**ROZDZIAŁ II – FORMULARZ OFERTY**

|  |  |
| --- | --- |
| *Nr postępowania*  **9/2024** | **OFERTA** |

składając ofertę w postępowaniu o udzielenie zamówienia publicznego na**:** **Zakup urządzeń sieciowych (agregacyjnych i sieciowych) – 4 szt. oraz dostępowych – 18 szt. wraz z systemem zarządzania i monitorowania sieci.**

**MY NIŻEJ PODPISANI**

**…………………………………………..…………………….………..…………..…………..………………………………………………….**

działając w imieniu i na rzecz

**..........................................................................................................................................................**

**..........................................................................................................................................................**

*[nazwa (firma) i dokładny adres Wykonawcy/ów; w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich wspólników spółki cywilnej lub członków konsorcjum]*

NIP: ………………………………………., REGON: ………………………………………, KRS: ………………………………….………..

* będącego mikroprzedsiębiorstwem \*
* będącego małym przedsiębiorstwem \*
* będącego średnim przedsiębiorstwem \*
* prowadzącego jednoosobową działalność gospodarczą \*
* będącego osobą fizyczną nieprowadzącą działalności gospodarczej \*
* inny rodzaj \*

*\* należy zaznaczyć/ wskazać właściwe*

*Definicja mikro, małego i średniego przedsiębiorcy znajduje się w art. 7 ust. 1 pkt 1, 2 i 3 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców (t.j. Dz. U. z 2024 r. poz. 236).*

**Kontakt:**

Adres do korespondencji: ……....................................................................................................................

Osoba do kontaktu: .........................................., tel.: ………………………..…., e-mail: ……………..…………………

1. Oferuję realizację przedmiotu zamówienia określonego w SWZ, OPZ i Projektowanych Postanowieniach Umowy za kwotę:

Netto …………………zł (słownie złotych…………………………………………………………………..)

VAT…………………….zł (słownie złotych…………………………………………………………………..)

Brutto…………………zł (słownie złotych…………………………………………………………………..)

**wynikającą z poniższej tabeli:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Wyszczególnienie | ilość | Cena netto za 1 szt./komplet | Kwota podatku VAT | Cena brutto za 1 szt./komplet | Wartość netto w zł | Ogółem wartość brutto w zł |
| **1** | **2** | **3** | **4** | **5** | **6=(4+5)** | **7=(3x4)** | **8=(3x6)** |
| 1. | Urządzenia sieciowe (agregacyjne i sieciowe) | **4** |  |  |  |  |  |
| 2 | Urządzenia dostępowe | **18** |  |  |  |  |  |
| 3 | System zarządzania i monitorowania sieci | **1** |  |  |  |  |  |
| 4 | Dodatkowe moduły optyczne i okablowanie | **Komplet** |  |  |  |  |  |
| 5 | razem | **x** | **x** | x | x |  |  |

**3. Oświadczenia:**

1. Oświadczamy,że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania;
2. Oświadczamy,iż wybór mojej oferty **będzie/ nie będzie**\* prowadził do powstania u Zamawiającego obowiązku podatkowego wynikającego z ustawy o podatku VAT.

Wskazujemy następującą nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, wskazuje ich wartość bez kwoty podatku, wskazuje stawkę podatku od towarów i usług, która zgodnie z moją wiedzą, będzie miała zastosowanie: ………………………………………………………….......................…….

1. Oświadczamy,że oferowany przez nas przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego w Specyfikacji Warunków Zamówienia oraz w OPZ i Projektowanych Postanowieniach Umowy.
2. Oświadczamy,że zrealizujemy przedmiot zamówienia w terminie wymaganym w dokumentach zamówienia.
3. Oświadczamy, że zaoferowana cena zawiera wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.
4. Uważamy się za związanych niniejszą ofertą na czas wskazany w Specyfikacji Warunków Zamówienia.
5. Akceptujemy dołączone do Specyfikacji Warunków Zamówienia Projektowane Postanowienia Umowyi zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na warunkach tam określonych, a także w miejscu i terminie wyznaczonym przez Zamawiającego.
6. Zobowiązujemy się do złożenia wymaganych dokumentów stanowiących formalności przed zawarciem umowy.
7. Oświadczamy, że oferta ***nie zawiera informacji*** stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.\*

Oświadczamy, że oferta ***zawiera informacje*** stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach \* : ..……………………………………………………..

1. Oświadczamy,że zamówienie zrealizujemysami\*/ przy udziale podwykonawców w następującym zakresie \*:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa (firma) podwykonawcy (jeżeli jest znana)** | **Część (zakres) prac, którą zamierzamy powierzyć podwykonawcy** |
| 1. |  |  |
| 2. |  |  |
| ***1****Wypełnić w zakresie zamierzonego powierzenia wykonania zamówienia Podwykonawcom, jeżeli są znani.* | | |

1. Wskazuję, **również w oświadczeniu stanowiącym Formularz II.1.**, iż następujące podmiotowe środki dowodowe/ dokumenty rejestrowe:

...........................................................................................................................................................

*wskazać jakie*

są dostępne w formie elektronicznej pod określonymi ogólnodostępnymi i bezpłatnymi adresami internetowymi baz danych, które można wyszukać za pomocą następujących danych:

...........................................................................................................................................................

*np. nazwa dokumentu/ oświadczenia/numer wpisu, numer NIP, numer REGON*

1. Na podstawie art. 127 ust. 2 Pzp wskazuję oznaczenie sprawy w postępowaniu o udzielenie zamówienia publicznego oraz podmiotowe środki dowodowe, które znajdują się w posiadaniu zamawiającego, w szczególności oświadczenia lub dokumenty, o których mowa w § 6 - 9 Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy, przechowywane przez zamawiającego zgodnie z art. 78 ust. 1 Pzp, w celu potwierdzenia okoliczności, o których mowa w art. 273 ust. 1 Pzp i potwierdzam ich prawidłowość i aktualność.

(należy wypełnić, jeżeli oświadczenia lub dokumenty, o których mowa w § 6-9 *Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy,* znajdują się w posiadaniu zamawiającego, w szczególności oświadczenia lub dokumenty przechowywane przez zamawiającego zgodnie z art. 78 ust. 1 Pzp).

|  |  |
| --- | --- |
| Nazwa/ numer bądź inne dane identyfikujące postępowanie | Rodzaj oświadczeń lub dokumentów (*znajdujących się w posiadaniu zamawiającego).* |
|  |  |

1. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*\*

*\* niepotrzebne skreślić*

\*\* *W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

Do niniejszej oferty załączamy (wybrać właściwe lub skreślić niepotrzebne):

* Oświadczenie, o którym mowa w art. 125 ust. 1 Pzp/ podmiotu trzeciego/ Wykonawców wspólnie ubiegających się o udzielenie zamówienia – Formularz II.1,
* Pełnomocnictwo do reprezentowania Wykonawcy (jeżeli dotyczy),
* Pełnomocnictwo do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy),
* Pełnomocnictwo do reprezentowania podmiotu udostępniającego zasoby (jeżeli dotyczy),
* Formularz II.2 – zobowiązanie podmiotu udostępniającego zasoby (wymienić nazwy podmiotów ……..),
* Formularz II.5 – oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy)dotyczące zakresu realizowanego zamówienia,
* Uzasadnienie zastrzeżenia dokumentów jako tajemnicy przedsiębiorstwa (jeżeli dotyczy)
* inne dokumenty: …………

(Dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym osoby umocowanej do reprezentowania Wykonawcy)

**ROZDZIAŁ II – FORMULARZ OFERTY**

**ZAŁĄCZNIK A**

|  |  |
| --- | --- |
| *Nr postępowania*  **9/2024** | **OFERTA** |

składając ofertę w postępowaniu o udzielenie zamówienia publicznego na**: Zakup urządzeń sieciowych (agregacyjnych i sieciowych) – 4 szt. oraz dostępowych – 18 szt. wraz z systemem zarządzania i monitorowania sieci.**

**MY NIŻEJ PODPISANI**

**…………………………………………..…………………….………..…………..…………..………………………………………………….**

działając w imieniu i na rzecz

**..........................................................................................................................................................**

**..........................................................................................................................................................**

*[nazwa (firma) i dokładny adres Wykonawcy/ów; w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich wspólników spółki cywilnej lub członków konsorcjum]*

*OFERUJEMY:*

Specyfikacja techniczna przełączników sieciowych (agregacyjne i data center) – 4 szt. - …………………

Producent/model

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Minimalne wymagania** | **Parametry techniczne oferowanego produktu /spełnia – nie spełnia/** |
| **Konfiguracja fizyczna** | Minimalna ilość portów QSFP obsługujących wszystkie wymienione tryby pracy (breakout) 4x10GE, 4x25GE, 1x40GE, 2x50GE, 1x100GE: 8 |  |
| Minimalna ilość portów SFP+ obsługujących 1GE/10GE/25GE: 48 |  |
| Przełącznik musi być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. W celu zachowania redundancji zasilania, każdy przełącznik musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu przełącznika oraz ograniczenia jego funkcjonalności i wydajności. Dostarczone zasilacze muszą umożliwiać poprawną pracę przełącznika w pełnej konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy. |  |
| Obudowa przeznaczona do montażu w szafie rackowej 19”, maksymalny rozmiar w jednostkach RackUnit (wysokość): 1RU |  |
| Maksymalna głębokość obudowy 46,8 [cm] |  |
| Wymagany kierunek przepływu powietrza (Front określony jako lokalizacja portów we/wy): 2x Front-Back, 2x Back-Front |  |
| Przełącznik musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 95% zakładając brak występowania zjawiska kondensacji pary wodnej. |  |
| Przełącznik musi poprawnie pracować w zakresie temperatur od 0° do 40° C |  |
| Wszystkie komponenty (sprzęt i system operacyjny) muszą pochodzić od jednego dostawcy |  |
| Elementy muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje dostawca musi je dostarczyć wraz z urządzeniami. Licencje nie mogą być czasowe. Restart Elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia - nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji. |  |
| Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach |  |
| Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. zasilacze, karty z interfejsami sieciowymi, moduły optyczne) w trakcie pracy urządzenia (ang. hot-swap). |  |
| Przełącznik musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom i widoczne publicznie na stronie producenta. Niedopuszczalne jest wykorzystanie przełączników prototypowych. |  |
| Oprogramowanie (system operacyjny) musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby projektu - nieoferowanej innym klientom. |  |
| Moduły optycznie (ang. transceiver) muszą pochodzić od producenta elementów sieciowych. Jednakże, karty liniowe, moduły lub porty przełącznika zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi, muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów bez utraty gwarancji dla przełącznika. Restart przełącznika nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych, które pozwolą na wykorzystywanie modułów optycznych innych producentów |  |
| Wszystkie przełączniki oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane za wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale) ani nie może być wiadomym, że urządzenia te nie będą objęte pomocą techniczną producenta (ang. end of life). |  |
| Usługi wsparcia muszą obejmować dostęp do wszelkich aktualizacji, łat i poprawek (w tym możliwość podniesienia wersji oprogramowania systemowego i zarządzającego do najnowszej wersji udostępnianej przez producenta) bez dodatkowych opłat. |  |
| Usługi wsparcia muszą być dostarczane i gwarantowane bezpośrednio przez producenta. |  |
| **Parametry wydajnościowe** | Minimalna wydajność przełączania sprzętowego full-duplex: 4 Tbps |  |
| Minimalna ilość przetwarzanych pakietów na sekundę: 1 Bpps |  |
| Opóźnienie przełączania pakietów nie większe niż: 0,8 µs |  |
| Minimalny bufor przechowywujący pakiety per urządzenie: 32 MB |  |
| Maksymalna moc pobierana przez urządzenie: 290 W |  |
| Typowa maksymalna moc pobierana przez urządzenie (przy 25 stopni Celsjusza i obciążeniu 50%): 119 W |  |
| **Funkcjonalność dla warstwy L2** | Przełącznik musi umożliwiać Trunking IEEE 802.1Q VLAN; |  |
| Minimalny rozmiar ramki Jumbo dla wszystkich portów (Jumbo Frame): 9216 |  |
| Minimalna ilość obsługiwanych VLANów dostępna dla użytkowników: 4096 |  |
| Minimalna ilość obsługiwanych adresów MAC: 288 000 |  |
| Minimalna ilość grup Link Aggregation Control Protocol (LACP): IEEE 802.3ad: 128 |  |
| Minimalna ilość portów w grupie LACP IEEE 802.3ad: 64 |  |
| Przełącznik musi obsługiwać IEEE 802.1s Multiple Spanning Tree (MST), IEEE 802.1w Rapid Spanning Tree (RSTP) oraz Rapid Per VLAN Spanning Tree (RPVST+) |  |
| Przełącznik musi posiadać mechanizmy zabezpieczenia przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) |  |
| Przełącznik musi umożliwiać stworzenie nadmiarowości, pozwalającej na terminowanie zagregowane interfejsy (LAG) na dwóch przełącznikach sieciowych (ang. Dual Homing) - odpowiednik rozwiązania vPC, Multichasis LAG. W ramach takiej protekcji wszystkie porty zagregowanego połączenia LAG muszą aktywnie przenosić dane (ang. Active/Active). Awaria jednego Elementu nie może wpływać na status połączenia zagregowanego. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree. |  |
| Wsparcie sprzętowe dla tunelowania QinQ i QinVNI |  |
| Obsługa Selective QinQ |  |
| Wsparcie sprzętowe dla VLAN translation |  |
| Wsparcie dla IGMPv2, IGMPv3, MLDv2 |  |
| Wsparcie dla IGMP snooping i MLDv2 snooping |  |
| **Funkcjonalność dla warstwy L3** | Sprzętowe przełączanie pakietów w warstwie L3 dla IPv4 i IPv6 |  |
| Routing w oparciu o trasy statyczne |  |
| Minimalna ilość wpisów IPv4 LPM obsługiwanych sprzętowo: 360 000 |  |
| Minimalna ilość obsługiwanych jednoczesnych ścieżek o równej metryce (ECMP): 128 |  |
| Protekcja VRRP i VRRPv3 |  |
| Przełącznik musi obsługiwać bezstanowy protokół First Hop Redundancy Protocol umożliwiający konfigurację wirtualnego adresu bramy na więcej niż dwóch urządzeniach, gdzie wszystkie urządzenia są jednocześnie aktywne. Funkcja nie może wymagać konfiguracji fizycznego IP innego każdym urządzeniu (jak w przypadku np. HSRP, VRRP). |  |
| Wsparcie dla wirtualnych tablic routingu VRF |  |
| Routing w oparciu o OSPF dla protokołów IPv4 oraz IPv6. |  |
| Routing w oparciu o BGP dla protokołów IPv4 oraz IPv6. |  |
| Routing w oparciu o ISIS dla protokołów IPv4 oraz IPv6. Obsługa wielu instancji ISIS |  |
| Obsługa weryfikacji wpisów BGP poprzez RPKI (Resource Public Key Infrastructure) |  |
| Wsparcie dla BFD (Bidirectional Forwarding Protocol) |  |
| Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) |  |
| Możliwość zmian routingu poprzez zdefiniowane polityki (PBR Policy-based routing) |  |
| Możliwość obsługi NAT (Network Address Translation) w trybie statycznym i dynamicznym |  |
| Obsługa sprzętowego tunelowania IP poprzez GRE. |  |
| **Funkcjonalność zapewnienia jakości obsługi w sieci** | Obsługa Layer 2 IEEE 802.1p (CoS) oraz DSCP |  |
| Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) |  |
| Kolejkowanie bezwzględne (strict-priority) |  |
| Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych. |  |
| Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |  |
| Obsługa ECN (Explicit Congestion Notification) |  |
| Obsługa PFC (Priority Flow Control) IEEE 802.1Qbb |  |
| Obsługa Pause Flow Control Tx 802.3x |  |
| **Funkcjonalność dla warstwy VXLAN i EVPN** | Elementy przełączające muszą obsługiwać MP-BGP EVPN (Ethernet VPN) jako mechanizm sygnalizacyjny (ang control-plane) i enkapsulacji VXLAN w szczególności urządzenia muszą mieć możliwość pełnienia funkcji Route-Reflector |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę przełączania w warstwie drugiej (bridging) zawartości pakietów przy enkapsulacji VXLAN. Protokołem sterującym musi być MP-BGP EVPN |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę przełączania w warstwie drugiej (bridging) zawartości pakietów przy enkapsulacji VXLAN z funkcjonalnością łączenia VLANów (BGP L2 EVPN VLAN aware bundle) |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę routingu w warstwie trzeciej zawartości pakietów przy enkapsulacji VXLAN. Protokołem sterującym musi być MP-BGP EVPN. Musi być możliwa obsługa routingu IP w trybie symetrycznym i asymetrycznym |  |
| Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) |  |
| Obsługa optymalizacji rozpływu multicastów w środowisku EVPN/VXLAN (OISM, EVPN Multicast Type-6, Type-7, Type-8) |  |
| Obsługa translacji VLAN, QinQ przy konfiguracji z VXLAN i EVPN |  |
| Urządzenie musi zapewnić wystarczającą skalowalność usług L2 (VLAN) przy konfiguracji EVPN/VXLAN (VNI per VLAN). Tak żeby było możliwe skonfigurowanie przynajmniej 4000 VLANów (802.1q trunk) na każdym porcie urządzenia poza dwoma przeznaczonymi dla obsługi EVPN/VXLAN. |  |
| Obsługa protekcji All-Active EVPN wykorzystując ESI (Ethernet Segment Identifier) |  |
| Obsługa protekcji Active-Standby EVPN wykorzystując ESI (Ethernet Segment Identifier) |  |
| Obsługa Multicast DNS (mDNS) przy konfiguracji z VXLAN i EVPN |  |
| **Funkcjonalność zarządzania i zabezpieczeń** | Dedykowany port zarządzający 10/100/1000 Baste-T (out-of-band) |  |
| Dedykowany port konsoli |  |
| Możliwość zarządzania In-band |  |
| Obsługa SSHv2, Telnet |  |
| RADIUS; Radius over TLS (szyfrowanie) |  |
| TACACS+ |  |
| Syslog; Syslog z możliwościa szyfrowania TLS |  |
| SNMP v1, v2c, v3; |  |
| Minimalna ilość wpisów ACL (access control list) obługiwanych sprzętowo: 4000 |  |
| Obsługa IEEE 802.1ab LLDP |  |
| Network Time Protocol (NTP, NTPv6). Funkcjonalność nie może wykluczać się z obsługą VXLAN, oraz terminowania pojedynczej wiązki LACP na 2 niezależnych przełącznikach (odpowiednik rozwiązania vPC, Multichasis LAG) |  |
| Precision Time Protocol IEEE1588 właczając ITU-TG.8275.1 dla Boundary Clock, Transparent Clock. Funkcjonalność nie może wykluczać się z obsługą VXLAN, oraz terminowania pojedynczej wiązki LACP na 2 niezależnych przełącznikach (odpowiednik rozwiązania vPC, Multichasis LAG) |  |
| Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |  |
| Monitorowanie parametrów optycznych DOM (Digital Optical Monitoring) |  |
| Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, na interfejs docelowy lub GRE za pośrednictwem specjalnego mechanizmu (mirroring, SPAN) |  |
| Administrator powinien mieć możliwość zdalnego zasygnalizowania/wyróżnienia urządzenia w celu łatwiejszej identyfikacji np. poprzez zdalne zapalenie dedykowanych diod. Funkcjonalność ta określana jest jako ang. Blue Beacon |  |
| Przełącznik musi mieć możliwość dostarczania danych o parametrach jakościowych łączy do innych przełączników. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss). Dane te muszą być poprawnie interpretowane i prezentowane w Systemie Zarządzania |  |
| Możliwość modyfikacji konfiguracji z potwierdzeniem zmian (commit), konfiguracja nie jest aktywna dopóki nie zostanie wydana komenda potwierdzenie. Musi istnieć możliwość wskazania czasu, po którym wymagane jest dodatkowe potwierdzenie poprawności zmian konfiguracji, w przeciwnym wypadku system musi wrócić automatycznie do poprzedniego stanu (rollback). |  |
| Możliwość diagnostyki wykorzystując podstawowe narzędzia Ping i Traceroute |  |
| Telemetria w oparciu o mechanizm strumieniowania, zapewniający (alternatywnie do SNMP) wysyłanie danych o stanie urządzenia poprzez protokoły gRPC lub Netconf. Bez konieczności czasu rzeczywistego |  |

Specyfikacja techniczna przełączników sieciowych (dostępowe) – 18 szt. - ………………………………………

Producent/model

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Minimalne wymagania** | **Parametry techniczne oferowanego produktu /spełnia – nie spełnia/** |
| **Konfiguracja fizyczna** | Minimalna ilość portów SFP+ obsługujących 1GE/10GE: 4 |  |
| Minimalna ilość portów RJ45 10M/100M/1G zasilaniem PoE 30W (802.3af/at): 48 |  |
| Przełącznik musi być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. W celu zachowania redundancji zasilania, każdy przełącznik musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu przełącznika oraz ograniczenia jego funkcjonalności i wydajności. Dostarczone zasilacze muszą umożliwiać poprawną pracę przełącznika w pełnej konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy. |  |
| Obudowa przeznaczona do montażu w szafie rackowej 19”, maksymalny rozmiar w jednostkach RackUnit (wysokość): 1RU |  |
| Maksymalna głębokość obudowy 43 [cm] |  |
| Wymagany kierunek przepływu powietrza (Front określony jako lokalizacja portów we/wy): Front-Back |  |
| Przełącznik musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 95% zakładając brak występowania zjawiska kondensacji pary wodnej. |  |
| Przełącznik musi poprawnie pracować w zakresie temperatur od 0° do 40° C |  |
| Wszystkie komponenty (sprzęt i system operacyjny) muszą pochodzić od jednego dostawcy |  |
| Elementy muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje dostawca musi je dostarczyć wraz z urządzeniami. Licencje nie mogą być czasowe. Restart Elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia - nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji. |  |
| Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach |  |
| Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów optycznych w trakcie pracy urządzenia (ang. hot-swap). |  |
| Przełącznik musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom i widoczne publicznie na stronie producenta. Niedopuszczalne jest wykorzystanie przełączników prototypowych. |  |
| Oprogramowanie (system operacyjny) musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby projektu - nieoferowanej innym klientom. |  |
| Moduły optycznie (ang. transceiver) muszą pochodzić od producenta elementów sieciowych. Jednakże, karty liniowe, moduły lub porty przełącznika zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi, muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów bez utraty gwarancji dla przełącznika. Restart przełącznika nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych, które pozwolą na wykorzystywanie modułów optycznych innych producentów |  |
| Wszystkie przełączniki oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane za wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale) ani nie może być wiadomym, że urządzenia te nie będą objęte pomocą techniczną producenta (ang. end of life). |  |
| Usługi wsparcia muszą obejmować dostęp do wszelkich aktualizacji, łat i poprawek (w tym możliwość podniesienia wersji oprogramowania systemowego i zarządzającego do najnowszej wersji udostępnianej przez producenta) bez dodatkowych opłat. |  |
| Usługi wsparcia muszą być dostarczane i gwarantowane bezpośrednio przez producenta. |  |
| **Parametry wydajnościowe** | Minimalna wydajność przełączania sprzętowego full-duplex: 176 Gbps |  |
| Minimalna ilość przetwarzanych pakietów na sekundę: 131 Mpps |  |
| Opóźnienie przełączania pakietów nie większe niż: 1,2 µs |  |
| Minimalny bufor przechowywujący pakiety per urządzenie: 4 MB |  |
| Maksymalna moc pobierana przez urządzenie: 830 W |  |
| **Funkcjonalność dla warstwy L2** | Przełącznik musi umożliwiać Trunking IEEE 802.1Q VLAN; |  |
| Minimalny rozmiar ramki Jumbo dla wszystkich portów (Jumbo Frame): 9216 |  |
| Minimalna ilość aktywnych VLANów dostępna dla użytkowników: 1021 |  |
| Minimalna ilość obsługiwanych adresów MAC: 64 000 |  |
| Minimalna ilość grup Link Aggregation Control Protocol (LACP): IEEE 802.3ad: 8 |  |
| Minimalna ilość portów w grupie LACP IEEE 802.3ad: 8 |  |
| Przełącznik musi obsługiwać IEEE 802.1s Multiple Spanning Tree (MST), IEEE 802.1w Rapid Spanning Tree (RSTP) oraz Rapid Per VLAN Spanning Tree (RPVST+) |  |
| Przełącznik musi posiadać mechanizmy zabezpieczenia przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) |  |
| Przełącznik musi umożliwiać stworzenie nadmiarowości, pozwalającej na terminowanie zagregowane interfejsy (LAG) na dwóch przełącznikach sieciowych (ang. Dual Homing) - odpowiednik rozwiązania vPC, Multichasis LAG. W ramach takiej protekcji wszystkie porty zagregowanego połączenia LAG muszą aktywnie przenosić dane (ang. Active/Active). Awaria jednego Elementu nie może wpływać na status połączenia zagregowanego. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree. |  |
| Wsparcie sprzętowe dla tunelowania QinQ i QinVNI |  |
| Wsparcie dla IGMPv2, IGMPv3, MLDv2 |  |
| Wsparcie dla IGMP snooping i MLDv2 snooping |  |
| **Funkcjonalność dla warstwy L3** | Sprzętowe przełączanie pakietów w warstwie L3 dla IPv4 i IPv6 |  |
| Routing w oparciu o trasy statyczne |  |
| Minimalna ilość wpisów IPv4 LPM obsługiwanych sprzętowo: 32 000 |  |
| Minimalna ilość obsługiwanych jednoczesnych ścieżek o równej metryce (ECMP): 64 |  |
| Protekcja VRRP i VRRPv3 |  |
| Przełącznik musi obsługiwać bezstanowy protokół First Hop Redundancy Protocol umożliwiający konfigurację wirtualnego adresu bramy na więcej niż dwóch urządzeniach, gdzie wszystkie urządzenia są jednocześnie aktywne. Funkcja nie może wymagać konfiguracji fizycznego IP innego każdym urządzeniu (jak w przypadku np. HSRP, VRRP). |  |
| Wsparcie dla wirtualnych tablic routingu VRF |  |
| Routing w oparciu o OSPF dla protokołów IPv4 oraz IPv6. |  |
| Routing w oparciu o BGP dla protokołów IPv4 oraz IPv6. |  |
| Routing w oparciu o ISIS dla protokołów IPv4 oraz IPv6. Obsługa wielu instancji ISIS |  |
| Obsługa weryfikacji wpisów BGP poprzez RPKI (Resource Public Key Infrastructure) |  |
| Wsparcie dla BFD (Bidirectional Forwarding Protocol) |  |
| Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) |  |
| Możliwość zmian routingu poprzez zdefinowane polityki (PBR Policy-based routing) |  |
| **Funkcjonalność zapewnienia jakości obsługi w sieci** | Obsługa Layer 2 IEEE 802.1p (CoS) oraz DSCP |  |
| Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) |  |
| Kolejkowanie bezwzględne (strict-priority) |  |
| Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych. |  |
| Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |  |
| Obsługa ECN (Explicit Congestion Notification) |  |
| Obsługa PFC (Priority Flow Control) IEEE 802.1Qbb |  |
| Obsługa Pause Flow Control Tx 802.3x |  |
| **Funkcjonalność dla warstwy VXLAN i EVPN** | Elementy przełączające muszą obsługiwać MP-BGP EVPN (Ethernet VPN) jako mechanizm sygnalizacyjny (ang control-plane) i enkapsulacji VXLAN w szczególności urządzenia muszą mieć możliwość pełnienia funkcji Route-Reflector |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę przełączania w warstwie drugiej (bridging) zawartości pakietów przy enkapsulacji VXLAN. Protokołem sterującym musi być MP-BGP EVPN |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę przełączania w warstwie drugiej (bridging) zawartości pakietów przy enkapsulacji VXLAN z funkcjonalnością łączenia VLANów (BGP L2 EVPN VLAN aware bundle) |  |
| Elementy przełączające muszą zapewniać sprzętową obsługę routingu w warstwie trzeciej zawartości pakietów przy enkapsulacji VXLAN. Protokołem sterującym musi być MP-BGP EVPN. Musi być możliwa obsługa routingu IP w trybie symetrycznym i asymetrycznym |  |
| Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) |  |
| Obsługa translacji VLAN, QinQ przy konfiguracji z VXLAN i EVPN |  |
| Obsługa protekcji All-Active EVPN wykorzystując ESI (Ethernet Segment Identifier) |  |
| Obsługa protekcji Active-Standby EVPN wykorzystując ESI (Ethernet Segment Identifier) |  |
| **Funkcjonalność zarządzania i zabezpieczeń** | Dedykowany port zarządzający 10/100/1000 Baste-T (out-of-band) |  |
| Dedykowany port konsoli |  |
| Możliwość zarządzania In-band |  |
| Obsługa SSHv2, Telnet |  |
| RADIUS; Radius over TLS (szyfrowanie) |  |
| TACACS+ |  |
| Syslog; Syslog z możliwościa szyfrowania TLS |  |
| SNMP v1, v2c, v3; |  |
| Minimalna ilość wpisów ACL (access control list) obługiwanych sprzętowo: 4000 |  |
| Obsługa IEEE 802.1ab LLDP |  |
| Network Time Protocol (NTP, NTPv6). Funkcjonalność nie może wykluczać się z obsługą VXLAN, oraz terminowania pojedynczej wiązki LACP na 2 niezależnych przełącznikach (odpowiednik rozwiązania vPC, Multichasis LAG) |  |
| Precision Time Protocol IEEE1588 właczając ITU-TG.8275.1 dla Boundary Clock, Transparent Clock. Funkcjonalność nie może wykluczać się z obsługą VXLAN, oraz terminowania pojedynczej wiązki LACP na 2 niezależnych przełącznikach (odpowiednik rozwiązania vPC, Multichasis LAG) |  |
| Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |  |
| Monitorowanie parametrów optycznych DOM (Digital Optical Monitoring) |  |
| Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, na interfejs docelowy lub GRE za pośrednictwem specjalnego mechanizmu (mirroring, SPAN) |  |
| Administrator powinien mieć możliwość zdalnego zasygnalizowania/wyróżnienia urządzenia w celu łatwiejszej identyfikacji np. poprzez zdalne zapalenie dedykowanych diod. Funkcjonalność ta określana jest jako ang. Blue Beacon |  |
| Przełącznik musi mieć możliwość dostarczania danych o parametrach jakościowych łączy do innych przełączników. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss). Dane te muszą być poprawnie interpretowane i prezentowane w Systemie Zarządzania |  |
| Możliwość modyfikacji konfiguracji z potwierdzeniem zmian (commit), konfiguracja nie jest aktywna dopóki nie zostanie wydana komenda potwierdzenie. Musi istnieć możliwość wskazania czasu, po którym wymagane jest dodatkowe potwierdzenie poprawności zmian konfiguracji, w przeciwnym wypadku system musi wrócić automatycznie do poprzedniego stanu (rollback). |  |
| Możliwość diagnostyki wykorzystując podstawowe narzędzia Ping i Traceroute |  |
| Telemetria w oparciu o mechanizm strumieniowania, zapewniający (alternatywnie do SNMP) wysyłanie danych o stanie urządzenia poprzez protokoły gRPC lub Netconf. Bez konieczności czasu rzeczywistego |  |

Specyfikacja techniczna systemu zarządzania i monitorowania sieci – 1 szt. - …..……………………………

Producent/nazwa oprogramowania

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Minimalne wymagania** | **Parametry techniczne oferowanego produktu /spełnia – nie spełnia/** |
| **Wymagania ogólne** | Interfejs użytkownika systemu zarządzania musi być dostępny z poziomu przeglądarki WWW bez konieczności instalowania dedykowanego oprogramowania klienta/administratora. Musi być zapewniona prawidłowa obsługa co najmniej następujących przeglądarek: Microsoft IE, Firefox, Google Chrome. |  |
| System Zarządzania (Kontroler) musi obsługiwać jednoczesną pracę wielu użytkowników. |  |
| "System Zarządzania (Kontroler) musi zapewniać możliwość zdalnego aktualizowania firmware’u (oprogramowania) dla zarządzanych Elementów, z możliwością wycofania i przywrócenia poprzedniej wersji firmware. Musi być możliwość przeprowadzenia procesu aktualizacji dla wielu Elementów jednocześnie, proces może rozpocząć się natychmiast lub w zaplanowanym czasie. System Zarządzania (Kontroler) musi zapewnić weryfikację nowo dodanego firmware pod kątem jego poprawności i integralności." |  |
| System Zarządzania (Kontroler) musi zapewniać możliwość wykorzystania interfejsu programistycznego (REST API) do wykonywania typowych operacji konfigurowania takich jak tworzenie, dodawanie i implementowanie Modułów Konfiguracyjnych (ang configlet) |  |
| Niedostępność Systemu Zarządzania nie może mieć jakiegokolwiek wpływu na zarządzane Elementy. W szczególności nie może uniemożliwiać lub ograniczać możliwością konfigurowania urządzeń za pomocą interfejsu CLI |  |
| System Zarządzania (Kontroler) musi być dostarczony jako skonfigurowany obraz maszyny wirtualnej do uruchomienia na platformie KVM lub VMWare. Maksymalne wymagania Systemu Zarządzania nie mogą przekroczyć 16 cores CPU, 32 GB RAM, 1TB HDD. Jeśli System Zarządzania (Kontroler) przekracza te wymagania wykonawca musi dostarczyć platformę sprzętową która zapewni odpowiednie parametry. |  |
| System Zarządzania (Kontroler) musi posiadać możliwość realizacji funkcji AAA poprzez integrację z zewnętrznym serwerem Radius oraz z zewnętrznym serwerem TACACS (przy czym nie jest wymagana integracja z dwoma tymi serwerami jednocześnie) |  |
| Licencja dostarczona wraz z systemem zarządzania musi umożliwić stworzenie klastra zapewniającego tryb wysokiej dostępności tak, aby awaria sprzętowa wyłączająca jedną z instancji nie powodowała przerwy w działaniu całego Systemu Zarządzania. |  |
| **Wymagania dla funkcjonalności monitorowania i wizualizacji** | "System Zarządzania (Kontroler) musi umożliwiać zbieranie i wizualizacja w postaci tabel i wykresów następujących parametrów:  - Parametry urządzenia: nazwa, model, numer seryjny, wersja firmware, wykorzystanie CPU, pamięci RAM, temperatura pracy.  - Interfejsy: stan administracyjny (aktywny, wyłączony, itp.), prędkość pracy, adres IP, statystyki ruchowe dla transmisji i odbioru, statystyki błędów, wartość MTU  - Synchronizacji czasu: PTP (status i parametry),  - Ethernet: tablica MAC, wpisy ARP  - IP routing: zbudowana tablica routingu IPv4 i IPv6, (wliczając wirtualne tablice routingu VRF),  - BGP: numery AS, zestawione sąsiedztwa" |  |
| System Zarządzania (Kontroler) musi zapewniać wizualizację topologii połączeń zarządzanych Elementów. Topologia połączeń musi być automatycznie wykrywana i budowana. |  |
| Na planie topologii połączeń, System Zarządzania (Kontroler) musi wizualizować:  - wydarzenia i alarmy  - szybkości interfejsów  - wykorzystanie pasma  - błędy w postaci utraconych pakietów  - przepływy pakietów dla wskazanych par IP i protokołów  - rozkład dystrybucji VLAN oraz VXLAN VNI |  |
| Wszystkie parametry muszą być wizualizowane w czasie rzeczywistym (odpowidającym zmianom w urządzeniach sieciowych) oraz historycznie z możliwością wyboru dowolnego przedziału czasowego z ostatniego miesiąca zbieranych danych. System Zarządzania (Kontroler) musi umożliwiać budowanie i komponowanie własnych zestawień parametrów do obserwacji |  |
| System Zarządzania (Kontroler) musi zbierać i prezentować parametry jakości transmisji pomiędzy Elementami przełączającymi. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss). |  |
| System Zarządzania (Kontroler) musi zbierać i prezentować informację o przepływach pakietów danych w postaci par IP i protokołów w postaci wykresów oraz wizualizować na topologi sieci. Dane zbierane są poprzez otwarte protokoły typu sFlow lub IPFIX |  |
| "System Zarządzania (Kontroler) musi umożliwiać definiowanie i budowanie własnych widoków (ang Dashboad), na których mogą być prezentowane dane dotyczące |  |
| **Wymagania dla funkcjonalności obsługi alarmów** | System Zarządzania (Kontroler) musi zbierać i prezentować alarmy generowane przez zarządzane Elementy. Alarmy muszą obejmować zdarzenia generowane przez syslog, zmiany stanu interfejsów, przekroczenia progów błędów na interfejsach wejściowych (CRC), przeciążenia ruchowe interfejsów wejściowych i wyjściowych. |  |
| System Zarządzania (Kontroler) musi zapewnić mechanizm potwierdzania alarmów i dodawania komentarzy. |  |
| System Zarządzania (Kontroler) musi zapewnić mechanizm wyróżniania ważności alarmów i zdarzeń oraz możliwość ich modyfikacji. Przy wyświetlaniu alarmów powinna być możliwość filtrowania alarmów pod kątem ważności |  |
| System Zarządzania (Kontroler) musi umożliwiać definiowanie progów po których przekroczeniu generowany jest alarm. Dotyczy to takich parametrów jak Obciążenia CPU, problemów z PTP, temperatur wkładek optycznych. |  |
| System Zarządzania (Kontroler) musi umożliwiać przekierowywanie alarmów do innych platform takich jak Email (SMTP), narzędzi analizujących logi i alarmy typu SIEM (np. Slack), klientów komunikatorów chat. |  |
| **Wymagania dla funkcjonalności wyszukiwania i analizy anomalii** | System Zarządzania (Kontroler) musi zapewnić możliwość dodawania prywatnych identyfikatorów Elementów oraz interfejsów, które następnie wspomagają proces wyszukiwania. |  |
| System Zarządzania (Kontroler) musi umożliwiać wyszukiwanie adresów IP oraz MAC widocznych z poziomu zarządzanych Elementów. Możliwość wyszukiwania dotyczy adresów statycznych i dynamicznych tablicach poszczególnych Elementów. Odnalezione adresy muszą być prezentowane wraz z kontekstem opisującym Elementy oraz interfejsy/tablice związane z danym adresem. |  |
| System Zarządzania (Kontroler) musi umożliwiać porównywanie i wizualizację różnic pomiędzy parametrami dla dwu dowolnych zarządzanych Elementów we wskazanych momentach czasowych. Parametrami podlegającymi porównaniu muszą być konfiguracje urządzeń, podstawowe tablice danych sieciowych (adresy IP, adresy MAC, wpisy ARP, sąsiedztwa sieciowe na bazie LLDP, tablice VXLAN, tablice NDP, tablice routingu IPv4, tablice routingu IPv6, tablice multicast IPv4 ). System musi umożliwiać równoczesne porównywanie stanu wymienionych metryk dwóch różnych urządzeń w niezależnych punktach czasu dla każdego z urządzeń. Np. Porównanie tablicy routingu IPv4 urządzenia A z godziny X z tablicą routingu urządzenia B z godziny Y. |  |
| System Zarządzania (Kontroler) musi na bieżąco (bez wymuszenia) sygnalizować modyfikację konfiguracji wykonaną z poziomu konsoli Elementów przełączający, która wprowadza różnicę pomiędzy konfiguracją budowaną przez System Zarządzania (Kontroler) a wprowadzoną na urządzeniu. Administrator Systemu Zarządzania powinien mieć możliwość przywrócenia poprzedniej konfiguracji lub akceptacji zmian dokonanych na poziomie konsoli. |  |
| System Zarządzania (Kontroler) musi prezentować informację o podatnościach bezpieczeństwa i wykrytych błędach dla zarządzanych Elementów. Jednocześnie sugerując właściwe wersje oprogramowania. |  |
| **Wymagania dla funkcjonalności zestawiania i konfigurowania usług (ang. provisioning)** | Za pomocą Systemu Zarządzania (kontrolera) musi istnieć możliwość skonfigurowania wszystkich parametrów zarządzanych Elementów. |  |
| System Zarządzania (Kontroler) musi umożliwiać budowanie konfiguracji Elementów. Konfiguracja musi być zgodna z konfiguracją tworzoną z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface / CLI). |  |
| Zintegrowanie Elementów z systemem zarządzania nie może wykluczać bezpośredniej pracy z interfejsami administracyjnymi Elementów. Rozwiązanie musi umożliwiać wymienną konfigurację Elementów: poprzez System Zarządzania (Kontroler) lub bezpośrednio z wykorzystaniem interfejsu tekstowego (ang. CLI). |  |
| System Zarządzania (Kontroler) musi wykrywać i wizualizować rozbieżności pomiędzy konfiguracją wynikającą z parametrów zdefiniowanych na systemie zarządzania oraz parametrów skonfigurowanych bezpośrednio na Elementach. |  |
| System Zarządzania (Kontroler) musi dostarczyć mechanizm budowania konfiguracji Elementów z wykorzystywaniem Modułów Konfiguracyjnych (części konfiguracji CLI, ang configlet). Musi istnieć możliwość wykorzystania Modułów Konfiguracyjnych w trybie hierarchicznym, to znaczy że Moduł Konfiguracji jest dziedziczony przez wszystkie Elementy znajdujące się w danej hierarchii. Modyfikacja Modułu Konfiguracji musi powodować odpowiednią zmianę konfiguracji wszystkich Elementów znajdujących się w danej hierarchii. |  |
| System musi umożliwiać budowanie hierarchii Modułów Konfiguracyjnych dla jednego i kilku obszarów lub likalizacji (Data Center). |  |
| Moduły Konfiguracji muszą być dostępne w trybie tekstowym (analogicznie jak pliki konfiguracyjne interfejsu tekstowego CLI). Ponadto, musi istnieć mechanizm automatyzacji tworzenia Modułów Konfiguracyjnych wykorzystując języka skryptów oparty na języku Python lub Perl. Tworzenie, testowanie, uruchamianie i zarządzanie skryptami Python/Perl musi w całości odbywać się poprzez interfejs GUI systemu zarządzania i musi stanowić integralną część tego systemu. |  |
| System Zarządzania (Kontroler) musi dostarczyć mechanizm weryfikacji oczekiwanych wyników przed implementacją Modułów Konfiguracyjnych na zarządzanych Elementach. Po implementacji zmian konfiguracyjnych opisanych w Modułach Konfiguracyjnych musi istnieć mechanizm wycofania tych zmian. |  |
| System Zarządzania (Kontroler) musi zapewnić automatyczną procedurę budowania konfiguracji początkowej (ang. ZTP „Zero Touch Provisioning). W szczególności, nowe urządzenie, z konfiguracją fabryczną, po podłączeniu do sieci, powinno za pomocą DHCP odnaleźć System Zarządzania (Kontroler) a następnie pobrać konfigurację początkową i automatycznie zintegrować się z systemem zarządzania. Proces ten musi uwzględniać automatyczną aktualizację oprogramowania urządzenia sieciowego do wskazanej wersji. |  |
| System Zarządzania (Kontroler) musi zapewnić funkcjonalność „Nadzoru Nad Zmianami” (ang. Change Control). W ramach tej funkcjonalności administrator musi mieć możliwość: A) weryfikacji zmiany konfiguracji przed implementacją. B) implementację zmiany. C) możliwość wycofania zmiany. |  |
| System Zarządzania (Kontroler) musi umożliwiać proces automatyzacji wielu zmian konfiguracyjnych i grupowania ich w pakiety (obejmujące wiele Elementów). System musi umożliwiać wykonywanie niestandardowych akcji (np. wykonania skryptu) jako jeden z elementów pakietów zamian. System musi umożliwiać zatrzymanie wykonywania kolejnych zmian w sekwencji, jeżeli zamiany je poprzedzające się nie powiodą. System musi umożliwiać zatwierdzanie pakietu zmian przez upoważnionego użytkownika zanim możliwe będzie uruchomienie pakietu. |  |
| System Zarządzania (Kontroler) musi zapewniać możliwość zapisania i odtworzenia kopi zapasowej Modułów Konfiguracyjnych. |  |
| System Zarządzania (Kontroler) musi zapewnić możliwość samodzielnego budowania uproszczonych narzędzi konfiguracyjnych (wizards) w ramach, których podawane są parametry wejściowe w formie graficznej (okna, zaznaczanie opcji, itp.) |  |

**Dodatkowo**:

Każde z urządzeń musi być wyposażone w port USB umożliwiający podłączenie nośnika klasy Flash. Port USB musi umożliwiać awaryjne uruchomienie urządzenia w przypadku awarii wewnętrznego modułu Flash. W sytuacji uruchomienia urządzenia z portu USB urządzenie musi korzystać z tego nośnika bez żadnych ograniczeń – tak jakby pracowało na fabrycznym module Flash/SSD.

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Minimalne wymagania** | **Parametry techniczne oferowanego produktu /spełnia – nie spełnia/** |
| **Gwarancja** | Serwis gwarancyjny musi być świadczony bezpośrednio przez producenta oferowanej platformy sprzętowej.  Wsparcie powinno być świadczone 24x7x365.  W ramach świadczonej usługi serwisowej zagwarantowany zostanie dostęp do nowych wersji systemu operacyjnego, poprawek, uaktualnień oraz możliwość zakładania zgłoszeń serwisowych bezpośrednio na portalu producenta lub telefonicznie. |  |
| Dostarczane razem z urządzeniami subskrypcje oraz wsparcie serwisowe muszą funkcjonować przez 60 miesięcy. |
| W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zostało ono wymienione w trybie Next-Business-Day czyli w następnym dniu roboczym. |

(Dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym osoby umocowanej do reprezentowania Wykonawcy)