodzaje interfejsów optycznych:   1. 44x 10GB SFP+ SR MM, 2. 4x 10GB SFP+ LR SM. |
| PRZEŁĄCZNIK – 03 | Przełącznik wyposażony w:   1. redundantne i wymienne moduły wentylatorów, 2. redundantne i wymienne zasilacze prądu zmiennego AC. |
| PRZEŁĄCZNIK – 04 | Przełącznik posiadający wydajność:   1. przepustowość nie mniejsza niż 960Gb/s, 2. szybkość przełączania/routingu minimum 700Mp/s. |
| PRZEŁĄCZNIK - 05 | Skalowalność:   1. min. 4.000 sieci VLAN, interfejsów SVI, instancji Spanning Tree, 2. min. 50.000 adresów MAC, 3. sprzętowa dla QoS i ACL - minimum 15.000 wpisów sprzętowych. |
| PRZEŁĄCZNIK – 06 | Min. 16GB pamięci DRAM. |
| PRZEŁĄCZNIK – 07 | Min. 16GB pamięci flash lub SSD. |
| PRZEŁĄCZNIK – 08 | Przełączanie w warstwie 2 i 3   1. obsługa VLAN 802.1Q i trunk na wszystkich portach, 2. obsługa routingu statycznego i dynamicznego (RIPv2, RIPng, OSPF v2/v3, IS-IS, BGP dla IPv4 i IPv6), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM), 3. obsługa co najmniej pięćdziesięciu wirtualnych tablic routingu (VRF) dla IPv4/IPv6 (w ramach VRF wymagana obsługa routingu statycznego i dynamicznego), 4. obsługa Policy-Based Routing dla IPv4 i IPv6, 5. obsługa protokołu BFD (Bidirectional Forwarding Detection) dla IPv4 i IPv6 dla routingu statycznego oraz dynamicznego – minimum dla protokołów OSPF, IS-IS i BGP, 6. obsługa protokołu redundancji bramy VRRP/HSRP lub innego równoważnego, 7. tablica routingu (FIB) musi umożliwiać obsługę minimum: 8. 60.000 wpisów dla IPv4, 9. 30.000 wpisów dla IPv6, 10. 8.000 wpisów dla ruchu multicast (IPv4/IPv6). 11. przełącznik musi obsługiwać ramki Jumbo (do min. 9100 bajtów). |
| PRZEŁĄCZNIK - 9 | Mechanizmy związane z zapewnieniem ciągłości pracy sieci:   1. 802.1w Rapid Spanning Tree, 2. 802.1s Multi-Instance Spanning Tree, 3. 802.3ad Link Aggregation Control Protocol, 4. urządzenie musi umożliwiać stworzenie wirtualnego systemu złożonego z min. 2 urządzeń będącego przedmiotem opisu, zarządzanego jako całość. Dla innych urządzeń taki system wirtualny musi być widoczny jako pojedynczy węzeł sieciowy. W ramach systemu wirtualnego musi istnieć możliwość tworzenia połączeń link aggregation terminowanych na dwóch fizycznych przełącznikach (tzw. multi-chassis link aggregation) zgodnych z IEEE 802.3ad. |
| PRZEŁĄCZNIK - 10 | Mechanizmy związane z zapewnieniem jakości usług w sieci:   1. obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu, 2. obsługa co najmniej jednej kolejki ze statusem strict priority, 3. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, 4. możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP, 5. obsługa kolejkowania, ograniczania (rate-limiting), kształtowania (shaping), zarządzania pasmem, 6. obsługa zaawansowanych mechanizmów aktywnego zarządzania długością kolejki (typu WTD lub podobny) oraz unikania zatorów (typu WRED lub podobny), 7. kontrola sztormów dla ruchu boradcast i multicast. |
| PRZEŁĄCZNIK - 11 | Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:   1. min. 5 poziomów dostępu administracyjnego poprzez konsolę, 2. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL, 3. obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, 4. obsługa funkcji Voice VLAN umożliwiającej segmentację ruchu głosowego od ruchu użytkowników, 5. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, 6. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, 7. wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie, 8. możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, 9. możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2, 10. możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec-128) line-rate dla wszystkich portów 1/10GE przełącznika (dla połączeń switch-switch), 11. obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6 (na poziomie portu, VLANu, interfejsu L3), 12. obsługa mechanizmu uRPF, 13. obsługa mechanizmów bezpieczeństwa Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, 14. obsługa mechanizmów bezpieczeństwa dla ruchu IPv6 na brzegu sieci – DHCPv6 Guard, IPv6 Snooping, IPv6 Router Advertisement (RA) Guard, IPv6 Source Guard, 15. możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+, 16. funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym. |
| PRZEŁĄCZNIK - 12 | Mechanizmy związane z zarządzaniem urządzeniem:   1. możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 100.000 (wymagane wsparcie sprzętowe), 2. przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku (bi-directional), 3. funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC, 4. obsługa protokołu LLDP i LLD-MED., 5. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych i 2 wersji oprogramowania, 6. możliwość cofnięcia ostatnich zmian konfiguracyjnych (config rollback), 7. urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, 8. urządzenie musi posiadać wbudowany analizator pakietów , 9. obsługa standardowego interfejsu programistycznego NetCONF i modeli YANG, 10. dedykowany port Ethernet do zarządzania urządzeniem. |
| PRZEŁĄCZNIK - 13 | Obudowa przystosowana do montażu w szafie 19”, wysokość nie większa niż 5RU. |

# **Przełącznik dostępowy Liczba urządzeń : 56 sztuk**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Identyfikator wymagania** | **Opis wymagań minimalnych** |
| PRZEŁĄCZNIK – 14 | Minimum 48 portów 100/1000GBase-T |
| PRZEŁĄCZNIK – 15 | Port na karty rozszerzeń umożliwiający instalację minimum:   1. Karty z minimum 4 porty 1/10GBase-X SFP+ 2. Karty z minimum 2 porty 40GBase-X |
| PRZEŁĄCZNIK – 16 | Urządzenie musi zostać dostarczone z kartą minimum 4 porty 1/10GBase-X SFP+ obsadzoną wkładkami 10GB SFP+ SR MM umożliwiającymi poprawną współpracę z oferowanym Przełącznikiem szkieletowym opisanym w pkt. 1. |
| PRZEŁĄCZNIK – 17 | Wszystkie porty Ethernet muszą być dostępne od przodu urządzenia. |
| PRZEŁĄCZNIK – 18 | Przełącznik wyposażony w:   1. redundantne i wymienne moduły wentylatorów, 2. wymienne zasilacze prądu zmiennego AC, 3. mechanizm redundancji zasilania, zapewniający podtrzymanie pracy stosu przy awarii zasilacza jednego z przełączników w stosie. |
| PRZEŁĄCZNIK – 19 | Przełącznik posiadający wydajność:   1. przepustowość nie mniejsza niż 256Gb/s, 2. szybkość przełączania/routingu minimum 150Mp/s, |
| PRZEŁĄCZNIK - 20 | Skalowalność:   1. min. 2.000 sieci VLAN, interfejsów SVI, instancji Spanning Tree, 2. min. 30.000 adresów MAC, 3. sprzętowa dla ACL - minimum 5000 wpisów sprzętowych, 4. min. 4GB pamięci DRAM, 5. min. 2GB pamięci Flash. |
| PRZEŁĄCZNIK – 21 | Urządzenia muszą zapewniać łączenie w stos   * 1. obsługa co najmniej 8 urządzeń w stosie,   2. przepustowość w stosie min. 320 Gbps,   3. stos widoczny jako jedno urządzenie z perspektywy protokołów sieciowych, routingu i zarządzania,   4. połączenie urządzeń w stos nie może zmniejszać dostępnej ilości portów Ethernet opisanych powyżej,   5. urządzenie musi zostać wyposażone w moduły i okablowanie niezbędne do podłączenia stosu. |
| PRZEŁĄCZNIK - 22 | Przełączanie w warstwie 2 i 3   1. obsługa VLAN 802.1Q i trunk na wszystkich portach, 2. obsługa routingu statycznego i dynamicznego (RIPv2, RIPng, OSPF v2/v3 dla IPv4 i IPv6 – co najmniej 200 tras), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM), 3. tablica routingu (FIB) musi umożliwiać obsługę minimum: 4. 16.000 wpisów „unicast routes” dla IPv4, 5. 4.000 wpisów „unicast routes” dla IPv6, 6. 4.000 wpisów dla ruchu multicast (IPv4/IPv6), 7. przełącznik musi obsługiwać ramki Jumbo (do min. 9100 bajtów). |
| PRZEŁĄCZNIK - 23 | Mechanizm związane z zapewnieniem ciągłości pracy sieci:   1. 802.1w Rapid Spanning Tree, 2. 802.1s Multi-Instance Spanning Tree, 3. 802.3ad Link Aggregation Control Protocol. |
| PRZEŁĄCZNIK – 24 | Mechanizmy związane z zapewnieniem jakości usług w sieci:   1. obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu, 2. obsługa co najmniej jednej kolejki ze statusem strict priority, 3. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, 4. możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP, 5. obsługa kolejkowania, ograniczania (rate-limiting), kształtowania (shaping), zarządzania pasmem, 6. obsługa zaawansowanych mechanizmów aktywnego zarządzania długością kolejki (typu WTD lub podobny) oraz unikania zatorów (typu WRED lub podobny), 7. kontrola sztormów dla ruchu boradcast i multicast. |
| PRZEŁĄCZNIK - 25 | Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:   1. min. 5 poziomów dostępu administracyjnego poprzez konsolę, 2. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL, 3. obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1.x, 4. obsługa funkcji Voice VLAN umożliwiającej segmentację ruchu głosowego od ruchu użytkowników, 5. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, 6. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1.x, 7. wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie, 8. możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, 9. możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2, 10. możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec-128) line-rate dla wszystkich portów 1/10GE przełącznika (dla połączeń przełącznik-przełącznik), 11. obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6 (na poziomie portu, VLAN-u, interfejsu L3), 12. obsługa mechanizmu uRPF, 13. obsługa mechanizmów bezpieczeństwa Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, 14. obsługa mechanizmów bezpieczeństwa dla ruchu IPv6 na brzegu sieci – DHCPv6 Guard, IPv6 Snooping, IPv6 Router Advertisement (RA) Guard, IPv6 Source Guard, 15. możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1.x) do serwerów RADIUS lub TACACS+, 16. funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLAN-u (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym. |
| PRZEŁĄCZNIK – 26 | Mechanizmy związane z zarządzaniem urządzeniem:   1. możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 50.000 (wymagane wsparcie sprzętowe), 2. przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku (bi-directional), 3. funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC, 4. obsługa protokołu LLDP i LLD-MED, 5. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych i 2 wersji oprogramowania, 6. możliwość cofnięcia ostatnich zmian konfiguracyjnych (config rollback), 7. funkcjonalność umożliwiająca tworzenie makr konfiguracyjnych aplikowanych do portu przy wykryciu dołączenie urządzenia określonego typu, 8. urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, 9. urządzenie musi posiadać wbudowany analizator pakietów, 10. obsługa standardowego interfejsu programistycznego NetCONF i modeli YANG, 11. dedykowany port Ethernet do zarządzania urządzeniem. |
| PRZEŁĄCZNIK - 27 | Obudowa przystosowana do montażu w szafie 19”, wysokość 1U. |

# **System kontroli dostępu do sieci Liczba urządzeń : 2 sztuki aplliance**

**Oferowany model \* …………………….. Producent \* …………………..**

|  |  |
| --- | --- |
| **Identyfikator wymagania** | **Opis wymagań minimalnych** |
| **Parametry techniczne:** | |
| SKDS - 01 | Dostarczone rozwiązanie musi być w postaci dedykowanego urządzenia (appliance) posiadającego poniższe parametry:   * + 1. procesor o taktowaniu co najmniej 2.40GHz, 6 rdzeni, 12 wątków,     2. dysk o pojemności co najmniej 600GB,     3. co najmniej 16 GB pamięci RAM,     4. co najmniej 4 porty 10/100/1000 RJ45. |
| SKDS - 02 | W celu zapewnienia redundancji muszą zostać dostarczone dwa identyczne urządzenia umożliwiające pracę w klastrze HA. |
| **Funkcjonalności:** | |
| SKDS – 03 | System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w ramach wzrostu liczby obsługiwanych stacji końcowych. |
| SKDS – 04 | System musi umożliwiać obsługę co najmniej 2.500 urządzeń końcowych dołączonych do sieci oraz zapewniać skalowalność do przynajmniej 25.000 urządzeń poprzez dalszą rozbudowę istniejącego wdrożenia. |
| SKDS – 05 | System musi umożliwiać 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. |
| SKDS – 06 | System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback). |
| SKDS – 07 | System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled). |
| SKDS – 08 | System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników. |
| SKDS – 09 | System musi umożliwiać 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 musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni. |
| SKDS – 10 | System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora. |
| SKDS – 11 | System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP. |
| SKDS – 12 | System musi wspierać następujące protokoły uwierzytelniania i standardy:   1. RADIUS, zgodnie z dokumentami:    * 1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS),      2. RFC 2139 — RADIUS Accounting,      3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS),      4. RFC 2866 — RADIUS Accounting,      5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support,      6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support,      7. RFC 2869 — RADIUS Extensions. 2. RADIUS Proxy dla zewnętrznego serwera RADIUS, 3. TACACS+. |
|
|
|
|
| SKDS – 13 | System musi wspierać protokół Lightweight Directory Access Protocol (LDAP) oraz integrację z Windows Active Directory, w tym co najmniej następujące repozytoria AD:   1. Microsoft Windows Active Directory 2012 R2, 2. Microsoft Windows Active Directory 2016. |
| SKDS – 14 | System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865. |
| SKDS - 15 | System musi wspierać następujące protokoły uwierzytelniania:   1. PAP/ASCII, 2. CHAP, 3. MS-CHAPv1, 4. MS-CHAPv2, 5. EAP-MD5, 6. LEAP, 7. EAP-TLS, 8. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi: 9. EAP-MS-CHAPv2, 10. EAP-GTC, 11. EAP-TLS. 12. System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect. |
| SKDS – 16 | System musi wspierać implementację 802.1.x z przynajmniej następującymi suplikantami:   1. wbudowanym klientem 802.1.x dla Windows 7/8/10, 2. Apple Mac OS X Supplicant, 3. Apple iOS Supplicant, 4. Google Android Supplicant. |
| SKDS – 17 | System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o reguły (rule-based). |
| SKDS – 18 | System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników. |
| SKDS – 19 | System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym). |
| SKDS – 20 | System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC. |
| SKDS - 21 | System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC |
| SKDS - 22 | System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:   1. tryb uwierzytelniania 802.1.x, w którym dozwolony jest jeden host per port, 2. tryb uwierzytelniania 802.1.x, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia, 3. tryb uwierzytelniania 802.1.x, 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, 4. tryb uwierzytelniania 802.1.x dozwalający wiele hostów na jednym porcie fizycznym, 5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny, 6. mechanizm umożliwiający poprawną obsługę sytuacji w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLAN-ie głosowym, 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, 8. mechanizm przypisania VLAN-u w procesie uwierzytelnienia i kontroli dostępu 802.1.x, 9. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1.x, 10. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1.x, w celu realizacji uwierzytelniania za pomocą przeglądarki, 11. mechanizm 802.1.x umożliwiający realizację dostępu gościnnego w dedykowanym VLAN-ie (Guest VLAN) dla użytkowników gościnnych, 12. mechanizm 802.1.x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLAN-u w sytuacji, gdy serwer AAA jest niedostępny, 13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLAN-ów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników, 14. uwierzytelnienie 802.1.x urządzenia telefonii IP znajdującego sie w VLAN-ie głosowym, 15. współpraca mechanizmu 802.1.x z urządzeniami używającymi mechanizmu Wake-on-LAN, 16. możliwość elastycznej konfiguracji kolejności metod 802.1.x użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1.x i uwierzytelnienia web, 17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika. |
|
| SKDS – 23 | System musi wspierać 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 802.1.x). |
| SKDS – 24 | System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla :   1. Microsoft Windows 7/8/10, 2. Apple Mac OS X 10.x, 3. Apple iOS 8.0, 7.x, 4. Google Android dla 2.2 i nowszych, 5. Linux. |
| SKDS - 25 | System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor). |
| SKDS – 26 | System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:   1. wewnętrzną bazę użytkowników, 2. zewnętrzne repozytorium użytkowników. |
| SKDS – 27 | System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:   1. logowania się do systemu, 2. tworzenia pojedynczego konta gościnnego, 3. tworzenia wielu kont gościnnych, 4. importowania kont gościnnych z pliku CSV, 5. wysyłania wiadomości email po utworzeniu konta gościnnego, 6. wysyłania wiadomości SMS po utworzeniu konta gościnnego, 7. wyświetlenia hasła konta gościnnego, 8. wydrukowania danych konta gościnnego, 9. wyświetlenia danych stworzonych kont gościnnych, 10. zawieszenia (suspend) i reinicjacji kont gościnnych. |
| SKDS - 28 | System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:   1. zmianę logo strony logowania, 2. zmianę obrazu tła strony logowania, 3. zmianę logo bannera, 4. zmianę obrazu tła bannera, 5. zmianę koloru tła strony z treścią. |
| SKDS – 29 | System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS. |
| SKDS – 30 | System musi umożliwiać zmianę adresu URL i FQDN strony sponsora. |
| SKDS – 31 | System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System musi umożliwiać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych. |
| SKDS – 32 | System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim i angielskim. |
| SKDS – 33 | System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:   1. Imienia, 2. Nazwiska, 3. Firmy, 4. adresu e-mail, 5. numeru telefonu, 6. danych opcjonalnych. |
| SKDS – 34 | System musi umożliwiać konfigurację dla użytkowników gościnnych:   1. wyświetlenia im informacji polityce akceptowalnego użycia sieci (AUP), 2. zezwolenia gościom na zmianę hasła, 3. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora. |
| SKDS – 35 | System musi umożliwiać honorowanie ustawień lokalnych przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego. |
| SKDS – 36 | System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego. |
| SKDS – 37 | System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 20 urządzeń per konto gościnne. |
| SKDS – 38 | System musi umożliwiać konfigurację czasu ważności hasła w dniach w zadanym przedziale. |
| SKDS – 39 | System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny. |
| SKDS – 40 | System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych. |
| SKDS – 41 | System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika |
| SKDS – 42 | System musi umożliwiać tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu. |
| SKDS – 43 | System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS. |
| SKDS – 44 | System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych. |
| SKDS – 45 | System musi umożliwiać rozbudowę o możliwość dokonania profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu. |
| SKDS – 46 | System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows. |
| SKDS – 47 | System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:   1. DHCP, 2. DHCP SPAN, 3. http, 4. DNS, 5. SNMP, 6. Network Scan (NMAP lub inne narzędzie profilowania aktywnego). |
| SKDS – 48 | System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji. |
| SKDS – 49 | System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy. |
| SKDS – 50 | System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:   1. Stacji roboczych pracujących z systemami Linux, Microsoft Windows, 2. Urządzeń mobilnych: Android, Apple, Blackberry, 3. Telefonów IP, 4. Drukarek sieciowych, 5. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych, 6. Routerów, 7. Punktów dostępu bezprzewodowego. |
| SKDS – 51 | System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:   1. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci, 2. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt. |
| SKDS – 52 | System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta. |
| SKDS - 53 | System musi umożliwiać generowanie przynajmniej następujących raportów:   1. raportów dla protokołów AAA, 2. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, 3. raportów dla systemu, w tym: 4. administratorów systemu i ich uprawnień, 5. logowania administratorów do systemu, 6. zmian konfiguracji serwera dokonanych przez administratorów, 7. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS), 8. zmian operacyjnych serwera dokonanych przez administratorów, 9. zmian haseł przez użytkowników. 10. raportów dla stacji końcowych, w tym: 11. uwierzytelnień typu MAC Authentication, 12. Top „N” uwierzytelnień per adres MAC stacji, 13. Top „N” uwierzytelnień per maszyna, 14. Top „N” uwierzytelnień per RADIUS Calling Station ID, 15. działań podsystemu profilera per adres MAC, 16. czasu wymaganego na sprofilowanie stacji per adres MAC. 17. raportów dla błędów, w tym: 18. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił, 19. sumarycznych przyczyn nieudanych uwierzytelnień. 20. raportów dla urządzeń sieciowych: 21. sumarycznych uwierzytelnień dla urządzeń sieciowych, 22. niedostępności serwera AAA dla urządzenia sieciowego, 23. wiadomości logowanych przez urządzenia sieciowe, 24. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP. 25. raportów użytkowników: 26. sumarycznych uwierzytelnień użytkowników, 27. Top „N” uwierzytelnień per użytkownik, 28. sesji użytkowników gościnnych, 29. aktywności użytkowników gościnnych, 30. sumarycznych uwierzytelnień sponsorów dostępu gościnnego, 31. uwierzytelnień per unikalny użytkownik. 32. raportów katalogu sesji 33. aktywnych sesji RADIUS, 34. historii sesji RADIUS, 35. zaterminowanych sesji RADIUS. |
|
| SKDS - 54 | System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą   1. wiadomości e-mail 2. syslog |
| SKDS – 55 | Alarmy muszą być generowane w następujących sytuacjach:   1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu, 2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego, 3. status krytycznych procesów będzie niepożądany, w tym status: 4. procesu wewnętrznej bazy danych systemu, 5. serwera aplikacyjnego systemu, 6. bazy danych sesji, 7. kolektora i procesora wiadomości log, 8. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej), 9. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:    1. obciążenie systemu (load),    2. zajętość pamięci. |
| SKDS - 56 | System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:   1. badanie łączności IP za pomocą ping, nslookup, traceroute, 2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem: 3. nazwy użytkownika, 4. adresu MAC, 5. statusu uwierzytelnienia (udana lub nieudana), 6. powodu, jeżeli uwierzytelnienie nieudane, 7. zakresu czasowego, co do dnia, godziny i minuty. 8. wykonanie zdalnego polecenia na urządzeniu sieciowym, 9. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: 10. definicji serwerów AAA, 11. protokołu RADIUS, 12. odkrywania urządzeń, 13. logowania, 14. uwierzytelniania Web, 15. konfiguracji trybu 802.1.x. 16. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu. |

# **Pozostałe wymagania Zamawiającego:**

1. Wykonawca opracuje Projekt Techniczny uruchomienia urządzeń zgodnie z ustaleniami z Zamawiającym.
2. Wykonawca skonfiguruje sprzęt tak aby wyżej wymienione przełączniki szkieletowe tworzyły dwa w pełni redundantne zestawy przełączników szkieletowych.
3. Wykonawca dokona montażu urządzeń w szafach rack w miejscu wskazanym przez Zamawiającego.
4. Wykonawca dokona niezbędnych prac w celu podłączenia dostarczanych urządzeń do zasilania elektrycznego (odpowiednie gniazda, przewody, bezpieczniki itp.). Wykonawca dostarczy 60 sztuk listw zasilających wyposażonych w minimum 5 gniazd elektrycznych oraz bezpiecznik w celu podłączenia przełączników szkieletowych i dostępowych.
5. Do obydwu zestawów przełączników szkieletowych, przełączniki dostępowe będą połączone min. dwoma redundantnymi linkami światłowodowymi MM. Ponadto Wykonawca skonfiguruje stos przełączników dostępowych w miejscach gdzie wskaże Zamawiający.
6. Wykonawca wdroży i uruchomi w sieci standard 802.1x przy pomocy dostarczanego Systemu kontroli dostępu do sieci dla wszystkich urządzeń PC i urządzeń peryferyjnych podłączonych do sieci LAN w siedzibie Zamawiającego.
7. Dostarczane urządzenia muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej niż 6 miesięcy przed ich dostarczeniem, nierefabrykowane) oraz nieużywane.
8. Urządzenia wraz z zainstalowanym na nich oprogramowaniem muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta i być przeznaczone do użytkowania na terenie Unii Europejskiej oraz posiadać pakiet usług gwarancyjnych skierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej.
9. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta/ów rozwiązania.
10. Dostarczone wraz z urządzeniami oprogramowanie musi być oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy przed terminem dostawy albo w ostatniej opublikowanej i rekomendowanej przez producenta). Wykonawca w momencie wdrożenia dokona aktualizacji wersji oprogramowania urządzeń do najnowszej rekomendowanej przez producenta.
11. Poszczególne funkcjonalności i protokoły wymagane dla obu typów przełączników muszą być kompatybilne.
12. Wykonawca wykona połączenia za pomocą niezbędnego okablowania pasywnego oferowanej infrastruktury sprzętowej z obecnie eksploatowaną infrastrukturą sprzętową Zamawiającego.
13. Dostawa musi obejmować wszystkie elementy wymagane przez producentów oferowanego rozwiązania do jego prawidłowego podłączenia i konfiguracji w tym do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10%, 50 Hz.
14. Wykonawca w ramach zamówienia zapewni wszystkie kable i patchcordy konieczne do podłączenie instalowanych urządzeń w szczególności: wymagane kable do tworzenia stosów z urządzeń, patchcordy światłowodowe wymagane do poprawnego działania przedstawionej w Projekcie Technicznym konfiguracji sprzętu wraz z nadmiarową niezbędną ilością do podłączenia wszystkich obsadzonych portów światłowodowych; patchcordy UTP/FTP min. Cat. 6A wymagane do poprawnego działania przedstawionej konfiguracji sprzętu wraz z nadmiarową niezbędną ilością do podłączenia wszystkich obsadzonych portów elektrycznych;

Zamawiający przewiduje zastosowanie 300 połączeń światłowodowych MM za pomocą kabli o długości 5m, 2000 połączeń kablem kat. 6e o długości 2m, 1000 połączeń kablem kat 6e o długości 3m, 1000 połączeń kablem kat 6e o długości 5m, 1000 połączeń kablem kat 6e o długości 10m, 300 połączeń kablem kat 6e o długości 15m. W ramach realizacji umowy należy dostarczyć wskazane ilości patchcordów.

1. W ramach realizacji zamówienia Wykonawca dostarczy po 4 vouchery szkoleniowe ważne przez okres 18 miesięcy na szkolenia w zakresie podstawowej i zaawansowanej konfiguracji dostarczanych przełączników oraz dostarczanego Systemu kontroli dostępu do sieci dla administratorów Zamawiającego.
2. Szkolenia zostaną przeprowadzone w autoryzowanym ośrodku szkoleniowym w Warszawie.

**UWAGI ZAMAWIAJĄCEGO:**

(\*) Należy podać nazwę oferowanego oprogramowania, numer wersji i producenta.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Czytelny Podpis/podpisy osoby/osób uprawnionego**

**do reprezentowania Wykonawcy**

**Miejscowość\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**