**OPIS PRZEDMIOTU ZAMÓWIENIA (dalej: OPZ)**

1. **Przedmiotem zamówienia jest:**

wdrożenie tj. dostawa, instalacja i konfiguracja Sprzętu dla Oprogramowania SDN Zamawiającego na potrzeby komunikacji w sieci LAN Data Center OPR (Ośrodek Przetwarzania Radom) i OPP (Ośrodek Przetwarzania Praga w Warszawie) w postaci:

1. Dostawy Sprzętu tj. 2 szt. przełączników Spine do OPR wraz z wyposażeniem (okablowanie zasilające, okablowanie do łączenia z urządzeniami, moduły), spełniających wymagania zawarte w Rozdziale 3;
2. Instalacji i konfiguracji Oprogramowania SDN Zamawiającego dla wszystkich dostarczonych urządzeń w ramach pkt 1 i wszystkich posiadanych przez Zamawiającego przełączników wskazanych w Rozdziale 2 oraz wg wymagań zawartych w Rozdziale 11.
3. Dostawy Sprzętu tj. 2 szt. przełączników Spine do OPP wraz z wyposażeniem (okablowanie zasilające, okablowanie do łączenia z urządzeniami, moduły), spełniających wymagania zawarte w Rozdziale 4;
4. Dostawy Sprzętu tj. 6 szt. przełączników Leaf do OPP wraz z wyposażeniem (okablowanie zasilające, okablowanie do łączenia z urządzeniami, moduły), spełniających wymagania zawarte w Rozdziale 5;
5. Dostawy serwera – arbitra do OPW (Ośrodek Przetwarzania Warszawa), spełniającego wymagania zawarte w Rozdziale 6;
6. Dostawa, instalacja i konfiguracja Oprogramowania SDN w OPP, które będzie tworzyło klaster wysokiej dostępności z istniejącym Oprogramowaniem SDN Zamawiającego w OPR oraz konfiguracja wszystkich dostarczonych urządzeń w ramach pkt 3-5 wg wymagań zawartych w Rozdziale 11.
7. **Aktualnie eksploatowane środowisko Zamawiającego.**

Zamawiający posiada i wykorzystuje następujące przełączniki i oprogramowanie Huawei:

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Model przełącznika** | **Liczba** |
| 1. | CE6863E-48S6CQ-B Leaf | 30 |
| 2. | CES5731-H24T4XC | 60 |
| 3. | CE6865-48S8CQ-EI | 24 |
| 4. | CE12804 | 2 |
| 5. | CE6810-48S4Q-LI | 8 |
| 6. | S5720-56C-EI-AC | 2 |

1. Zarządzanie środowiskiem przełączników odbywa się z wykorzystaniem licencji eSight 21.0.0.SPC010. System do zarządzania środowiskiem IT - dalej nazywany NMS - obsługuje kompleksowo usługi zarządzania zarówno samymi elementami infrastruktury IT, jak również wszystkimi zdarzeniami w czasie ich cyklu życia. Zarządzanie opiera się o ramy modelu FCAPS (fault, configuration, accounting, performance and security). System posiada architekturę wysokiej dostępności, odporną na awarię całości systemu NMS, jak i poszczególnych jego części. System NMS wspiera funkcje i cechy systemu zarządzania eSight firmy Huawei, ze względu na dużą zainstalowaną bazę urządzeń producenta Huawei.
2. Oprogramowanie SDN Zamawiającego zrealizowane jest za pomocą NCE Huawei (wersja:iMaster NCE-Fabric V100R022C00SPC1b0) w Ośrodku Przetwarzania Radom.
3. Zamawiający wymaga, aby dostarczone urządzenia – przełączniki i licencje współpracowały z posiadanym środowiskiem Zamawiającego.
4. **Opis minimalnych wymagań funkcjonalnych dla** **urządzenia – przełącznika Spine w OPR typu Huawei CloudEngine CE8865-4C (lub równoważny).**

Przełączniki muszą być dostarczone do OPR.

|  |  |
| --- | --- |
| **Wymaganie** | **Minimalne parametry** |
| **Ogólne** | 1. Przełącznik warstwy trzeciej typu „Spine” o rozmiarze max 2U 2. Wyposażony w bufor o pojemności min 64MB. 3. Wszystkie interfejsy muszą być zatwierdzone przez producenta do użytku w oferowanym przełączniku. 4. Dostawa w obudowie przystosowanej do montażu w szafie 19” wraz z niezbędnym osprzętem (bez dostawy szafy) 5. Zasilanie: Napięcie zmienne: 230 V, 50 Hz 6. praca w temperaturze od 0 do 40 °C. 7. praca przy wilgotności powietrza od 10% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej |
| **Rodzaj portu/ilość i typ portów** | 1. 64 porty 40/100GE QSFP28 |
| **Zasilanie i system wentylacji** | 1. min 2 zasilacze z możliwością wymiany podczas pracy urządzenia. 2. min 2 wiatraki z możliwością wymiany podczas pracy urządzenia. 3. zapewniający przepływ powietrza w konfiguracjach front-to-back i back-to-front. |
| **Funkcjonalności** | 1. Przełącznik musi zapewniać możliwość obsługi technologii Multichassis Etherchannel (np. vPC lub M-LAG) lub innej równoważnej - łączącej przełączniki w 1 logiczną jednostkę 2. posiadać wsparcie dla min 128 konkurentnych ścieżek protokołu ECMP. 3. Wsparcie dla mechanizmów PFC oraz ECN 4. zapewnienie funkcjonalności zabezpieczenia portów przed wymuszeniem zmiany lokalizacji Root Bridge; 5. zapewnienie funkcjonalności prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym; 6. Min 30000 list dostępowych (ACL); 7. obsługa mikrosegmentacji lub równoważnego mechanizmu izolacji 8. obsługa mechanizmów obrony przed atakami DoS, ARP, and ICMP; 9. obsługa mechanizmów związane z zapewnieniem jakości usług w sieci: 10. Implementacja co najmniej ośmiu kolejek sprzętowych dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie; 11. zapewnienie obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority); 12. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP; 13. obsługa mechanizmów traffic policing, traffic shaping, congestion avoidance (RED lub WRED); 14. obsługa dla L2/L3/L4 ACL |
| **Wydajność** | * 1. Minimalna szybkość przełączania 16 Tbps;   przy spełnieniu wymagania  minimalna przepustowość: 2400 Mpps |
| **Wymagana funkcjonalność dla warstwy 2:** | * + - 1. trunking IEEE 802.1Q VLAN;       2. obsługa min. 4094 sieci VLAN;       3. obsługa min. 600 000 adresów MAC;       4. obsługa Rapid Spanning Tree: np. IEEE 802.1w, PVRST lub równoważne;       5. obsługa Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s);       6. Internet Group Management Protocol (IGMP) snooping;       7. Port Aggregation Protocol: np. IEEE 802.3ad;       8. prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast;       9. Wsparcie dla ramek Jumbo dla wszystkich portów (min 9198 bajtów); |
| **Wymagana funkcjonalność dla warstwy 3:** | * + - 1. obsługa protokołu VxLAN w modelach centralized and distributed gateway;       2. obsługa protokołu BGP eVPN;       3. obsługa 16 000 virtual tunnel endpoints (VTEPs)       4. obsługa 4000 VRFs       5. Minimalny rozmiar FIB 1,5M IPv4 / 750K IPv6;       6. Minimalna wielkość tablicy routingu multicast powinna być 30000;       7. Wsparcie dla protokołu IPv6;       8. Wsparcie dla protokołu BFD dla OSPF, BGP, IS-IS, oraz static route;       9. Wsparcie dla IPv6 ND i PMTU discovery;       10. Wsparcie dla dynamicznych protokołów routingowych jak OSPF, IS-IS oraz BGP. |
| **Bezpieczeństwo** | * + - 1. musi zapewniać autoryzacja użytkowników w oparciu o IEEE 802.1x;       2. Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;       3. musi zapewniać autoryzację prób logowania do urządzenia (dostęp administracyjny) na serwerach RADIUS lub TACACS+;       4. obsługa protokołu Spanning Tree przed zmianą topologii. |
| **Zarządzanie i monitorowanie** | 1. Musi zapewniać funkcjonalność zapisu logów systemowych do zewnętrznego serwera syslog; 2. Liczniki pakietów wchodzących/wychodzących per każdy port; 3. 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 wielu plików konfiguracyjnych; 4. Implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć IP (zdalny port mirroring – ERSPAN); 5. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2,dostęp do pełnej konfiguracji z konsoli urządzenia (Fully Managed) poprzez protokół SSH; 6. Zabezpieczenie dostępu do przełącznika poprzez interfejs graficzny (jeśli istnieje) za pomocą SSL z jednoczesną możliwością blokady dostępu osobno dla http i https; 7. zarządzanie poprzez interfejs CLI z poziomu portu konsoli; 8. Min.4 poziomy dostępu administracyjnego poprzez konsole (poziomy dostępu mogą być predefiniowane w systemie operacyjnym urządzenia lub jego konfiguracji również za pomocą definicji własnych grup dostępu, mechanizmów ACL, mechanizmów nadawania lub odbierania uprawnień do wybranych poleceń CLI w tym uruchomienia nowej powłoki); 9. Obsługa mechanizmu Netsteam lub równoważnego min. rozmiar pamięci tablicy "flow-ów" 256 000; 10. funkcjonalność telemetrii; 11. Obsługa protokołu NTP lub SNTP 12. Obsługa protokołu IEEE 802.1ab. |
| **Wyposażenie** | Moduły (wkładki optyczne) dla 1 szt. dostarczanego przełącznika:  - 57 szt. wkładek 40GE QSFP+  - 8 szt. wkładek 100GE QSFP28  Wkładki muszą być zatwierdzone przez producenta przełącznika do użytku w oferowanym przełączniku i pracy w środowisku SDN Zamawiającego. |
| **Dodatkowe informacje/wymagania** | 1. przełącznik musi zostać dostarczony wraz z wszystkimi elementami (kable zasilające, przewody) oraz licencjami zapewniającymi korzystanie z wszystkich wykazanych funkcjonalności 2. dostawa wraz z gwarancją producenta urządzenia i Oprogramowania na okres min. 36 miesięcy wraz z zapewnieniem aktualizacji oprogramowania w okresie gwarancji. |

1. **Opis minimalnych wymagań funkcjonalnych dla** **urządzenia – przełącznika Spine w OPP typu Huawei CloudEngine 8865-4C-32 (lub równoważny).**

Przełączniki muszą być dostarczone do OPP.

|  |  |
| --- | --- |
| **Wymaganie** | **Minimalne parametry** |
| **Ogólne** | 1. Przełącznik warstwy trzeciej typu „Spine” o rozmiarze max 2U 2. Wyposażony w bufor o pojemności min 64MB. 3. Wszystkie interfejsy muszą być zatwierdzone przez producenta do użytku w oferowanym przełączniku. 4. Dostawa w obudowie przystosowanej do montażu w szafie 19” wraz z niezbędnym osprzętem (bez dostawy szafy) 5. Zasilanie: Napięcie zmienne: 230 V, 50 Hz 6. praca w temperaturze od 0 do 40 °C. 7. praca przy wilgotności powietrza od 10% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej |
| **Rodzaj portu/ilość i typ portów** | 32 porty 40/100GE QSFP28 z możliwością rozbudowy do 64 portów. |
| **Zasilanie i system wentylacji** | 1. min 2 zasilacze z możliwością wymiany podczas pracy urządzenia. 2. min 2 wiatraki z możliwością wymiany podczas pracy urządzenia. 3. zapewniający przepływ powietrza w konfiguracjach front-to-back i back-to-front. |
| **Funkcjonalności** | 1. Przełącznik musi zapewniać możliwość obsługi technologii Multichassis Etherchannel (np. vPC lub M-LAG) lub innej równoważnej - łączącej przełączniki w 1 logiczną jednostkę 2. posiadać wsparcie dla min 128 konkurentnych ścieżek protokołu ECMP. 3. Wsparcie dla mechanizmów PFC oraz ECN 4. zapewnienie funkcjonalności zabezpieczenia portów przed wymuszeniem zmiany lokalizacji Root Bridge; 5. zapewnienie funkcjonalności prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym; 6. Min 30000 list dostępowych (ACL); 7. obsługa mikrosegmentacji lub równoważnego mechanizmu izolacji 8. obsługa mechanizmów obrony przed atakami DoS, ARP, and ICMP; 9. obsługa mechanizmów związane z zapewnieniem jakości usług w sieci: 10. Implementacja co najmniej ośmiu kolejek sprzętowych dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie; 11. zapewnienie obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority); 12. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP; 13. obsługa mechanizmów traffic policing, traffic shaping, congestion avoidance (RED lub WRED); 14. obsługa dla L2/L3/L4 ACL |
| **Wydajność** | 1. Minimalna szybkość przełączania 16 Tbps;   przy spełnieniu wymagania  minimalna przepustowość: 2400 Mpps |
| **Wymagana funkcjonalność dla warstwy 2:** | 1. trunking IEEE 802.1Q VLAN; 2. obsługa min. 4094 sieci VLAN; 3. obsługa min. 600 000 adresów MAC; 4. obsługa Rapid Spanning Tree: np. IEEE 802.1w, PVRST lub równoważne; 5. obsługa Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s); 6. Internet Group Management Protocol (IGMP) snooping; 7. Port Aggregation Protocol: np. IEEE 802.3ad; 8. prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast; 9. Wsparcie dla ramek Jumbo dla wszystkich portów (min 9198 bajtów); |
| **Wymagana funkcjonalność dla warstwy 3:** | 1. obsługa protokołu VxLAN w modelach centralized and distributed gateway; 2. obsługa protokołu BGP eVPN; 3. obsługa 16 000 virtual tunnel endpoints (VTEPs) 4. obsługa 4000 VRFs 5. Minimalny rozmiar FIB 1,5M IPv4 / 750K IPv6; 6. Minimalna wielkość tablicy routingu multicast powinna być 30000; 7. Wsparcie dla protokołu IPv6; 8. Wsparcie dla protokołu BFD dla OSPF, BGP, IS-IS, oraz static route; 9. Wsparcie dla IPv6 ND i PMTU discovery; 10. Wsparcie dla dynamicznych protokołów routingowych jak OSPF, IS-IS oraz BGP. |
| **Bezpieczeństwo** | 1. musi zapewniać autoryzacja użytkowników w oparciu o IEEE 802.1x; 2. Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard; 3. musi zapewniać autoryzację prób logowania do urządzenia (dostęp administracyjny) na serwerach RADIUS lub TACACS+; 4. obsługa protokołu Spanning Tree przed zmianą topologii. |
| **Zarządzanie i monitorowanie** | 1. Musi zapewniać funkcjonalność zapisu logów systemowych do zewnętrznego serwera syslog; 2. Liczniki pakietów wchodzących/wychodzących per każdy port; 3. 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 wielu plików konfiguracyjnych; 4. Implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć IP (zdalny port mirroring – ERSPAN); 5. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2,dostęp do pełnej konfiguracji z konsoli urządzenia (Fully Managed) poprzez protokół SSH; 6. Zabezpieczenie dostępu do przełącznika poprzez interfejs graficzny (jeśli istnieje) za pomocą SSL z jednoczesną możliwością blokady dostępu osobno dla http i https; 7. zarządzanie poprzez interfejs CLI z poziomu portu konsoli; 8. Min. 4 poziomy dostępu administracyjnego poprzez konsole (poziomy dostępu mogą być predefiniowane w systemie operacyjnym urządzenia lub jego konfiguracji również za pomocą definicji własnych grup dostępu, mechanizmów ACL, mechanizmów nadawania lub odbierania uprawnień do wybranych poleceń CLI w tym uruchomienia nowej powłoki); 9. Obsługa mechanizmu Netsteam lub równoważnego min. rozmiar pamięci tablicy "flow-ów" 256 000; 10. funkcjonalność telemetrii; 11. Obsługa protokołu NTP lub SNTP 12. Obsługa protokołu IEEE 802.1ab. |
| **Wyposażenie** | Moduły (wkładki optyczne) dla 1 szt. dostarczanego przełącznika:  - 24 szt. wkładek 40GE QSFP+  - 8 szt. wkładek 100GE QSFP28  Wkładki muszą być zatwierdzone przez producenta przełącznika do użytku w oferowanym przełączniku i pracy w środowisku SDN Zamawiającego. |
| **Dodatkowe informacje/wymagania** | 1. przełącznik musi zostać dostarczony wraz z wszystkimi elementami (kable zasilające, przewody) oraz licencjami zapewniającymi korzystanie z wszystkich wykazanych funkcjonalności 2. dostawa wraz z gwarancją producenta urządzenia i Oprogramowania na okres min. 36 miesięcy wraz z zapewnieniem aktualizacji oprogramowania w okresie gwarancji. |

1. **Opis minimalnych wymagań funkcjonalnych dla urządzenia – przełącznika Leaf w OPP typu Huawei CloudEngine CE6863E-48S6CQ-B (lub równoważny).**

Przełączniki muszą być dostarczone do OPP.

|  |  |
| --- | --- |
| **Wskaźnik** | **Specyfikacja techniczna/wymagania** |
| **Ogólne** | 1. Przełącznik warstwy trzeciej o rozmiarze 1U 2. Wyposażony w bufor o pojemności min 42MB. 3. Wszystkie interfejsy muszą być zatwierdzone przez producenta do użytku w oferowanym przełączniku. 4. Dostawa w obudowie przystosowanej do montażu w szafie 19” wraz z niezbędnym osprzętem (bez dostawy szafy). 5. Zasilanie: Napięcie zmienne: 230 V, 50 Hz 6. Praca w temperaturze od 10 do 40 °C. 7. Praca przy wilgotności powietrza od 20% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej. |
| **Rodzaj portu/ilość i typ portów** | 1. 48 szt. 10/25G SFP28   oraz   1. min. 6 portów 40/100G (QSFP 28) |
| **Zasilanie i system wentylacji** | 1. Min. 2 zasilacze z możliwością wymiany podczas pracy urządzenia. 2. Min. 2 wiatraki z możliwością wymiany podczas pracy urządzenia. 3. Zapewniający przepływ powietrza w konfiguracjach front-to-back i back-to-front. |
| **Dostęp** | Przełącznik musi posiadać wsparcie dla secure boot lub równoważnej funkcjonalności zapewniającej możliwość weryfikacji poprawności oprogramowania systemowego przed jego uruchomieniem. |
| **Funkcjonalności** | 1. Zapewnia wirtualizację N:1 w oparciu o rozwiązania agregacji łącza lub Stacking. Urządzenia muszą posiadać technologię zapewniającą agregację łącz między urządzeniami. Musi to umożliwiać urządzeniom w tym samym stanie przeprowadzenie negocjacji agregacji łącza między nimi. Technologia musi pozwalać na oddzielne aktualizowanie urządzeń w sposób zapewniający nieprzerwaną obsługę ruchu sieciowego. 2. Posiada wsparcie dla min 128 konkurentnych ścieżek protokołu ECMP. 3. Zapewnienie funkcjonalności konfiguracji stałej lub automatycznej portu dostępowego tak, aby samodzielnie przechodził do stanu FORWARDING z pominięciem stanów LISTENING i LEARNING 4. Zapewnienie funkcjonalności zabezpieczenia portów przed wymuszeniem zmiany lokalizacji Root Bridge."; 5. Zapewnienie funkcjonalności prywatnego VLAN-u, czyli możliwości blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym; 6. Min. 30000 list dostępowych (ACL); 7. Obsługa mikrosegmentacji lub równoważnego mechanizmu izolacji zapewniającego tożsamy skutek jak mikrosegmentacja 8. Obsługa mechanizmów obrony przed atakami DoS, ARP i ICMP; 9. Obsługa mechanizmów związanych z zapewnieniem jakości usług w sieci: 10. implementacja co najmniej czterech kolejek sprzętowych dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie; 11. zapewnienie obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority); 12. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP; 13. obsługa mechanizmów traffic policing, traffic shaping, congestion avoidance (RED lub WRED); 14. Obsługa dla L2/L3/L4 ACL. |
| **Wydajność** | * 1. Minimalna szybkość przełączania 3,6 Tbps;   przy spełnieniu wymagania   * 1. Minimalna przepustowość: 940 Mbps. |
| **Wymagana funkcjonalność dla warstwy 2:** | * + - 1. Trunking IEEE 802.1Q VLAN;       2. Obsługa min. 4094 sieci VLAN;       3. Obsługa min. 256 000 adresów MAC;       4. Obsługa Rapid Spanning Tree: np. IEEE 802.1w, PVRST lub równoważnego dla obsługi Rapid Spanning Tree;       5. Obsługa Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s);       6. Internet Group Management Protocol (IGMP) snooping;       7. Port Aggregation Protocol: np. IEEE 802.3ad;       8. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast;       9. Wsparcie dla ramek Jumbo dla wszystkich portów (min 9198 bajtów); |
| **Wymagana funkcjonalność dla warstwy 3:** | * + - 1. Obsługa protokołu VxLAN w modelach centralized and distributed gateway;       2. Obsługa protokołu BGP eVPN;       3. Minimalny rozmiar FIB 200000 IPv4 / 80000 IPv6;       4. Minimalna wielkość tablicy routingu multicast – 32000 dla IPv4;       5. Wsparcie dla protokołu IPv6;       6. Wsparcie dla protokołu BFD dla OSPF, BGP, IS-IS, oraz static route;       7. Wsparcie dla IPv6 ND i PMTU discovery;       8. Wsparcie dla dynamicznych protokołów routingowych jak OSPF, IS-IS oraz BGP. |
| **Bezpieczeństwo** | * + - 1. Musi zapewniać autoryzację użytkowników w oparciu o IEEE 802.1x;       2. Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;       3. Musi zapewniać autoryzację prób logowania do urządzenia (dostęp administracyjny) na serwerach RADIUS lub TACACS+;       4. Obsługa protokołu Spanning Tree przed zmianą topologii. |
| **Zarządzanie i monitorowanie** | 1. Musi zapewniać funkcjonalność zapisu logów systemowych do zewnętrznego serwera syslog; 2. Liczniki pakietów wchodzących/wychodzących per każdy port; 3. 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 wielu plików konfiguracyjnych; 4. Implementacja mechanizmu SPAN PORT lub analogiczna funkcjonalność; 5. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, dostęp do pełnej konfiguracji z konsoli urządzenia (Fully Managed) poprzez protokół SSH; 6. Zabezpieczenie dostępu do przełącznika poprzez interfejs graficzny (jeśli istnieje) za pomocą SSL z jednoczesną możliwością blokady dostępu osobno dla http i https; 7. Zarządzanie poprzez interfejs CLI z poziomu portu konsoli; 8. Min.4 poziomy dostępu administracyjnego poprzez konsole (poziomy dostępu mogą być predefiniowane w systemie operacyjnym urządzenia lub jego konfiguracji również za pomocą definicji własnych grup dostępu, mechanizmów ACL, mechanizmów nadawania lub odbierania uprawnień do wybranych poleceń CLI w tym uruchomienia nowej powłoki); 9. Obsługa mechanizmów flexible Netflow, Netsteam min. rozmiar pamięci tablicy (aggregated flows) - 256 000; 10. Funkcjonalność telemetrii; 11. Obsługa protokołu NTP lub SNTP 12. Obsługa protokołu IEEE 802.1ab. |
| **Wyposażenie** | 1. Wszystkie porty muszą być wyposażone w kable do ich łączenia z urządzeniami Zamawiającego – 54 sztuki kabli dla 1 przełącznika. 2. Moduły (wkładki optyczne) dla 1 szt. dostarczanego przełącznika:   - 48 szt. 10/25G SFP28  - 6 szt. 40/100G QSFP 28  Wkładki muszą być zatwierdzone przez producenta przełącznika do użytku w oferowanym przełączniku i pracy w środowisku SDN Zamawiającego. |
| **Dodatkowe informacje/wymagania** | 1. Przełącznik musi zostać dostarczony wraz z wszystkimi elementami (kable zasilające, przewody) oraz licencjami zapewniającymi korzystanie z wszystkich wykazanych funkcjonalności 2. Dostawa wraz z gwarancją producenta urządzenia i Oprogramowania Wspomagającego na okres min. 36 miesięcy wraz z zapewnieniem aktualizacji oprogramowania w okresie gwarancji. |

1. **Opis minimalnych wymagań funkcjonalnych dla urządzenia serwer – arbiter.**

Serwer musi być dostarczony do OPW.

|  |  |
| --- | --- |
| **Wymaganie** | **Minimalne parametry** |
| **Ogólne** | * Funkcja arbitrażu musi posiadać cechy pozwalające na wywołanie automatycznego przełączenia się oprogramowania kontrolera SDN ze środowiska „aktywnego” (active) na środowisko „rezerwowe” (stand-by). * Funkcję arbitrażu można zrealizować, zarówno w oparciu o autonomiczny serwer fizyczny (Bare Metal) jak i o maszynę wirtualną. * Komunikacja pomiędzy elementami systemu Disaster Recovery kontrolera SDN (kontrolerem aktywnym, zapasowym oraz serwisem arbitrażowym) jak i środowiskiem zewnętrznym (np. przegladarki) musi być zabezpieczona odpowiednimi mechanizmami certyfikatów bezpieczeństwa. |
| **Funkcja arbitrażowa** | * Serwer na którym działa funkcja arbitrażu musi tworzyć tzw „trzecią stronę” (Third site) - niezależną od środowiska na którym jest uruchomiony „aktywny” kontroler SDN (active) oraz „rezerwowy” kontroler SDN (stndby). Niezależność środowiska „trzeciej strony” rozumiana jest jako odrębna „fault domain” (domena awarii). * „Trzecia strona” z funkcją arbitrażu musi być wybrana w taki sposów, aby niezależnie od tego czy awarii ulegnie:   + Główne Centrum Przetwarzania Danych   + Zapasowe Centrum Przetwarzania Danych   + Trzecia strona z funkcją arbitra,   sieć komputerowa DCN była zawsze pod kontrolą pełnosprawnego kontrolera SDN.   * Funkcja arbitra powinna posiadać architekturę oraz algorytmy pozwalające na przełączenie aktywnego kontrolera SDN na kontroler „optymalny”/ zapasowy w przypadku:   + Katastrofy głównego / aktywnego Centrum Przetwarzania Danych   + Awarii aktywnego kontrolera SDN, uniemożliwiającej zarządzanie siecią DCN   + Awarii funkcji lub serwera arbitrażowego   + Niewykrycia aktywności sygnału „heartbeat” pomiędzy kontrolerami : głównym, zapasowym i funkcją arbitrażu „trzeciej strony”. Stan sygnału „heartbeat” musi być sprawdzany nie rzadziej niż co 10 sekund. |
| **Serwer arbitrażowy** | * Serwer poninien spełniać min. poniższe wymagania sprzętowe :   + Min 4 procesory (CPU), 16 GB pamięci, 2 karty sieciowe   + Dopuszczalne są zarówno procesory (CPU) w architekturze ARM jak i x86   + Wspierane systemy operacyjne: co najmniej EulerOS lub SUSE Linux Enterprise Server * Serwery arbitra, aktywnego kontrolera SDN oraz rezerwowego kontrolera SDN muszą być połączone siecią komputerową o nastepujących parametrach:   + przepustowość min 2Mb/s   + Opóźnienie < 50 ms   + Utrata pakietów < 1% |

1. **Wymagania minimalne dla Systemu SDN (automatyzacji zarządzania) wraz z zapewnieniem funkcjonalności systemu analitycznego dla kontrolera SDN dla dostarczonych przełączników.**
2. **System do zarządzania środowiskiem LAN DC dla dostarczanych przełączników.**

|  |  |
| --- | --- |
| **Wskaźnik** | **Specyfikacja techniczna/wymagania** |
| **Architektura** | 1. System należy dostarczyć w formie urządzeń applianace bądź wraz z niezbędną platformą serwerową. Fizyczne urządzenia appliance bądź platforma serwerowa musi spełniać poniższe wymagania:   - Minimum 2 procesory 20 corowe;  - Minimum 256 GB pamięci RAM;  - Minimum 8 dyski o pojemności minimum 1200 GB każdy;  - Minimum 4 porty 10G SFP+;  - Minimum 6 portów 1G RJ45;  - Redundantne zasilanie.  2. Sprzęt musi być dedykowany do pracy z Systemem.  3. Sprzęt musi umożliwiać realizację wysokiej dostępności wszystkich elementów funkcjonalnych (ang. HA). Aby zapewnić wysoką dostępność, system powinien być wdrożony w postaci klastra, który potrafi równoważyć obciążenia między wieloma węzłami klastra. Gdy pojedynczy węzeł ulegnie awarii, cały klaster może nadal działać poprawnie. Ponadto System musi obsługiwać elastyczną rozbudowę pojemności w celu zwiększenia wydajności całego klastra. |
| 1. System musi mieć możliwość integracji poprzez interfejsy programistyczne z:  a) platformą chmurową w kierunku północnym,  b) urządzeniami sieciowymi w kierunku południowym oraz  c) platformą zarządzania serwerami oraz kontenerami w kierunku wschód-zachód.  2. System musi realizować udostępnianie zasobów sieciowych, obliczeniowych i pamięci masowej. Ponadto system musi współpracować z modułem analitycznym. |
| **Instalacja i wdrożenie** | 1. Aby ułatwić wdrożenie, system musi udostępniać dwa tryby instalacji: instalacja fabryczna oraz instalacja jednym kliknięciem (ZTP) za pomocą automatycznego narzędzia. Usługi do wdrożenia można wybrać na stronie instalacji zgodnie z wymaganiami. |
| 1. Aby w pełni wykorzystać zasoby serwera, kontroler można wdrożyć na fizycznych maszynach i maszynach wirtualnych w systemie jednowęzłowym lub klastrze. |
| **Pojemność wydajności** | 1. Klaster kontrolera z trzema węzłami (wdrożony na maszynach fizycznych lub maszynach wirtualnych) musi zarządzać co najmniej 1,8 tys. węzłów NVE. Klaster z największą liczbą węzłów (wdrożonych na maszynach fizycznych lub maszynach wirtualnych) musi zarządzać co najmniej 4,2 tys. węzłów NVE. |
| 1. Rozwiązanie do wdrażania na małą skalę (kontroler jednowęzłowy) musi zarządzać co najmniej 34 węzłami NVE, niezależnie od trybu wdrażania (na maszynie fizycznej lub maszynie wirtualnej). |
| **Otwarty ekosystem** | 1. Aby uprościć zarządzanie, wymagany jest zunifikowany portal do obsługi i konserwacji urządzenia oraz dostarczania usług oraz konfiguracji (zarówno sieci podkładowej jak i nakładkowej). |
| 1. Dostęp do kontrolera oraz do jego części analitycznej [analizatora] musi być realizowany za pomocą SSO. |
| 1. Kontroler musi korzystać ze standardowych protokołów interfejsu południowego, takich jak OpenFlow, NETCONF, SNMP i SSH, do łączenia się z urządzeniami sieciowymi. |
| 1. Aby zachować zgodność z istniejącymi przełącznikami w działającej sieci, system powinien mieć możliwość jednolitego zarządzania i dostarczania konfiguracji do przełączników innych producentów. |
| 1. Kontroler musi mieć możliwość integracji, zarządzania i dostarczania konfiguracji – co najmniej na poziomie sieci L3 – z urządzeniami typu VAS (Value Added Services) innych producentów, w tym co najmniej z zaporami sieciowymi posiadanymi przez Zamawiającego Fortinet, Palo Alto, Check Point oraz systemy równoważenia (LB) obciążenia F5. |
| 1. W przypadku urządzeń VAS innych producentów (takich jak WAF, zapory ogniowe i systemy równoważenia obciążenia), którymi nie można zarządzać, kontroler musi mieć możliwość przekierowywania do nich ruchu sieciowego. |
| **Dostępność systemu** | 1. Podczas pracy systemu, aby zapobiec wpływowi awarii systemu na całą sieć lub w trybie offline, kontroler nie uczestniczy w przekazywaniu danych. Gwarantuje to, że istniejące usługi sieciowe nie zostaną naruszone po awarii wszystkich węzłów kontrolera. |
| 1. Aby zapewnić wysoką niezawodność, system musi obsługiwać wdrażanie klastrów. Węzły w klastrze pracują w trybie równoważenia obciążenia i zapewniają unikalny adres IP zarządzania dla systemu aplikacji wyższej warstwy i platformy chmurowej. Gdy mniej niż połowa węzłów w klastrze jest uszkodzona, klaster może nadal działać poprawnie, a adres IP zarządzania może zostać przełączony z wadliwego węzła na działający węzeł, co nie jest postrzegane przez system usług wyższej warstwy. |
| 1. Aby zapewnić możliwość DR, system musi obsługiwać zdalne wdrażanie DR. Gdy aktywne centrum danych jest wadliwe, a usługi są przełączane do rezerwowego centrum danych, żadne dane nie są tracone. |
| 1. Po wdrożeniu nadmiarowości geograficznej kontroler obsługuje ręczne i automatyczne przełączanie między klastrami aktywnymi i rezerwowymi za pośrednictwem usługi arbitrażu. Usługa arbitrażu może być świadczona przez dostawcę lub oprogramowanie arbitrażowe. W przypadku potrzeby uruchomienia usługi, Wykonawca uzgodni dostawcę lub oprogramowanie z Zamawiającym, a ten wybierze rodzaj realizacji usługi. |
| 1. Aby zapewnić szybkie odzyskanie pojedynczego węzła w klastrze po wystąpieniu błędu, system musi obsługiwać wymianę pojedynczego węzła. |
| 1. Aby zapewnić, że klaster może szybko odzyskać sprawność po awarii, system musi obsługiwać tworzenie kopii zapasowych i przywracanie klastra. |
| **Sieć podkładowa** | 1. Aby zarządzać łączami w bardziej elastyczny sposób, kontroler musi obsługiwać automatyczne wykrywanie i ręczne tworzenie łączy. |
| 1. Aby poprawić wydajność wdrażania, system musi obsługiwać uproszczony tryb ZTP, aby szybko wdrożyć automatyczną konfigurację sieci warstwy 3 i automatyczne dołączanie urządzeń. Serwer DHCP może elastycznie wybrać wbudowaną lub zewnętrzną usługę DHCP kontrolera. Kontroler obsługuje również elastyczne konfiguracje elementów sieci podkładowej, takie jak szablony konfiguracji połączeń wychodzących spine/RR, a także konfiguracje O&M (takie jak syslogs). |
| 1. Aby zapewnić bezpieczeństwo, kontroler obsługuje dwukierunkowe uwierzytelnianie certyfikatem, gdy urządzenia przechodzą w tryb online przez ZTP. |
| 1. Aby znacznie uprościć planowanie i wdrażanie sieci podkładowej, system musi obsługiwać automatyczne planowanie sieci szkieletowej DC i automatyczne generowanie topologii. Konfiguracja topologii może być modyfikowana, symulowana i weryfikowana przed jej ostatecznym wdrożeniem. |
| 1. Aby zapobiec błędom po planowaniu i wdrożeniu sieci podkładowej, system musi obsługiwać różne mechanizmy weryfikacji, takie jak weryfikacja łączności między VTEP-ami, weryfikacja adresu IP VTEP, weryfikacja adresu identyfikatora routera, weryfikacja adresu MAC VTEP, weryfikacja pętli routingu. |
| 1. Kontroler musi wspierać automatyczną rozbudowę zasobów DC w zakresie dostępowych przełączników sieci L&S jak i serwerów – aby uniknąć ewentualnych błędów spowodowanych ręczną konfiguracją, system musi obsługiwać automatyczną konfigurację dodatkowych przełączników dostępowych i rozbudowanych zasobów serwerowych. |
| 1. Aby wyeliminować zagrożenia bezpieczeństwa podczas ZTP, system musi obsługiwać ZTP w trybie zarządzania z sieci OOB, aby odizolować kontroler od sieci usługowej. |
| 1. Kontroler musi wspierać Ipv6. |
| **Połączenie z platformą chmurową** | 1. Kontroler musi łączyć się z platformą chmurową OpenStack w oparciu o model standardowy w celu wdrożenia ujednoliconego zarządzania i planowania zasobów sieciowych na żądanie. |
| 1. Jeśli OpenStack jest połączony, usługi muszą być udostępniane w oparciu o IPv6 i IPv4, w tym między innymi podsieć, port, QoS, serwer bare metal, proxy metadanych, grupę bezpieczeństwa, politykę bezpieczeństwa, komunikację VPC i sieć zewnętrzną. |
| 1. Aby zapewnić bezpieczeństwo udostępniania serwerów typu bare metal, kontroler automatycznie konwertuje grupy zabezpieczeń w OpenStack na listy ACL na przełącznikach typu leaf switch serwera i wdraża zasady grup bezpieczeństwa, aby zapewnić takie samo bezpieczeństwo maszyn wirtualnych i serwerów typu bare metal. |
| 1. W rozwiązaniu nakładkowym OpenStack VXLAN przełączniki liściowe (przełączniki dostępowe) mogą być używane jako urządzenia VXLAN VTEP. Sprzęt przełącznika hermetyzuje i dekapsuluje pakiety VXLAN, zmniejszając obciążenie przetwarzania w sieci hosta. |
| 1. Aby zapewnić bezpieczne i niezawodne połączenie z OpenStack, między wtyczką platformy chmurowej a kontrolerem, musi być obsługiwane dwukierunkowe uwierzytelnianie certyfikatów, w tym uwierzytelnianie HTTPS, WebSocket i SAN. |
| **Połączenie kontenerów** | 1. Kontroler umożliwia, aby podstawowe oprogramowanie kontenerowe, takie jak open-source K8S, czy Docker można ze sobą łączyć używając wtyczek [plug-in], aby wdrożyć wspólne udostępnianie usług sieciowych kontenerów. |
| 1. Obsługiwane są adresy IP klastra. Wtyczka kontenera wykrywa adres IP klastra i przekazuje kontrolerowi informacje o adresie IP klastra, które są następnie zapisywane w kontrolerze. |
| 1. Obsługiwane są porty węzłów. Wtyczka kontenera wykrywa port węzła i powiadamia kontrolera o informacjach o porcie węzła, które są następnie zapisywane w kontrolerze. |
| 1. Wizualizowany model sieci kontenerowej: Wizualizowana jest topologia sieci logicznej kontenera i topologia sieci aplikacji. |
| **Połączenie VMware** | 1. Kontroler musi mieć możliwość integracji z VMware vCenter, aby przekazać konfiguracje sieci wirtualnej do vSwitch, wdrażając ujednolicone planowanie sieci fizycznych i wirtualnych. Kontroler musi wykrywać zdarzenia online, offline i migracji maszyn wirtualnych w celu migracji konfiguracji sieci. |
| 1. Kontroler obsługuje połączenia z VMware Fault Tolerance (FT), aby zapewnić wyższą niezawodność. |
| 1. Kontroler obsługuje połączenie z wieloma systemami vCenter i migrację wirtualnych maszyn pomiędzy tymi vCenter. |
| 1. Gdy kontroler łączy się z VMware, tryb PVLAN włącza na VMware, aby domyślnie izolować ruch różnych maszyn wirtualnych w grupie portów. W ten sposób maszyny wirtualne komunikują się ze sobą tylko za pośrednictwem przełącznika. Na przełączniku konfiguruje się reguły mikrosegmentacji, aby umożliwić komunikację tylko między maszynami wirtualnymi w tej samej podsieci. |
| **Usługi nakładkowe** | 1. Aby zminimalizować wpływ „flooding” na sieć, sterownik musi obsługiwać funkcję „flooding suppression”. Kontroler lub przełącznik SDN musi mieć możliwość włączenia lub wyłączenia tej funkcji. Gdy ta funkcja jest włączona, można skutecznie zapobiegać zdarzeniom „zalewania – flooding” sieci przez pakiety typu BUM. |
| 1. System musi obsługiwać zarówno zarządzanie konfiguracją metodą „GUI kontrolera”, jak i oparte na interfejsie CLI. Ponadto należy zapewnić mechanizm blokady wprowadzania zmian na elementach sieci, aby zapobiec konfliktom konfiguracji. |
| 1. System wspiera rozwiązania L2 i L3 VxLAN multicast |
| 1. System obsługuje IPv6/IPv4 dla VXLAN. |
| 1. Aby poprawić wydajność konfiguracji, system musi obsługiwać: 2. zbiorcze importowanie [batch import] tras statycznych, VPC, zewnętrznych gateways, reguł dotyczących SFC [Service Function Chaining] 3. zbiorczy eksport konfiguracji VPC i urządzeń oraz 4. zbiorczą modyfikację nazw i opisów portów, haseł urządzeń i Konfiguracje RR na węzłach kręgosłupa. |
| 1. Aby zapewnić wysoką dostępność połączenia między centrum danych a siecią zewnętrzną, kontroler musi obsługiwać wiele grup przełączników wyjściowych [egress gateway] . |
| 1. Aby uprościć wdrażanie sieci nakładkowej i poprawić wydajność wdrażania usług, system automatycznie identyfikuje intencje użytkownika i inteligentnie rekomenduje rozwiązania sieci logicznej. |
| 1. Aby uprościć wdrażanie sieci nakładkowej i poprawić wydajność wdrażania usług, system automatycznie identyfikuje intencje użytkownika i inteligentnie rekomenduje rozwiązania sieci logicznej bez konieczności orkiestracji usług, w tym uruchamiania aplikacji. |
| 1. Symulacja i weryfikacja: Aby zapewnić poprawność dostarczania usługi sieci nakładkowej i zmian konfiguracji, kontroler musi obsługiwać symulację i weryfikację przed udostępnieniem usługi czy wdrożeniem zmienionej konfiguracji (zarówno dla sieci IPv4 i IPv6). W oparciu o istniejące i nowe konfiguracje urządzeń, kontroler wykonuje modelowanie i symulację zasobów, łączności i wpływu zmian. Zmiany konfiguracji, które należy zweryfikować, obejmują co najmniej sieci logiczne, mikrosegmentację, sieci zewnętrzne. Zasoby podlegające weryfikacji obejmują VRF, trasy statyczne, podinterfejsy warstwy 2 oraz VNI/BD/EVPN. Zapobiega to wpływowi nieprawidłowych konfiguracji na istniejące usługi. |
| 1. Aby szybko wycofać usługi, które nie spełniają oczekiwań po wdrożeniu usługi, system musi obsługiwać wycofywanie zmian [rollback] : na poziomie usługi, tenanta oraz całej sieci. |
| 1. Aby zapewnić spójność danych w kierunku południowym i północnym, kontroler musi obsługiwać weryfikację spójności danych konfiguracyjnych z platformą chmurową w kierunku północnym i przełącznikami w kierunku południowym. |
| **Łączenie funkcji usługowych (SFC)** | 1. Pule zasobów polityki bezpieczeństwa muszą być tworzone w celu skutecznej ochrony dostępu wschód-zachód. Kontroler implementuje izolację bezpieczeństwa w oparciu o grupy aplikacji. Grupy aplikacji są podzielone na podstawie wymagań serwisowych i oddzielone od topologii i infrastruktury. Terminale w tej samej podsieci IP mogą być przydzielone do różnych grup aplikacji. Gwarantuje to, że komunikacja między terminalami w różnych grupach aplikacji jest kontrolowana i filtrowana przez zasady międzygrupowe, nawet jeśli terminale znajdują się w tej samej podsieci i korzystają z tej samej bramy. |
| 1. SFC: Aby zaoszczędzić zasoby ACL, system musi obsługiwać standardowy model SFC IETF, tryby SFC oparte na NSH i PBR oraz protokoły IPv4/IPv6 SFC. |
| 1. Aby spełnić różne wymagania dotyczące bezpieczeństwa usług, system musi obsługiwać orkiestrację usług L4-L7, takich jak WAF, NAT, IPsec i zapora za pośrednictwem SFC, a także zapewniać, że ruch usług przechodzi przez węzły typu „multi-hop”. |
| 1. Aby spełnić różne wymagania dotyczące bezpieczeństwa usług, system musi zapewniać bezpieczeństwo dla ruchu wewnątrz sieci VPN wschód-zachód, ruchu między sieciami VPN wschód-zachód, przez SFC. |
| 1. Obejście SFC: W rozwiązaniu SFC typu multi-hop, jeśli zapora sieciowa jest uszkodzona, ruch może ominąć wadliwy węzeł, aby zapewnić działanie usługi. |
| **Mikrosegmentacja** | 1. System musi obsługiwać mikrosegmentację IPv4/IPv6 i stosować zasady EPG na przełącznikach w celu wdrożenia kontroli bezpieczeństwa i izolacji. |
| **Multi-DC** | 1. System musi obsługiwać wspólne zarządzanie wieloma kontrolerami domeny na różnych kontrolerach domeny. Użytkownicy muszą szybko organizować usługi między domenowe za pomocą ujednoliconego interfejsu GUI w trybie przeciągania i upuszczania. Struktury tranzytowe można tworzyć na potrzeby aranżacji usług w wielu chmurach, a tranzytowe VPC można tworzyć w sieci szkieletowej tranzytu w celu implementacji komunikacji cross-DC między wielodostępnymi sieciami VPC. Ponadto DC mogą być połączone liniami prywatnymi. Należy dostarczyć raport z testu rozwiązania wydany przez autorytatywną organizację zewnętrzną. |
| 1. Kontroler musi obsługiwać zarządzanie współpracą z chmurą publiczną. |
| 1. Aby zapewnić poprawność dostarczania usług między DC i zmian konfiguracji, system musi obsługiwać symulację przed zdarzeniem i weryfikację usług sieciowych między DC. Przed udostępnieniem usług, system przeprowadza modelowanie i symulację zasobów, łączności i wpływu zmian, aby zapobiec wpływowi nieprawidłowych konfiguracji na istniejące usługi. |
| 1. Aby zapewnić deterministyczne SLA usług cross-cloud, kontroler musi zezwolić usługom między DC na wejście do różnych tuneli SRv6 w oparciu o wymagania usług użytkowników. |
| **Widoczność sieci** | 1. Aby lepiej lokalizować urządzenia, konfiguracje i usterki, system musi obsługiwać powiązane wyświetlanie aplikacji, topologii logicznych i fizycznych, a także wyświetlanie relacji mapowania. |
| **Wykrywanie anomalii** | 1. Aby lepiej wykrywać wyjątki w sieci, system musi być w stanie wykryć możliwe pętle i punkty awarii w sieci VXLAN oraz zapewnić środki eliminujące pętle. System musi wykrywać pętle na pojedynczym interfejsie pojedynczego urządzenia, na wielu interfejsach pojedynczego urządzenia oraz między urządzeniami. |
| **Rozwiązywanie problemów** | 1. Aby lepiej analizować wpływ operacji serwisowych na usługi podczas rozwiązywania problemów, system musi wspierać analizę wpływu takich prac serwisowych na usługi sieciowe przed wymianą lub naprawą urządzenia. |
| 1. Aby szybko naprawić usterki, sterownik musi być w stanie współpracować z modułem analitycznym w celu rozpoznania usterek, lokalizacji usterek i usunięcia usterek. Ponadto kontroler może naprawić co najmniej 20 rodzajów błędów poprzez współpracę z analizatorem, w tym analizę wpływu zmian konfiguracji i dostarczanie zasad rozwiązywania problemów. |
| 1. Aby szybko przywrócić omyłkowo usunięte konfiguracje podczas rozwiązywania problemów czy naprawy awarii, kontroler musi obsługiwać audyt konfiguracji, aby wykryć konfiguracje, które zostały omyłkowo usunięte z przełączników obsługujących zarówno konfigurację opartą na GUI, jak i CLI oraz przywracanie błędnie usuniętych konfiguracji jednym kliknięciem. |
| **Panel informacyjny** | 1. Aby pomóc użytkownikom w szybkim poznaniu stanu sieci, kontroler musi wyświetlać krótkie informacje o sprzęcie urządzenia, sieci podkładowej i nakładkowej, a także powiązane statystyki, takie jak dzienniki i alarmy. Ponadto kontroler musi wyświetlać szczegółowe informacje o sieci fizycznej, sieci wirtualnej, takie jak wirtualna sieć warstwy łącza, wirtualny router, wirtualny port i wirtualna podsieć. |
| 1. Aby szybko powiadamiać użytkowników o awariach w działającej sieci, kontroler musi mieć możliwość automatycznego powiadamiania powiązanego personelu przez e-mail lub SMS o awarii. |
| 1. Aby pomóc użytkownikom w dogłębnym zrozumieniu sieci, kontroler musi obsługiwać monitorowanie wydajności urządzenia, w tym co najmniej : zużycie procesora, pamięci, i dziennego wskaźnika niedostępności urządzenia. Kontroler obsługuje również ujednolicone wyświetlanie statusu urządzeń sieciowych, w tym ich paneli, etykiet elektronicznych i interfejsów. |
| **Wymagania dotyczące audytu bezpieczeństwa** | 1. Kontroler szczegółowo rejestruje osobę dokonującą zmiany, czas zmiany i treść zmiany związaną ze zmianą konfiguracji każdego zarządzanego obiektu. |
| **Kontrola bezpieczeństwa** | 1. Kontroler obsługuje kontrolę dostępu opartą na rolach w celu odizolowania dzierżawców oraz zarządzania kontami i uprawnieniami użytkowników. |
| 1. Kontroler obsługuje uwierzytelnianie lokalne oparte na hasłach i uwierzytelnianie bezpieczeństwa użytkownika, takie jak uwierzytelnianie RADIUS i LDAP. |
| 1. Kontroler umożliwia dodawanie użytkowników i zmianę haseł dla istniejących użytkowników. |

1. **Funkcjonalność analityczna Kontrolera SDN dla wszystkich dostarczonych w ramach Zamówienia przełączników i wszystkich posiadanych przez Zamawiającego urządzeń wskazanych w Rozdziale 2.**

|  |  |
| --- | --- |
| **Wskaźnik** | **Specyfikacja techniczna/wymagania** |
| **Architektura systemu** | 1. Jeżeli moduł analityki wymaga dodatkowego urządzenia appliance bądź platformy serwerowej, to urządzenie musi spełniać poniższe wymagania:   1. Minimum 2 procesory 20 corowe; 2. Minimum 256GB pamięci RAM; 3. Minimum 8 dysków o pojemności minimum 1200GB każdy; 4. Minimum 6 portów 10G SFP+; 5. Minimum 4 porty 1G RJ45; 6. Redundantne zasilanie   System musi być oparty przynajmniej na architekturze AS  (active-standby). |
| 1. Analizator obsługuje rozproszone przetwarzanie w czasie rzeczywistym oraz umiejętność korzystania z Big Data i AI w oparciu o frameworki, co najmniej takie jak Spark, Hadoop czy Kafka. |
| 1. Analizator obsługuje rozproszone obliczenia, agregację i przechowywanie dużych ilości danych w czasie rzeczywistym w oparciu o np. Bazę druid lub inne rozproszone bazy danych, zapewniając szybkie wielowymiarowe wyszukiwanie i możliwości zapytań statystycznych. |
| 1. System zapewnia wdrożenie samodzielne i klastrowe, aby zaspokoić potrzeby różnych scenariuszy; wdrożenie klastra jest wysoce niezawodne i zapewnia elastyczne rozszerzanie pojemności. |
| 1. Kolektor obsługuje telemetrię, w tym protokół GRPC. |
| 1. Moduł zbierający obsługuje zbieranie dzienników zgłaszanych przez urządzenia, wykrywanie wyjątków urządzeń w odpowiednim czasie i usuwanie błędów. |
| **Monitorowanie telemetria** | 1. Monitorowanie wskaźników wydajności urządzeń / płyt / chipów za pomocą telemetrii, w tym wykorzystania procesora / pamięci, wykorzystania elementów tabeli FIB, wykorzystania elementów tabeli MAC i wykorzystania zasobów TCAM. |
| 1. Monitorowanie wskaźników wydajności interfejsu za pomocą telemetrii, w tym liczby pakietów / bajtów / odrzuconych pakietów / pakietów błędów / pakietów rozgłoszeniowych / pakietów multiemisji / pakietów unicast / wykorzystania przepustowości w kierunkach odbierania i wysyłania. |
|  | 1. Monitorowanie liczby kolejek, bajty bufora za pomocą telemetrii z okresem zbierania 100 ms, aby precyzyjne monitorować micro-bursts pamięci podręcznej. |
| **Analiza stanu sieci** | 1. Wsparcie sprawdzania stanu zdrowia całej sieci. Musi wyświetlać stan łączności sieciowej, średnie opóźnienie transmisji, wskaźnik utraty pakietów i inne kluczowe wskaźniki. |
| 1. Wyświetlanie stanu sieci pod kątem różnych kryteriów, takich jak urządzenie, sieć i protokół w bieżących i określonych zakresach czasowych. Obsługa eksportu w czasie rzeczywistym lub regularne przesyłanie raportu oceny stanu w celu ułatwienia codziennej obsługi i konserwacji. |
| **Problemy z aktywnym wykrywaniem i lokalizacją** | 1. Przeglądanie listy problemów w bieżącym i określonym przedziale czasowym oraz szybkiego wyszukiwania problemów zgodnie z zadanymi warunkami filtrowania, takimi jak stan, struktura i obiekty. |
| 1. Wyświetlanie szczegółów problemów, w tym podstawowych informacji o problemach, przyczyn źródłowych i analizy wpływu na usługi sieci DC. |
| 1. Monitorowanie i aktywna identyfikacja wyjątków tabeli zasobów urządzenia, w tym zasobów ACL, elementów tabeli MAC, elementów tabeli ARP, elementów tabeli FIB4. |
| 1. Aktywne wykrywanie podrzędnych modułów optycznych lub łączy w sieci. Wskaźniki wykrywania obejmują odbiór/emitowanie mocy, napięcia, prądu polaryzacji, temperatury i anomalii CRC. |
| 1. Wspieranie aktywnej identyfikacji potencjalnych problemów takich jak pętle warstwy 2 w sieci wraz ze wskazaniem lokalizacji interfejsu powodującego pętlę. |
| **IP 360** | 1. Śledzenie IP maszyn wirtualnych, w tym adresu IP maszyny wirtualnej, dystrybucji adresów IPv4/IPv6, śledzenie historii dostępu do maszyn wirtualnych. |
| **Weryfikacja zmian / różnic** | 1. Automatyczne sprawdzanie różnic konfiguracji i tabel po zmianach sieci, w tym konfiguracji urządzenia / tabeli ARP / ND / RIB itp. oraz analizowanie szczegółowe pozycji zmian po zmianach sieci. |
| **Autoryzacja biznesowa** | 1. Wspiera weryfikację intencji biznesowych dostępności i izolacji. System wstępnie ustawia reguły weryfikacji intencji, a także umożliwia użytkownikom elastyczne dostosowywanie reguł weryfikacji intencji . |
| 1. Weryfikuje intencje osiągalności usług, w tym routingu, tunelu vxlan i weryfikacji osiągalności tej samej podsieci / między podsieciami / między VPC . |
| 1. Weryfikuje intencje izolacji usługi, zdefiniowane przez użytkownika reguły weryfikacji izolacji i weryfikuje, czy dwie podsieci (lub adres IP) są zgodne z intencją izolacji usługi. |
| **Szukaj w sieci** | 1. Obsługuje globalne wyszukiwanie obiektów sieciowych, takich jak urządzenia sieciowe, interfejsy, płyty, logiczne elementy sieci, OSPF, wpisy w tablicy ARP, wpisy w tablicy routingu IPv4/IPv6 i pliki konfiguracyjne w strukturze oraz wyświetla odpowiednie szczegóły. |
| 1. Obsługuje przeglądanie fizycznej topologii i hierarchicznych informacji o topologii obiektów sieciowych, takich jak urządzenia sieciowe, interfejsy, płyty, logiczne elementy sieci i OSPF w strukturze. |

**8. Zakres zamówienia obejmuje:**

1. Wykonanie i dostarczenie Projektu Technicznego Wdrożenia, zgodnie z Rozdziałem 9;
2. Przeprowadzenie warsztatów instruktażowych, zgodnie z Rozdziałem 10;
3. Dostawę wraz z rozładunkiem Sprzętu do miejsca wskazanego przez Zamawiającego, zgodnie z Rozdziałami 3 - 6;
4. Instalację oraz konfigurację dostarczonego Sprzętu oraz Oprogramowania SDN, zgodnie z Rozdziałem 11;
5. Przeprowadzenie testów akceptacyjnych Sprzętu, zgodnie z Rozdziałem 13;
6. Wykonanie i dostarczenie dokumentacji powykonawczej, zgodnie z Rozdziałem 13;
7. Udzielenie przez Wykonawcę gwarancji na dostarczony Sprzęt na *okres co najmniej 36 miesięcy (stanowi kryterium oceny ofert)*, od dnia podpisania bez zastrzeżeń przez Strony Protokołu Odbioru Wdrożenia, którego wzór stanowi **Załącznik nr 5** do Umowy, zgodnie z Rozdziałem 14.
8. Wykonawca jest zobowiązany do **wykonania i dostarczenia Projektu Technicznego Wdrożenia:**
   1. **Termin wykonania:** do 14 dni od dnia zawarcia Umowy.
   2. **Forma Projektu Technicznego Wdrożenia:** Elektroniczna, plik w formacie MS Word oraz PDF, zgodnie ze standardem określonym w Rozdziale 13 do niniejszego opisu.
   3. Przygotowany przez Wykonawcę Projekt Techniczny Wdrożenia podlegać będzie akceptacji przez Zamawiającego w trybie roboczym.
   4. Wymiana uwag Zamawiającego i Wykonawcy, wymaganych poprawek i aktualizacja odbywać się będzie drogą e-mailową na adresy wskazane w Umowie, w trybie roboczym.
   5. Akceptacja Projektu Technicznego Wdrożenia potwierdzona zostanie podpisanym bez zastrzeżeń przez Strony Protokołem Odbioru Projektu Technicznego Wdrożenia, którego wzór stanowi Załącznik nr 4 do Umowy.
   6. Zamawiający odbierze Projekt Techniczny Wdrożenia w terminie nie dłuższym niż 10 dni od daty jego przedłożenia przez Wykonawcę lub zgłosi do niego uwagi. Wykonawca ma obowiązek uwzględnić uwagi Zamawiającego i przedłożyć Projekt Techniczny Wdrożenia ponownie do odbioru w terminie 5 dni od daty otrzymania uwag.
   7. Projekt Techniczny Wdrożenia musi zawierać co najmniej następujące elementy:

1.WSTĘP

1.1 Zakres realizacji

1.2 Oznaczenia używane w opracowaniu

1.3 Opcje poufności informacji przedstawionych w opracowaniu

1.4 Cel projektu

1.5 Założenia projektowe

2. OPIS STOSOWANYCH ROZWIĄZAŃ TECHNICZNYCH

2.1 Architektura

2.1.1 Podział na architekturę fizyczną i logiczną systemu

3. KONFIGURACJA SPRZĘTU

3.1 Elementy składowe i nazewnictwo

3.2 Konfiguracja urządzeń wchodzących w skład Sprzętu

3.3 Połączenia fizyczne

4. REALIZOWANE USŁUGI

4.1 Aspekty bezpieczeństwa

5. SPECYFIKACJA SPRZĘTU

5.1 Lista sprzętu z parametrami technicznymi

5.2 Wymagania środowiskowe urządzeń

6. INSTALACJA FIZYCZNA

6.1 Scenariusze wdrożenia

6.2 Miejsce instalacji

6.3 Zalecenia do instalacji

6.4 Zasilanie urządzeń

6.5 Połączenia fizyczne między urządzeniami dostarczanego Sprzętu

* 1. Połączenia fizyczne Sprzętu ze środowiskiem sieciowym Zamawiającego

7. INTEGRACJA Z SYSTEMAMI ZAMAWIAJĄCEGO

7.1 Opis sposobu integracji:

* 1. Kont lokalnych administratorów Sprzętu
  2. Grup użytkowników
  3. Polityk dostępowych
  4. Integracji z system AAA,
  5. Integracji z systemem SIEM
  6. Integracji z systemem NTP
  7. Integracji z systemem DNS

8. ZARZĄDZANIE

8.1 Opis sposobu zarządzania urządzeniami Sprzętu

9. PROCEDURY OBSŁUGI ZGŁOSZEŃ BŁĘDÓW

9.1 Urządzeń Sprzętu

11. TESTY AKCEPTACYJNE Sprzętu

11.1 Proponowany sposób realizacji testów dla:

1. Weryfikacji poprawności licencji
2. Weryfikacji aktualności wersji
3. Testu przełączeniowego zasilania awaryjnego
4. Testu odporności na awarie w trybie HA
5. Weryfikacji prawidłowości ustawienia konfiguracji interfejsów sieciowych,
6. Weryfikacji prawidłowości ustawienia integracji z systemem AAA (uwierzytelnianie, autoryzacja, rozliczalność)
7. Weryfikacji prawidłowości ustawienia integracji z SIEM
8. Weryfikacji prawidłowości ustawienia integracji z NTP
9. Weryfikacji prawidłowości ustawienia integracji z DNS

10) Weryfikacja prawidłowości działania w sieci Zamawiającego.

1. **WARSZTATY INSTRUKTAŻOWE**

Wykonawca przeprowadzi warsztaty instruktażowe, w tym warsztaty przedwdrożeniowe oraz warsztaty powdrożeniowe, przy czym warsztaty przedwdrożeniowe muszą być przeprowadzone wg poniższych wymagań:

- warsztaty dla min. 20 administratorów,

- czas trwania warsztatów instruktażowych: co najmniej 3 dni, w terminie od poniedziałku do piątku, w godzinach pracy Zamawiającego, od 8:00 do 16:00 tj. co najmniej 24 godziny zegarowe,

- warsztaty odbędą się w dwóch różnych terminach – w pierwszym terminie dla min. 8 administratorów, w drugim terminie dla min. 8 administratorów.

* 1. Warsztaty instruktażowe muszą odbywać się w języku polskim lub angielskim.
  2. Zamawiający dopuszcza możliwość przeprowadzenia warsztatów instruktażowych zdalnie. W przypadku zorganizowania warsztatów instruktażowych zdalnie, nie ma zastosowania pkt 6 i 7 poniżej. W takim przypadku Wykonawca zobowiązany jest do zapewnienia Zamawiającemu wszelkiej infrastruktury (w szczególności narzędzia umożliwiającego zdalną komunikację pomiędzy uczestnikami warsztatów instruktażowych, a osobą realizującą warsztaty instruktażowe) umożliwiającej przeprowadzenie warsztatów instruktażowych zdalnie.
  3. W trakcie warsztatów instruktażowych każdy uczestnik musi mieć zapewniony dostęp do Sprzętu lub maszyn wirtualnych lub środowiska wirtualnego odwzorowującego rozwiązanie będące przedmiotem zamówienia, oraz do materiałów technicznych udostępnianych przez producenta urządzenia. W przypadku warsztatów on-line, Zamawiający zapewnia przenośne komputery i dostęp do sieci Internet dla osób skierowanych na warsztat instruktażowy.
  4. Po zakończeniu warsztatów instruktażowych uczestnicy otrzymają dokument potwierdzający ukończenie warsztatów instruktażowych.
  5. Wykonawca na czas warsztatów instruktażowych przeprowadzanych stacjonarnie zobowiązany jest do zapewnienia posiłków, w tym obiadu oraz serwisu kawowego w przerwach warsztatów instruktażowych, dla wszystkich uczestników warsztatów instruktażowych, oraz noclegów, dla wskazanych przez Zamawiającego osób.
  6. W przypadku wskazania przez Wykonawcę miejsca stacjonarnego warsztatów instruktażowych innego niż będące siedzibą Zamawiającego (Warszawa, Radom), Wykonawca zapewni transport, hotel i całodzienne wyżywienie uczestnikom warsztatów instruktażowych, których będzie ono dotyczyło.
  7. Wykonawca przedstawi w trybie roboczym, w terminie do 30 dni od dnia zawarcia umowy, propozycje co najmniej 2 terminów i lokalizacji warsztatów instruktażowych, do akceptacji przedstawiciela Zamawiającego.
  8. Najpóźniej na 3 dni przed proponowanym terminem warsztatów instruktażowych, Wykonawca przedstawi program warsztatów instruktażowych, który wymaga zatwierdzenia przez Zamawiającego.
  9. Przeprowadzenie warsztatów instruktażowych zostanie potwierdzone, wraz z innymi etapami realizacji przedmiotu zamówienia, w Protokole Odbioru Wdrożenia, którego wzór stanowi **Załącznik nr 5** do Umowy.
  10. W terminie od dnia zawarcia Umowy, lecz po uruchomieniu Sprzętu w środowisku produkcyjnym Zamawiającego, Wykonawca przeprowadzi **powdrożeniowe warsztaty instruktażowe** dla Sprzętu zainstalowanego przez Wykonawcę wg poniższych wymagań:
      1. warsztaty odbędą się:

- dla min. 20 administratorów,

- czas trwania warsztatów instruktażowych: co najmniej 2 dni, w terminie od poniedziałku do piątku, w godzinach pracy Zamawiającego, od 8:00 do 16:00, tj. co najmniej 16 godzin zegarowych,

* + 1. zakres warsztatów instruktażowych będzie zawierał przede wszystkim elementy wynikające z Projektu Technicznego Wdrożenia, będzie obejmował zagadnienia z instalacji, konfiguracji, w szczególności zagadnienia związane z: obsługą dostarczonego Sprzętu, instalacją, konfiguracją, obsługą operatorską, w tym zarządzaniem administracyjnym, zagadnieniami możliwych sytuacji awaryjnych w środowisku Zamawiającego,
    2. warsztaty zostaną zrealizowane na dostarczonym Sprzęcie.

Wykonawca zrealizuje warsztaty w co najmniej 2 różnych terminach dla Sprzętu, w pierwszym terminie dla min. 10 administratorów, w drugim terminie dla min. 10 administratorów. Wykonawca przedstawi w trybie roboczym, w terminie do 30 dni od dnia zawarcia umowy propozycje co najmniej 2 terminów i lokalizacji warsztatów instruktażowych, do akceptacji przedstawiciela Zamawiającego.

* + 1. przeprowadzenie warsztatów zostanie potwierdzone, wraz z innymi etapami realizacji przedmiotu zamówienia, w Protokole Odbioru Wdrożenia, którego wzór stanowi **Załącznik nr 5** do Umowy.
    2. najpóźniej 3 dni przed proponowanym terminem warsztatów, Wykonawca przedstawi program warsztatów, który wymaga zatwierdzenia przez Zamawiającego.

1. **WDROŻENIE: DOSTAWA, INSTALACJA I KONFIGURACJA DOSTARCZONEGO SPRZĘTU I OPROGRAMOWANIA SDN:**
2. Zamawiający wymaga, aby Sprzęt:
   1. spełniał wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie,
   2. był fabrycznie nowy, kompletny, nieużywany i bez oznak używania, nierefabrykowany i nieregenerowany, nienaprawiany, nie podlegał ponownej obróbce oraz był w jednolitej konfiguracji,
   3. nie był zarejestrowany na inny podmiot niż Wykonawca lub Zamawiający,
   4. nie wykazywał jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość ich prawidłowego użytkowania,
   5. został dopuszczony do obrotu gospodarczego na terytorium Rzeczpospolitej Polskiej,
   6. był zgodny ze stosowanymi normami technicznymi,
   7. posiadał certyfikaty dopuszczające do stosowania w Unii Europejskiej,
   8. posiadał gwarancję na Sprzęt zgodnie z Rozdziałem 12 niniejszego opisu.
3. Na dzień składania ofert, Sprzęt nie może być zakwalifikowane przez Producenta do wycofania ze sprzedaży i wsparcia w okresie następnych 24 miesięcy liczonych od dnia składania ofert.
4. Wykonawca jest zobowiązany do dostarczenia wszystkich niezbędnych elementów konfiguracyjnych i montażowych, w tym odpowiedniej ilości patchcordów światłowodowych, okablowania sieciowego oraz innych elementów niezbędnych do instalacji, konfiguracji i uruchomienia dostarczonego Sprzętu.
5. Instalacja dostarczonego Sprzętu, musi polegać na podłączeniu do środowiska sieciowego Zamawiającego Sprzętu w sposób określony w Projekcie Technicznym Wdrożenia.
6. Po zainstalowaniu i uruchomieniu rozwiązania, Wykonawca przystąpi do konfiguracji Sprzętu i Oprogramowania SDN w środowisku Zamawiającego.
7. Integracja z systemami AAA, SIEM, NTP, DNS nastąpi w sposób opisany w Projekcie Technicznym Wdrożenia.
8. Dostawa, instalacja i konfiguracja zostaną potwierdzone, wraz z innymi etapami realizacji przedmiotu zamówienia, w Protokole Odbioru Wdrożenia, którego wzór stanowi **Załącznik nr 5** do Umowy.
9. Opis wymagań instalacji i konfiguracji:
10. Zamawiający wymaga, aby dostarczone w ramach tego Zamówienia przełączniki zostały podłączone do sieci LAN Zamawiającego.
11. Zamawiający wymaga, aby 2 przełączniki Spine zostały zainstalowane w OPR i 2 przełączniki Spine zostały zainstalowane w OPP.
12. Zamawiający wymaga, aby 6 przełączników Leaf zostało zainstalowanych w OPP.
13. Zamawiający wymaga, aby serwer – arbiter został zainstalowany w OPW.
14. Zamawiający wymaga, aby Oprogramowanie SDN Zamawiającego zostało skonfigurowane w taki sposób, aby:
15. W OPR zostały uruchomione 2 przełączniki Spine
16. W OPP zostały uruchomione 2 przełączniki Spine
17. W OPR zostały uruchomione przełączniki Leaf Zamawiającego opisane w Rozdziale 2
18. W OPP zostało uruchomionych 6 przełączników Leaf dostarczonych w ramach tego Zamówienia
19. W OPW został uruchomiony serwer – arbiter
20. W OPP został uruchomiony zapasowy klaster Oprogramowania SDN
21. Oprogramowanie SDN Zamawiającego zostało rozciągnięte na OPR i OPP i zarządzało wszystkimi przełącznikami Zamawiającego opisanymi w Rozdziale 2 i dostarczonymi w ramach tego Zamówienia, stanowiąc jednolite środowisko SDN.
22. Oprogramowanie SDN Zamawiającego pozwalało na sukcesywne przełączanie serwerów z obecnej sieci LAN Zamawiającego do środowiska SDN w OPR i OPP.
23. **TESTY AKCEPTACYJNE**
24. **Termin realizacji:** po dostawie, instalacji i konfiguracji Sprzętu i Oprogramowania SDN.
25. **Czas trwania testów:** do 14 dni.
26. W ramach testów, zgodnie z Projektem Technicznym Wdrożenia, wykonane zostaną następujące czynności:
27. Weryfikacja poprawności licencji,
28. Weryfikacja aktualności systemu operacyjnego zainstalowanego na urządzeniach dostępowych,
29. Test przełączeniowy zasilania awaryjnego,
30. Test odporności na awarie w trybie HA,
31. Weryfikacja prawidłowości ustawienia integracji z systemami AAA, SIEM, NTP, DNS,
32. Test poprawności działania Sprzętu i Oprogramowania SDN w środowisku produkcyjnym.
33. Do czasu zakończenia testu poprawności działania Sprzętu i Oprogramowania SDN w środowisku produkcyjnym, Wykonawca jest zobowiązany do usunięcia wszystkich problemów zgłoszonych w trakcie trwania testu.
34. Wynik testów akceptacyjnych wdrożenia potwierdzony zostanie wraz z innymi etapami wdrożenia na podpisanym bez zastrzeżeń przez Strony Protokole Odbioru Wdrożenia, którego wzór stanowi Załącznik nr 5 do Umowy.
35. **Dokumentacja Powykonawcza**
36. **Termin realizacji:** do 55 dni od dnia zawarcia Umowy, po wykonaniu testów akceptacyjnych.
37. **Forma:** Elektroniczna, plik w formacie MS Word oraz PDF zgodnie ze standardem określonym w Rozdziale 13 niniejszego opisu.
38. Po zakończeniu testów akceptacyjnych, Wykonawca dostarczy do akceptacji Zamawiającego dokumentację powykonawczą wdrożenia.
39. Dokument podlegać będzie akceptacji przez Zamawiającego w trybie roboczym. Wymiana uwag, wymaganych poprawek i aktualizacja wersji dokumentów odbywać się będzie drogą e-mailową, na adresy wskazane w Umowie.
40. Akceptacja dokumentacji powykonawczej wdrożenia potwierdzona zostanie wraz z innymi etapami wdrożenia na Protokole Odbioru Wdrożenia, którego wzór stanowi Załącznik nr 5 do Umowy.
41. Wymagany zakres Dokumentacji Powykonawczej Wdrożenia:

1.WSTĘP

1.1 Zakres realizacji

1.2 Oznaczenia używane w opracowaniu

1.3 Opcje poufności informacji przedstawionych w opracowaniu

1.4 Cel projektu

1.5 Weryfikacja założeń projektowych

2. OPIS ZASTOSOWANYCH ROZWIĄZAŃ TECHNICZNYCH

2.1 Architektura systemu

2.1.1 Podział na architekturę fizyczną i logiczną systemu

3. KONFIGURACJA ELEMENTÓW SYSTEMU

3.1 Elementy składowe i nazewnictwo

3.2 Konfiguracja urządzeń Sprzętu i Oprogramowania SDN

3.3 Połączenia fizyczne

4. REALIZOWANE USŁUGI

4.1 Integracja z AAA

4.2 Integracja z SIEM, NTP, DNS

4.3 Aspekty bezpieczeństwa

4.4 Polityka bezpieczeństwa

4.5 Zarządzanie polityką bezpieczeństwa

4.6 Konta na Sprzęcie

4.7 Uwierzytelnianie użytkowników i administratorów.

5. SPECYFIKACJA SPRZĘTU I OPROGRAMOWANIA SDN

5.1 Dostarczone urządzenia i oprogramowanie

5.2 Wymagania środowiskowe urządzeń

5.3 Zestawianie wersji zainstalowanych produktów.

6. INSTALACJA FIZYCZNA ELEMENTÓW SYSTEMU

6.1 Zrealizowany scenariusz wdrożenia

6.2 Miejsce instalacji urządzeń

6.3 Zasilanie urządzeń

6.4 Połączenia fizyczne między urządzeniami w systemie

6.5 Połączenia fizyczne urządzeń Sprzętu i Oprogramowania SDN ze środowiskiem sieciowym Zamawiającego

6.6 Zalecenia powdrożeniowe.

7. ZARZĄDZANIE URZĄDZENIAMI

7.1 Procedury:

7.1.1 Dodania konta użytkownika

7.1.2 Integracji z AAA

7.1.3 Integracji z SIEM

7.1.4 Integracji z NTP

7.1.5 Integracji z DNS

8. PROCEDURY OBSŁUGI ZGŁOSZEŃ

9.WYNIKI TESTÓW AKCEPTACYJNYCH.

1. **Gwarancja:**
2. Wykonawca zobowiązuje się do udzielenia gwarancji dla zainstalowanego Sprzętu przez okres **min. 36 m-cy** (*zgodnie z ofertą wykonawcy*) od dnia podpisania bez zastrzeżeń przez Strony Protokołu Odbioru Wdrożenia, którego wzór stanowi **Załącznik nr 5** do Umowy.
3. Zakres gwarancji obejmuje:
4. Aktualizację oprogramowania (w szczególności firmware, oprogramowanie zarządzające zainstalowane na Sprzęcie), w szczególności poprzez dostarczanie nowych wersji oprogramowania, dostarczanie wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych.
5. Wsparcie w korzystaniu z oprogramowania polega w szczególności na:
6. świadczeniu Zamawiającemu pomocy w zakresie obsługi Zgłoszeń, w formie elektronicznej poprzez serwis internetowy pod wskazany przez Wykonawcę adres, drogą elektroniczną lub telefonicznie na adresy/numery wskazane w Umowie, w języku polskim,
7. zapewnieniu elektronicznego dostępu do informacji w języku polskim lub angielskim na temat posiadanego oprogramowania, wykaz znanych symptomów i rozwiązań w języku polskim lub angielskim, biuletynów technicznych, poprawek programistycznych oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu - pod wskazanym przez Wykonawcę adresem internetowym,
8. rozwiązywaniu problemów dotyczących bieżącej eksploatacji i konfiguracji Sprzętu,
9. zapewnieniu elektronicznego dostępu do informacji na temat posiadanego Sprzętu, wykazu znanych symptomów i rozwiązań w języku polskim lub angielskim (w tym programy korygujące do oprogramowania), biuletynów technicznych, dokumentacji technicznych poprawek programistycznych, oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu.
10. W ramach gwarancji Wykonawca będzie zobowiązany do świadczenia usług wsparcia gwarancyjnego (gwarancji) dla administratorów Zamawiającego przez 7 dni w tygodniu, 24 godziny na dobę, przez wszystkie dni w roku.
11. W ramach gwarancji Wykonawca będzie zobowiązany do obsługi Zgłoszeń Błędów. Definicje błędów opisano w Umowie.
12. Błędy będą zgłaszane Wykonawcy elektronicznie. Potwierdzenie Zgłoszenia Błędu stanowi przesłany przez Zamawiającego do Wykonawcy formularz Protokołu Zgłoszenia Błędu (stanowiący ***Załącznik nr 6*** do Umowy) na adres email wskazany w Umowie.
13. Zamawiający wymaga, aby w ramach gwarancji Wykonawca reagował na Zgłoszenie Błędu Sprzętu (potwierdził odebranie Zgłoszenia) w czasie nie dłuższym niż 1 godziny od momentu przekazania przez Zamawiającego Zgłoszenia. W Czasie reakcji Wykonawca ma obowiązek potwierdzić przyjęcie zgłoszenia tą samą drogą, którą nastąpiło zgłoszenie.
14. Zamawiający wymaga, aby Czas naprawy Błędu wynosił:
15. nie dłużej niż 8 godzin (nie wyłączając świąt, sobót i niedziel) - w przypadku Zgłoszenia Błędu Krytycznego, od momentu przekazania przez Zamawiającego Zgłoszenia,
16. nie dłużej niż 48 godzin (nie wyłączając świąt, sobót i niedziel) - w przypadku Zgłoszenia Błędu Poważnego, od momentu przekazania przez Zamawiającego Zgłoszenia,
17. nie dłużej niż 14 dni (nie wyłączając świąt, sobót i niedziel) - w przypadku Zgłoszenia Błędu Drobnego, od momentu przekazania przez Zamawiającego Zgłoszenia.
18. W Czasie naprawy przewidzianym dla poszczególnych rodzajów Zgłoszeń, Wykonawca ma obowiązek zdiagnozować i usunąć problem, co zostanie potwierdzone podpisaniem Protokołu z wykonania naprawy (stanowiący ***Załącznik nr 7*** do Umowy).
19. Wszelkie koszty transportu i diagnozowania niesprawnego Sprzętu pokrywa Wykonawca. Sprzęt, który uległ awarii (w którym zaistniał Błąd), będzie zwracany do Wykonawcy na jego koszt, po każdorazowej wymianie.
20. W przypadku wystąpienia drugiego Błędu tego samego Sprzętu, Wykonawca zobowiązuje się do wymiany niesprawnego Sprzętu na nowy, wolny od wad, w terminie 5 dni od daty przekazania Zgłoszenia przez Zamawiającego. Do nowego elementu/Sprzętu Wykonawca zobowiązany jest załączyć jego dokumentację w języku polskim lub angielskim. Potwierdzeniem wydania Sprzętu w ramach wymiany, będzie Protokół Odbioru Sprzętu dostarczony w ramach wymiany, którego wzór stanowi **Załącznik nr 8** do Umowy, podpisany bez zastrzeżeń przez przedstawiciela Zamawiającego. Z dniem podpisania przez Zamawiającego powyższego protokołu bez zastrzeżeń, na Zamawiającego przechodzi własność wymienianego Sprzętu wskazanego w protokole.
21. W przypadku wymiany Sprzętu na nowy, wolny od wad, okres gwarancji biegnie na nowo od daty dostarczenia i uruchomienia prawidłowego Sprzętu, co zostanie potwierdzone podpisanym przez Strony bez zastrzeżeń Protokołem Odbioru Sprzętu, którego wzór stanowi **Załącznik nr 8** do Umowy.
22. Odpowiedzialność za szkody powstałe w związku z transportem Sprzętu dostarczonego w ramach wymiany/naprawy do siedziby Zamawiającego oraz w związku z instalacją Sprzętu w siedzibie Zamawiającego ponosi Wykonawca, do momentu podpisania przez przedstawiciela Zamawiającego Protokół Odbioru Sprzętu bez zastrzeżeń.
23. Po usunięciu Błędu, dostarczeniu sprzętu zastępczego lub wymianie na Sprzęt nowy, wolny od wad, obowiązkiem Wykonawcy będzie również uruchomienie Sprzętu wraz z Oprogramowaniem SDN w miejscu jego użytkowania oraz odtworzenia pełnej konfiguracji i danych oraz funkcjonalności sprzed zgłoszenia Błędu.
24. Sprzęt dostarczony w ramach wymiany musi być nowy, wolny od wad, o parametrach wydajnościowych i funkcjonalnych takich samych lub wyższych, jak Sprzęt wymieniany.
25. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za wady fizyczne Sprzętu niezależnie od uprawnień wynikających z gwarancji jakości.
26. Wykonawca jest zobowiązany w dniu wykonania naprawy do sporządzenia w 2 egzemplarzach dokumentu Protokołu Wykonania Naprawy (którego wzór stanowi **Załącznik nr 7** do Umowy) potwierdzającego wykonanie naprawy. Ww. dokument musi zostać podpisany (data, godzina i podpis) przez przedstawiciela Zamawiającego, co będzie równoznaczne z potwierdzeniem przez Zamawiającego wykonania naprawy przez Wykonawcę. Data i godzina podpisania ww. dokumentu przez przedstawiciela Zamawiającego jest datą i godziną wykonania naprawy. Zamawiający podpisze protokół niezwłocznie.
27. W przypadku udzielenia gwarancji przez producenta Sprzętu, Wykonawca zobowiązuje się przekazać Zamawiającemu ważne dokumenty gwarancyjne.
28. Wykonawca zobowiązany jest przeprowadzić 1 gwarancyjny serwis prewencyjny na każde 12 miesięcy trwania okresu gwarancji całego Sprzętu, oprogramowania na zgłoszenie Zamawiającego, w terminach w trybie roboczym ustalonych z przedstawicielem Zamawiającego, polegające na:
    1. oczyszczeniu;
    2. odkurzeniu wnętrza sprzętu, oczyszczeniu wentylatorów;
    3. analizie plików komunikatów o błędach sprzętowych;
    4. sprawdzeniu i ew. korekcie (po akceptacji Zamawiającego) wersji oprogramowania typu BIOS, firmware, driver, oprogramowania zarządzającego.

Przeprowadzenie każdego z serwisów prewencyjnych zostanie potwierdzone Protokołem Wykonania Serwisu Prewencyjnego, którego wzór stanowi **Załącznik nr 10** do Umowy.

1. Wykonawca zobowiązuje się do prowadzenia rejestru zdarzeń gwarancyjnych zawierającego:
2. liczbę Błędów, konsultacji, serwisów prewencyjnych,
3. Czasów naprawy,
4. specyfikację Sprzętu/oprogramowania, którego dotyczyło Zgłoszenie,
5. informacji o wymienionych lub naprawionych podzespołach,
6. informacji o sposobie naprawy Sprzętu.
7. Wykonawca jest zobowiązany do przekazania Zamawiającemu w formie elektronicznej rejestru, o którym mowa powyżej, w ostatnim dniu trwania okresu gwarancji.
8. Rejestr będzie podlegał weryfikacji przez Zamawiającego, w przypadku stwierdzenia nieprawidłowości w zapisach, Zamawiający zwraca rejestr Wykonawcy w celu uzupełnienia/poprawienia.
9. Zamawiający zastrzega sobie prawo wglądu do rejestru, o którym mowa w ust. 21, w każdym czasie trwania okresu gwarancji, a Wykonawca jest zobowiązany rejestr ten udostępnić w terminie nie dłuższym niż 2 dni od żądania jego udostępnienia.
10. Zamawiający zastrzega sobie prawo do zmiany lokalizacji Sprzętu, przy czym zmiana będzie realizowana w granicach woj. mazowieckiego. Zamawiający z co najmniej 14 dniowym wyprzedzeniem poinformuje Wykonawcę o planowanej zmianie. Wykonawca nie może odmówić świadczenia gwarancji w takiej sytuacji.
11. **Standard dokumentacji projektowej infrastruktury**

|  |  |
| --- | --- |
| **Nazwa** | Standard dokumentacji projektowej infrastruktury. |
| **Streszczenie** | Dokument opisuje standard dokumentacji projektowej dla komponentów infrastrukturalnych. |
| **Opis** | **Cechy ogólne**   * Dokumentacja musi być przygotowana zgodnie z szablonem ustalonym dla całej organizacji lub wyodrębnionego projektu. * Kolejne sekcje dokumentacji muszą być numerowane w sposób kontekstowy – numeracja kolejnych podsekcji musi być poprzedzona numerem sekcji wyższej.   **Strona tytułowa**   * Musi zawierać co najmniej następujące informacje:   + Tytuł dokumentu   + Nazwę lub numer tematu (zagadnienia)   + Nazwę projektu   + Informacje o autorach dokumentu:     - Imiona, Nazwiska     - Zajmowane stanowiska lub role pełnione w projekcie     - Nazwa organizacji * Strona tytułowa może zawierać inne, dodatkowe informacje, zgodnie z ustalonym szablonem, np.:   + Identyfikator projektu, identyfikator dokumentu w projekcie lub inne identyfikatory   + Dodatkowe informacje precyzujące temat zagadnienia, np. nazwę podprojektu, określenie konkretnego tematu lub zagadnienia   + Nazwę organizacji , nazwę jednostki organizacyjnej   + Adres organizacji lub jednostki organizacyjnej   + Bardziej szczegółowe informacje o autorach dokumentu:     - Telefony kontaktowe     - Adresy poczty elektronicznej   **Metryka**   * Metryka dokumentu musi zawierać co najmniej następujące informacje:   + Określenie aktualnej wersji dokumentu   + Datę publikacji dokumentu   + Bardziej szczegółowe informacje o autorach dokumentu (jeśli nie były określone na stronie tytułowej):     - Telefony kontaktowe     - Adresy poczty elektronicznej   + Historię zmian w dokumencie, zawierającą co najmniej następujące pola:     - Wersję     - Datę     - Imiona i nazwiska autorów zmian     - Krótki opis dokonanych zmian   + Informację o akceptacji dokumentu – miejsca na podpisy właściwych osób (jeżeli akceptacja jest wymagana) * Metryka musi zawierać:   + Informacje o sposobie weryfikacji dokumentu     - Datę dokonania weryfikacji     - Imiona i nazwiska osób dokonujących weryfikacji     - Zajmowane stanowiska i role pełnione w projekcie     - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)   + Informacje o osobie odpowiedzialnej za nadzorowanie projektu w ramach którego przygotowywana jest dokumentacja:     - Imiona i nazwiska     - Zajmowane stanowiska lub role pełnione w projekcie     - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)   **Prawa autorskie**   * Sekcja musi zawierać informacje o autorze opracowania   **Zastrzeżenia**   * Sekcja musi zawierać informacje dotyczące poufności dokumentu   **Indeksy**   * Sekcja musi zawierać spis treści * Sekcja musi zawierać:   + Spis rysunków   + Spis tabel * Sekcja może zawierać inne indeksy   **Słowniki**   * Sekcja musi zawierać:   + Słownik pojęć, skrótów, określeń i zwrotów używanych w dokumencie.  Jeśli opisywane pojęcie jest skrótem, słownik musi zawierać rozwinięcie skrótu. Jeśli pojęcie jest słowem obcym, słownik musi zawierać tłumaczenie słowa na język polski. * Sekcja musi zawierać:   + Opis symboli graficznych wykorzystywanych w rysunkach.   **Konwencje typograficzne**   * Sekcja musi zawierać opis sposobu oznaczania charakterystycznych treści dokumentu, np.   + Wszystkie słowa obcego pochodzenia piszemy *kursywą*;   + Wszystkie nazwy komponentów piszemy **czcionką pogrubioną**;   + Wszystkie fragmenty komunikacji z terminalem zawarte są w szarym polu otoczonym czarną ramką;   + Wszelkie przykłady komunikacji z systemem operacyjnym opisywane są czcionką regularną.   + Wyjątkowo istotne uwagi przedstawiono w ramce z wykrzyknikiem.   **Wstęp**   * Sekcja musi zawierać:   + Cel opracowania dokumentu   + Informację o dokumentach powiązanych lub referencje do innych dokumentów, których treść może mieć znaczenie w kontekście zawartości tego konkretnego dokumentu * Sekcja może zawierać:   + Określenie docelowych odbiorców dokumentu   + Streszczenie dokumentu, opisujące pokrótce zawartość dalszych sekcji   **Założenia i wymagania**  Sekcja musi zawierać informacje o przedłożonych wymaganiach oraz założeniach przyjętych w ramach tworzenia projektu.   * Sekcja musi zawierać:   + Wymagania ogólne   + Założenia ogólne * Sekcja musi zawierać:   + Wymagania i założenia szczegółowe, np. w zakresie:     - Cech funkcjonalnych rozwiązania     - Cech ergonomicznych rozwiązania     - Parametrów niezawodnościowych     - Parametrów wydajnościowych     - Utrzymania rozwiązania     - Wdrożenia rozwiązania     - Interfejsów komunikacyjnych oraz metod interakcji     - Parametrów fizycznych     - Ograniczeń   + Inne wymagania i założenia specyficzne dla opisywanego rozwiązania, nie ujęte w żadnej z powyższych kategorii   **Zakres projektu**   * Sekcja musi opisywać:   + Zakres projektowanego rozwiązania;   + Zasięg rozwiązania – definiujący rozległość rozwiązania (ulokowanie komponentów w poszczególnych ośrodkach).   **Definicja środowisk**   * Sekcja musi zawierać definicje i opis projektowanych środowisk, z wyszczególnieniem podstawowych zadań realizowanych przez każde środowisko, np.   + Produkcyjne   + Akceptacyjne   + Testowe   + Deweloperskie   **Rozwiązanie techniczne**  Sekcja opisuje konkretne rozwiązanie techniczne w odniesieniu do każdego ze zdefiniowanych środowisk.  Dokument musi zawierać opis wszystkich zagadnień technicznych, które można zdefiniować na etapie projektowania.  Zagadnienia mogą być dopracowane i uszczegółowione podczas etapu wdrożenia rozwiązania. Wówczas wszelkie dokonane w nich zmiany względem dokumentacji projektowej będą uwzględnione w dokumentacji powykonawczej.   * Dla każdego środowiska muszą być opisane (o ile mają zastosowanie):   + Architektura logiczna rozwiązania     - Rozmieszczenie komponentów zwirtualizowanych (jeśli występują)   + Budowy fizyczna     - Rozmieszczenie komponentów w środowiskach fizycznych   + Wykaz komponentów użytych do budowy rozwiązania (jeśli w projekcie następuje wybór urządzeń/oprogramowania), np:     - Serwery, terminale, komputery użytkowników     - Macierze i inne zasoby dyskowe     - Biblioteki taśmowe i wirtualne     - Komponenty sieci LAN     - Komponenty sieci SAN     - Komponenty sieci WAN     - Bazy danych     - Aplikacje     - Oprogramowanie do zarządzania     - Inne oprogramowanie     - Stacje robocze   albo:   * + - Definicja rozwiązań dla katalogu technicznego     - Definicja rozwiązań dla katalogu usług   + Architektura sieciowa i połączenia     - Schemat fizyczny połączeń w sieci LAN/SAN/WAN     - Opis planowanego/przewidywanego obciążenia poszczególnych sieci przez komunikację w systemie     - Adresacja     - Nazwy w systemie DNS     - Źródła i sposób synchronizacji czasu   + Wytyczne konfiguracyjne dla poszczególnych komponentów rozwiązania.   **Integracja**   * Punkty styku oraz sposób integracji z innymi rozwiązaniami   + Wykaz integrowanych systemów   + Koncepcja rozwiązania   **Bezpieczeństwo**   * Opis konfiguracji mechanizmów bezpieczeństwa dla wszystkich komponentów:   + Wykorzystane mechanizmy ochrony komunikacji   + Sposób uwierzytelniania użytkowników   + Uprawnienia dla ról, użytkowników, grup   + Mechanizmy szyfrowania * Sposób tworzenia kopii zapasowych rozwiązania   + Koncepcja – w szczególność sposób kopiowania poszczególnych   + Wymagane usługi   + Definicje podstawowych parametrów polityk kopiowania danych (np. harmonogramu kopiowania) * Sposób odtwarzania systemu z kopii – koncepcja.   **Zarządzanie**   * Wykaz wykorzystywanych mechanizmów zarządzania * Opis sposobu zrządzania rozwiązaniem   **Procedury**   * Wykaz procedur dla rozwiązania   **Testy**  Sekcja musi zawierać wykaz testów, jakie należy przeprowadzić po wdrożeniu rozwiązania.  Szczegółowy opis testów musi się znaleźć w scenariuszach testowych, które wraz z wynikami i raportami z realizacji testów stanowią element dokumentacji zbiorczej.   * Testy muszą obejmować:   + Cechy funkcjonalne rozwiązania   + Cechy wydajnościowe rozwiązania   **Zakres dokumentacji powykonawczej**   * Informacja o zakresie dokumentacji powykonawczej   **Załączniki**   * Wykaz załączników do dokumentacji projektowej |

**Standard dokumentacji powykonawczej infrastruktury**

|  |  |
| --- | --- |
| **Nazwa** | Standard dokumentacji powykonawczej infrastruktury. |
| **Streszczenie** | Dokument opisuje standard dokumentacji powykonawczej dla rozwiązań infrastrukturalnych. |
| **Opis** | **Cechy ogólne**   * Dokumentacja musi być przygotowana zgodnie z szablonem ustalonym dla całej organizacji lub wyodrębnionego projektu. * Kolejne sekcje dokumentacji muszą być numerowane w sposób kontekstowy – numeracja kolejnych podsekcji musi być poprzedzona numerem sekcji wyższej. * Format dokumentu oraz sposób jego przetwarzania mogą być szczegółowo określone przez Kancelarię Tajną lub Administratora Informacji Niejawnych * Opis sekcji przedstawiono w kolejności, w jakiej muszą one występować w dokumencie. * Główną ideą opracowania dokumentacji powykonawczej jest przedstawienie opisu zbudowanego systemu lub środowiska w sposób jak najlepiej odzwierciedlający rzeczywistość.Wsadem do dokumentacji powykonawczej mogą być elementy, stworzonej wcześniej, dokumentacji projektowej – zmodyfikowane, uzupełnione i uszczegółowione w sposób urealniający stan systemu i prezentujący rozwiązanie w jego ostatecznej, zaakceptowanej i używanej formie – tak, jak ono rzeczywiście wygląda.   **Strona tytułowa**   * Musi zawierać co najmniej następujące informacje:   + Tytuł dokumentu   + Nazwę lub numer tematu (zagadnienia)   + Nazwę projektu   + Informacje o autorach dokumentu:     - Imiona, Nazwiska     - Zajmowane stanowiska lub role pełnione w projekcie     - Nazwę organizacji * Strona tytułowa może zawierać inne, dodatkowe informacje, zgodnie z ustalonym szablonem, np.:   + Identyfikator projektu, identyfikator dokumentu w projekcie lub inne identyfikatory   + Dodatkowe informacje precyzujące temat zagadnienia, np. nazwę podprojektu, określenie konkretnego tematu lub zagadnienia   + Nazwę organizacji , nazwę jednostki organizacyjnej   + Adres organizacji lub jednostki organizacyjnej   + Bardziej szczegółowe informacje o autorach dokumentu:     - Telefony kontaktowe     - Adresy poczty elektronicznej   **Metryka**   * Metryka dokumentu musi zawierać co najmniej następujące informacje:   + Określenie aktualnej wersji dokumentu   + Datę publikacji dokumentu   + Bardziej szczegółowe informacje o autorach dokumentu (jeśli nie były określone na stronie tytułowej):     - Telefony kontaktowe     - Adresy poczty elektronicznej   + Historię zmian w dokumencie, zawierającą co najmniej następujące pola:     - Wersję     - Datę     - Imiona i nazwiska autorów zmian     - Krótki opis dokonanych zmian   + Informację o akceptacji dokumentu – miejsca na podpisy właściwych osób (jeżeli akceptacja jest wymagana) * Metryka musi zawierać:   + Informacje o sposobie weryfikacji dokumentu     - Datę dokonania weryfikacji     - Imiona i nazwiska osób dokonujących weryfikacji     - Zajmowane stanowiska i role pełnione w projekcie     - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)   + Informacje o osobie odpowiedzialnej za nadzorowanie projektu w ramach którego przygotowywana jest dokumentacja:     - Imiona i nazwiska     - Zajmowane stanowiska lub role pełnione w projekcie     - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)   **Prawa autorskie**   * Sekcja musi zawierać informacje o ochronie praw autorskich   **Zastrzeżenia**   * Sekcja musi zawierać informacje dotyczące poufności dokumentu   **Indeksy**   * Sekcja musi zawierać spis treści * Sekcja musi zawierać:   + Spis rysunków   + Spis tabel * Sekcja może zawierać inne indeksy   **Słowniki**   * Sekcja musi zawierać:   + Słownik pojęć, skrótów, określeń i zwrotów używanych w dokumencie.  Jeśli opisywane pojęcie jest skrótem, słownik musi zawierać rozwinięcie skrótu. Jeśli pojęcie jest słowem obcym, słownik musi zawierać tłumaczenie słowa na język polski. * Sekcja musi zawierać:   + Opis symboli graficznych wykorzystywanych w rysunkach.   **Konwencje typograficzne**   * Sekcja musi zawierać opis sposobu oznaczania charakterystycznych treści dokumentu, np.   + Wszystkie słowa obcego pochodzenia piszemy *kursywą*;   + Wszystkie nazwy komponentów piszemy **czcionką pogrubioną**;   + Wszystkie fragmenty komunikacji z terminalem zawarte są w szarym polu otoczonym czarną ramką;   + Wszelkie przykłady komunikacji z systemem operacyjnym opisywane są czcionką regularną.   + Wyjątkowo istotne uwagi przedstawiono w ramce z wykrzyknikiem.   **Wstęp**   * Sekcja musi zawierać:   + Cel opracowania dokumentu   + Informację o dokumentach powiązanych lub referencje do innych dokumentów, których treść może mieć znaczenie w kontekście zawartości tego konkretnego dokumentu * Sekcja może zawierać:   + Określenie docelowych odbiorców dokumentu   + Streszczenie dokumentu, opisujące pokrótce zawartość dalszych sekcji   **Zakres i zasięg rozwiązania**   * Sekcja musi opisywać:   + Zakres zbudowanego rozwiązania;   + Zasięg zbudowanego rozwiązania – opisujący rozległość rozwiązania (ulokowanie komponentów w poszczególnych ośrodkach).   **Definicja środowisk**   * Sekcja musi zawierać definicję i opis zbudowanych środowisk, z wyszczególnieniem podstawowych zadań realizowanych przez każde środowisko, np.   + Produkcyjne   + Akceptacyjne   + Testowe   + Deweloperskie   **Rozwiązanie techniczne**  Sekcja opisuje konkretne rozwiązanie techniczne w odniesieniu do każdego ze zdefiniowanych środowisk.  Dokument musi zawierać opis wszystkich zagadnień technicznych stworzonego rozwiązania.   * Dla każdego środowiska muszą być opisane (o ile mają zastosowanie):   + Wynikowa architektura logiczna rozwiązania     - Rozmieszczenie poszczególnych komponentów w przestrzeni całego rozwiązania   + Budowy fizyczna     - Fizyczne rozmieszczenie komponentów w wyodrębnionych środowiskach operacyjnych   + Cechy funkcjonalne uzyskanego rozwiązania   + Cechy ergonomiczne rozwiązania   + Parametry niezawodnościowe   + Parametry wydajnościowe   + Sposób utrzymania rozwiązania   + Interfejsy komunikacyjne oraz metod interakcji   + Parametry fizyczne   + Ograniczenia   + Komponenty użyte do budowy rozwiązania, np:     - Serwery, terminale, komputery użytkowników     - Macierze i inne zasoby dyskowe     - Biblioteki taśmowe i wirtualne     - Komponenty sieci LAN     - Komponenty sieci SAN     - Komponenty sieci WAN     - Bazy danych     - Aplikacje     - Oprogramowanie do zarządzania     - Inne oprogramowanie     - Stacje robocze   + Architektura sieciowa i połączenia     - Schemat fizyczny połączeń w sieci LAN/SAN/WAN     - Adresacja     - Tabela połączeń sieciowych (źródło/cel/protokół przykład w szablonie KiC)     - Nazwy w systemie DNS     - Źródła i sposób synchronizacji czasu   + Konfiguracja poszczególnych komponentów rozwiązania.   **Integracja**   * Sekcja musi opisywać punkty styku oraz sposób integracji zbudowanego rozwiązania z innymi rozwiązaniami. Musi zawierać co najmniej:   + Wykaz zintegrowanych systemów   + Opis użytych rozwiązań integracyjnych   **Bezpieczeństwo**   * Opis konfiguracji mechanizmów bezpieczeństwa dla wszystkich komponentów:   + Wykorzystane mechanizmy ochrony komunikacji   + Sposób uwierzytelniania użytkowników   + Uprawnienia dla ról, użytkowników, grup   + Mechanizmy szyfrowania * Sposób tworzenia kopii zapasowych rozwiązania   + Sposób kopiowania danych poszczególnych komponentów   + Harmonogramu kopiowania * Sposób odtwarzania systemu z kopii.   **Zarządzanie**   * Wykaz wykorzystywanych mechanizmów zarządzania * Opis sposobu zrządzania komponentami rozwiązania   **Załączniki**   * Wykaz załączników do dokumentacji powykonawczej |

Szablon tworzenia procedur administracyjnych i operacyjnych.

|  |  |
| --- | --- |
| **Identyfikator** | Unikalny identyfikator procedury |
| **Nazwa** | **Szablon procedury** (*Wpisać nazwę procedury*) |
| **Rodzaj** | Rodzaj procedury: Operacyjna/Administracyjna |
| **Streszczenie** | Cel i krótki opis procedury |
| **Zakres stosowania** | Informacja o zakresie stosowania procedury:   * na jakich urządzeniach/instancjach wirtualnych urządzeń może być wykonana; |
| **Wykonawca** | Informacja o użytkowniku, który musi/może przeprowadzić procedurę:   * funkcja użytkownika w strukturach organizacji; * wymagane uprawnienia użytkownika wykonującego procedurę:   + nazwa konta/kont w systemie;   + nazwa konta/kont w aplikacji;   + rola/role w systemie. |
| **Współzależności** | Nazwy oraz identyfikatory procedur współzależnych, które muszą/mogą być wykonane w związku z realizacją czynności opisanych w tej procedurze.   |  |  | | --- | --- | | **Identyfikator** | **Nazwa** | | Identyfikator 1 | Nazwa procedury 1. | | Identyfikator 2 | Nazwa procedury 2. | | … | … | | Identyfikator N | Nazwa procedury N. | |
|  | |
| **Sytuacja początkowa** | Opis sytuacji, jaka musi zaistnieć, aby wykonanie procedury mogło być rozpatrywane.  Ostateczna decyzja o zrealizowaniu procedury podejmowana jest po upewnieniu się, że spełnione zostaływarunki opisane w polu *Warunki użycia*. |
| **Warunki użycia** | Opis warunków, jakie muszą być spełnione, aby możliwe było wykonanie procedury, np.:   * wskazanie na określony typ urządzeń/instancji * informacja o wymaganej dostępności sieci LAN/SAN/WAN lub innych komponentów; * informacja o problemach powodujących, że zastosowanie procedury jest uzasadnione/wskazane. |
| **Sytuacja końcowa** | Informacja o wymaganym stanie końcowym komponentów, które biorą udział w realizacji procedury lub na które jej wykonanie może wpłynąć. |
| **Proces** | Opis kroków realizowanych sekwencyjnie w celu prawidłowego przeprowadzenia procedury.  Sekwencyjność postępowania w procesie może być modyfikowana poprzez:   * warunki (np. „Krok 4: Krok 4 wykonywany jest tylko w sytuacji, gdy wynik polecenia *polecenie* w kroku 3 był następujący: *wynik*”); * warunkowe polecenia skoku – pominięcia ciągu kroków (np. „Krok 6: Jeśli serwer *serwer1* jest wyłączony, przejdź do wykonania kroku 9”); * pętle (np. „Krok 8: Jeśli wynik polecenia *polecenie* jest następujący: *wynik*, kontynuuj proces ponownie od kroku 6”).  |  |  | | --- | --- | | **Krok** | **Opis czynności** | | 1 | Opis czynności realizowanych w kroku 1. | | 2 | Opis czynności realizowanych w kroku 2. | | … | … | | N | Opis czynności realizowanych w kroku N. |   Opis procesu może być uzupełniony schematem blokowym. Przykładowy schemat przedstawiono poniżej.  Wykorzystanie schematu nie jest obowiązkowe i zależy od stopnia komplikacji procedury.  Decyzję o ewentualnym umieszczeniu schematu blokowego podejmuje autor procedury.  Obraz zawierający tekst, zrzut ekranu, Czcionka, diagram  Opis wygenerowany automatycznie  *Rysunek 1 Przykład schematu blokowego procedury.* |

Standard tworzenia planu testów i scenariuszy testowych.

Wstęp

Niniejszy dokument opisuje standard tworzenia Planu Testów Akceptacyjnych Budowy/Rozbudowy Systemu, który będzie przygotowywany dla każdego systemu infrastrukturalnego podlegającemu rozbudowie w ramach realizacji projektu. Plan Testów Akceptacyjnych Rozbudowy Systemu będzie dokumentował działania, jakie należy wykonać, aby uzyskać potwierdzenie, że rozbudowa systemu osiągnęła zamierzone cele i funkcjonalności.

Zakłada się, że testy budowy/rozbudowy każdego systemu infrastrukturalnego będą realizowane w środowisku produkcyjnym i potwierdzą jego gotowość do rozpoczęcia eksploatacji.

Cel dokumentu

Dokument został przygotowany w celu:

* + - * + ustanowienia standardu tworzenia Planów Testów Akceptacyjnych Rozbudowy Systemu,
        + dostarczenia autorom Planów Testów Akceptacyjnych Rozbudowy Systemu wytycznych, do których należy się stosować podczas tworzenia Planów Testów Akceptacyjnych Rozbudowy Systemu,
        + zapewnienia jednolitości dokumentacji testowej tworzonej na potrzeby rozbudowy różnych systemów infrastrukturalnych,
        + budowania zestawu Planu Testów Akceptacyjnych Rozbudowy Systemu,
        + opracowywania Scenariuszy Testów Akceptacyjnych Rozbudowy Systemu,
        + zapewnienia kompletności tworzonych Planów Testów Akceptacyjnych Rozbudowy Systemu.

Odbiorcy dokumentu

Dokument przeznaczony jest dla Wykonawców rozbudowy systemów infrastrukturalnych - autorów Planów Testów Akceptacyjnych Rozbudowy Systemu.

Struktura Procedury Testowej

Struktura Procedury Testowej jest uniwersalna i będzie miała zastosowanie do wszystkich wdrażanych systemów w ramach projektu. W szczególności będzie służyła do budowy Planu Testów Akceptacyjnych Rozbudowy Systemu i Scenariuszy Testów Akceptacyjnych Rozbudowy Systemu w scenariuszach rozbudowy systemów infrastrukturalnych.

Procedura Testowa składa się następujących sekcji:

• identyfikacji wdrażanego systemu,

• wykazu czynności przygotowawczych,

• wykazu scenariuszy testowych,

• wykazu czynności końcowych.

Identyfikacja wdrażanego systemu

W sekcji identyfikacji wdrażanego systemu dokumentowane są dane ewidencyjne systemu, dla którego tworzony jest Plan Testów Akceptacyjnych Rozbudowy Systemu takie jak nazwa i identyfikator systemu oraz jego krótki opis.

Ponadto w sekcji tej należy umieścić (alternatywnie: dołączyć, jako załącznik lub wskazać lokalizację w repozytorium) Projekt Wykonawczy Rozbudowy Systemu – dokument stanowiący produkt fazy planowania opisanej w Scenariuszu Rozbudowy.

Wykaz czynności przygotowawczych Procedury Testowej

W sekcji opisującej czynności przygotowawcze należy zidentyfikować a następnie uporządkować według kolejności ich wykonywania wszystkie czynności, jakie należy przeprowadzić przed przystąpieniem do testów tj. przed wykonywaniem scenariuszy testowych. Sekcja czynności przygotowawczych Procedury Testowej jest wypełniana tylko w takim przypadku, gdy czynności przygotowawcze mają zastosowanie w danej Procedurze Testowej.

Czynności przygotowawcze powinny obejmować między innymi takie zadania jak:

* + - * + weryfikacja dostępności raportu z testów umożliwiającego rejestrowanie przebiegu i wyników wykonania Procedury Testowej.
        + weryfikacja poprawności instalacji i konfiguracji oprogramowania podlegającego testom.
        + weryfikacja zasobów niezbędnych do przeprowadzenia i udokumentowania testów
        + weryfikacja oprogramowania niepodlegającego testom, ale niezbędnego do prawidłowego przeprowadzenia testów.
        + weryfikacja użytkowników i ich uprawnień systemowych niezbędnych do wykonania testów.
        + weryfikacja dostępności i poprawności danych testowych.
        + weryfikacja dostępności narzędzi do weryfikacji wyników poszczególnych testów (np. skrypty, narzędzia pomiarowe, narzędzia monitorujące, narzędzia administracyjne itp.).

Przebieg i rezultaty wykonania czynności przygotowawczych dokumentowane są w raporcie z wykonania Procedury Testowej (stanowią integralną część dokumentacji z wykonanych testów).

Wykaz scenariuszy testowych Procedury Testowej

W sekcji przedstawiającej wykaz scenariuszy testowych należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie scenariusze testowe przewidziane do realizacji w ramach Procedury Testowej. Następnie każdy scenariusz testowy należy opisać zgodnie z poniższymi wytycznymi.

Podczas identyfikacji scenariuszy testowych należy kierować się zasadą, że każdy scenariusz testowy to zbiór przypadków (kroków) testowych, których wykonanie jest potrzebne do sprawdzenia poprawności działania systemu w określonym zakresie. Każdy scenariusz testowy powinien być odzwierciedleniem dokładnie określonej funkcjonalności systemu lub sprawdzeniem cech niefunkcjonalnych takich jak: wydajność, niezawodność, bezpieczeństwo itp.

Struktura scenariusza testowego

Opis każdego scenariusza testowego posiada następującą strukturę:

• identyfikację scenariusza testowego,

• wykaz czynności przygotowawczych,

• wykaz przypadków testowych,

• wykaz czynności końcowych.

Identyfikacja scenariusza testowego

W sekcji identyfikacji scenariusza testowego dokumentowane są następujące dane ewidencyjne scenariusza testowego:

* + - * + unikalny identyfikator (w ramach Planu Testów Akceptacyjnych Rozbudowy Systemu) i nazwa scenariusza testowego,
        + opis scenariusza testowego przedstawiający cel/cele jego wykonania,
        + typ scenariusza (rodzaj testu wykonywanego w ramach danego scenariusza np. testy funkcjonalne, testy wydajnościowe, testy niezawodności, testy bezpieczeństwa itp.).

Wykaz czynności przygotowawczych scenariusza testowego

W sekcji opisującej czynności przygotowawcze scenariusza testowego należy zidentyfikować a następnie uporządkować, według kolejności ich wykonywania, wszystkie czynności, jakie powinny być wykonane przed przystąpieniem do realizacji scenariusza testowego tj. przed wykonywaniem pierwszego przypadku testowego. Sekcja czynności przygotowawczych scenariusza testowego jest wypełniana tylko w takim przypadku, gdy te czynności mają zastosowanie w danym scenariuszu testowym.

Czynności przygotowawcze scenariusza testowego są uzupełnieniem czynności przygotowawczych Procedury Testowej. Obejmują one te czynności, które nie mogą być wykonane w ramach czynności przygotowawczych Procedury Testowej, gdyż:

* + - * + uniemożliwiłby wykonanie poprzedzających scenariuszy testowych lub zafałszowałyby wynik wykonania tych scenariuszy;
        + uniemożliwiłby wykonanie następnych scenariuszy testowych lub zafałszowałby wynik wykonania tych scenariuszy; w tym przypadku, w ramach czynności końcowych danego scenariusza testowego należy wykonać odpowiednie działania eliminujące efekt wykonania czynności przygotowawczych w celu umożliwienia wykonania następnych scenariuszy testowych.

Wykaz przypadków testowych scenariusza testowego

W sekcji przedstawiającej wykaz przypadków testowych scenariusza testowego należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie przypadki testowe przewidziane do realizacji w ramach danego scenariusza testowego. Następnie każdy przypadek testowy należy opisać zgodnie z poniższymi wytycznymi.

Podczas identyfikacji przypadków testowych należy kierować się zasadą, że każdy przypadek testowy jest określony przez: zbiór danych wejściowych, warunków początkowych oraz oczekiwanych wyników i warunków końcowych i jest on tworzony w celu realizacji określonej funkcjonalności i/lub w celu weryfikacji zgodności z określonym wymaganiem.

Struktura przypadku testowego

Opis każdego przypadku testowego posiada następującą strukturę:

• identyfikacja przypadku testowego,

• wykaz czynności przygotowawczych,

• warunki początkowe,

• zestaw danych testowych,

• lista weryfikowanych wymagań/funkcjonalności,

• wykaz kroków przypadku testowego,

• oczekiwany rezultat wykonania przypadku testowego,

• metodę weryfikacji poprawności rezultatu wykonania przypadku testowego,

• wykaz czynności końcowych.

Identyfikacja przypadku testowego

W sekcji identyfikacji przypadku testowego dokumentowane są następujące dane ewidencyjne przypadku testowego:

* + - * + unikalny identyfikator (w ramach Planu Testów Akceptacyjnych Rozbudowy Systemu) i nazwa przypadku testowego.
        + opis przypadku testowego przedstawiający cel jego wykonania.

Wykaz czynności przygotowawczych przypadku testowego

Analogicznie jak w przypadku czynności przygotowawczych scenariusza testowego.

Warunki początkowe przypadku testowego

W sekcji opisującej warunki początkowe przypadku testowego dokumentuje się wszystkie warunki, jakie muszą być spełnione, aby przystąpić do wykonywania kroków przypadku testowego. Spełnienie tych warunków powinno być zapewnione poprzez poprawne wykonanie:

* + - * + czynności przygotowawczych Procedury Testowej,
        + czynności przygotowawczych oraz czynności końcowych wszystkich poprzedzających scenariuszy i przypadków testowych.

Zestawy danych testowych dla przypadku testowego

W niniejszej sekcji należy opisać wszystkie zestawy danych testowych wykorzystywane w krokach danego przypadku testowego. Dla każdego zestawu należy podać:

* + - * + unikalny identyfikator (w ramach Planu Testów Akceptacyjnych Rozbudowy Systemu).
        + charakterystykę danych opisywanego zestawu (opcjonalnie - np. w przypadki pojedynczych danych wprowadzanych przez testera do systemu poprzez GUI; obowiązkowo – np. w przypadku dużego wolumenu danych wprowadzanych do systemu poprzez automatyczny import).
        + nazwy i konkretne wartości danych testowych (alternatywnie: dołączyć zbiór z zestawem danych testowych, jako załącznik lub wskazać lokalizację zbioru w repozytorium).

Lista weryfikowanych wymagań/funkcjonalności

Każdy przypadek testowy ma na celu weryfikację zgodności z określonym wymaganiem i/lub weryfikację poprawności określonej funkcjonalności. W niniejszej sekcji należy wskazać wymagania i/lub funkcjonalności weryfikowanych (testowanych) w ramach danego przypadku testowego. Poprawny wynik wykonania danego przypadku testowego jest tożsamy z pozytywną weryfikacją wymagań i/lub funkcjonalności powiązanych z danym przypadkiem testowym o ile te wymagania i/lub funkcjonalności nie są powiązane z jeszcze innymi przypadkami testowymi. Jeśli istnieje powiązanie z innymi przypadkami testowymi, to pozytywna weryfikacja określonego wymagania/funkcjonalności następuje w przypadku pozytywnego wykonania wszystkich przypadków testowych powiązanych z danym wymaganiem/funkcjonalnością.

Wykaz kroków przypadku testowego

W sekcji przedstawiającej wykaz kroków przypadku testowego należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie czynności, jakie należy przeprowadzić w celu wykonania danego przypadku testowego. Dla każdego kroku należy wskazać identyfikator odpowiedniego zestawu danych testowych, o ile w danym kroku następuje wprowadzenie danych testowych do systemu.

Oczekiwany rezultat wykonania przypadku testowego

Dla każdego przypadku testowego należy opisać oczekiwany rezultat wykonania danego przypadku testowego (wykonania wszystkich kroków przypadku testowego). Zgodność oczekiwanego rezultatu wykonania przypadku testowego z rzeczywistym rezultatem otrzymanym po wykonaniu danego przypadku testowego jest tożsamy z pozytywnym wynikiem wykonania danego przypadku testowego.

Metoda weryfikacji poprawności rezultatu wykonania przypadku testowego

W niniejszej sekcji należy opisać metodę weryfikacji rezultatu wykonania przypadku testowego z rezultatem oczekiwanym. W szczególności w przypadku analizy dużego wolumenu danych wynikowych lub zebranych pomiarów, należy dokładnie wskazać narzędzia (np. skrypty, narzędzia pomiarowe, narzędzia monitorujące, narzędzia administracyjne itp.) niezbędne do wykonania weryfikacji oraz sposób i wyniki ich użycia.

Wykaz czynności końcowych przypadku testowego

W sekcji opisującej czynności końcowe przypadku testowego należy zidentyfikować a następnie uporządkować według kolejności wykonywania wszystkie czynności, jakie należy wykonać po zakończeniu wykonywania przypadku testowego tj. po wykonaniu ostatniego kroku przypadku testowego. Sekcja czynności końcowych przypadku testowego jest wypełniania tylko w takim przypadku, gdy czynności końcowe mają zastosowanie w danym przypadku testowym.

Czynności końcowe przypadku testowego obejmują te czynności, bez których wykonanie następnych przypadków i scenariuszy testowych byłoby niemożliwe lub wynik ich wykonania byłby zafałszowany lub które wynikają z wymogów polityk bezpieczeństwa.

Wykaz czynności końcowych scenariusza testowego

Analogicznie jak w przypadku czynności końcowych przypadku testowego.

Wykaz czynności końcowych Procedury Testowej

W sekcji opisującej czynności końcowe Procedury Testowej należy zidentyfikować a następnie uporządkować według kolejności wykonywania wszystkie czynności, jakie należy wykonać po zakończeniu wykonywania ostatniego scenariusza testowego. Sekcja czynności końcowych Procedury Testowej jest wypełniana tylko w takim przypadku, gdy czynności końcowe mają zastosowanie w danej Procedurze.

W szczególności czynności końcowe mogą obejmować:

* + - * + Zabezpieczenie/usunięcie danych wrażliwych.
        + Usunięcie/zablokowanie użytkowników i uprawnień w celu eliminacji ryzyka nieuprawnionego dostępu i użytkowania środowiska testowego.
        + Zwolnienie limitowanych zasobów i narzędzi niezbędnych do realizacji innych zadań.
        + Przywrócenie standardowych ustawień zasobów, dla których na czas testów nastąpiła rekonfiguracja.
        + Archiwizację danych, konfiguracji i logów, w celu dalszej analizy.