Załacznik nr 1

*Dostawa i montaż urządzeń sieciowych dla POPD w ramach projektu „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych w Sprawach Karnych (iSDA 2.0)*”

**Spis treści**

[1 Słownik pojęć i skrótów. 5](#_Toc19094711)

[2 Ogólny Opis Przedmiotu Zamówienia 6](#_Toc19094712)

[2.1 Kontekst postepowania 6](#_Toc19094713)

[2.2 Przedmiot postępowania POS-7 8](#_Toc19094714)

[3 SPECYFIKACJA PRODUKTÓW 9](#_Toc19094715)

[3.1 Dostawa sprzętu i oprogramowania 9](#_Toc19094716)

[3.2 Projekt techniczny ITS dla Środowisk Produkcyjnych (dokument) 11](#_Toc19094717)

[3.3 Projekt techniczny ITS Środowisk Nieprodukcyjnych (dokument) 13](#_Toc19094718)

[3.4 Opracowanie Scenariuszy Testów (Dokument) 14](#_Toc19094719)

[3.5 Montaż sprzętu, instalacja oprogramowania (usługa) 16](#_Toc19094720)

[3.6 Konfiguracja środowisk zgodnie z projektami technicznymI (usługa) 19](#_Toc19094721)

[3.7 Przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa) 20](#_Toc19094722)

[3.8 Opracowanie dokumentacji powykonawczej (dokument) 21](#_Toc19094723)

[3.9 Opracowanie procedur utrzymania ITS (dokument) 22](#_Toc19094724)

[3.10 Przygotowanie materiałów szkoleniowych (dokument) 22](#_Toc19094725)

[3.11 Szkolenia (Usługa) 23](#_Toc19094726)

[3.12 Serwis gwarancyjny, wsparcie eksploatacji 26](#_Toc19094727)

[3.13 Specyfikacja dostarczanego Sprzętu i Oprogramowania Gotowego 29](#_Toc19094728)

[3.13.1 Infrastruktura sieci LAN i SAN 29](#_Toc19094729)

[3.13.1.1 WYMAGANIA OGÓLNE DLA WSZYSTKICH DOSTARCZANYCH ROZWIĄZAŃ 29](#_Toc19094730)

[3.13.1.2 Przełączniki SAN TYP I – 7 sztuk 31](#_Toc19094731)

[3.13.1.2.1 MODUŁ SAN SFP 16Gb STANDARDU SW – 224 sztuki 33](#_Toc19094732)

[3.13.1.3 Przełączniki LAN – wymagania ogólne 33](#_Toc19094733)

[3.13.1.4 Przełącznik LAN TYP I - 2 sztuki 35](#_Toc19094734)

[3.13.1.5 Przełącznik LAN TYP II - 15 sztuk 36](#_Toc19094735)

[3.13.1.6 Przełącznik LAN TYP III - 2 sztuki 36](#_Toc19094736)

[3.13.1.7 Przełącznik LAN TYP IV - 4 sztuki 37](#_Toc19094737)

[3.13.1.8 WKŁADKI I KABLE OPTYCZNE DO PRZEŁĄCZNIKÓW LAN 40](#_Toc19094738)

[3.13.1.8.1 MODUŁ SFP 1GE STANDARDU 1000Base-T – 52 sztuki 40](#_Toc19094739)

[3.13.1.8.2 MODUŁ SFP 1GE STANDARDU SX – 142 sztuki 40](#_Toc19094740)

[3.13.1.8.3 MODUŁ SFP+ 10GE STANDARDU SR – 274 sztuki 40](#_Toc19094741)

[3.13.1.8.4 MODUŁ QSFP+ 40GE STANDARDU SR4 – 12 sztuk 40](#_Toc19094742)

[3.13.1.8.5 Przewód QSFP+ AOC 100GE o długości 3M – 18 sztuk 41](#_Toc19094743)

[3.13.1.8.6 Przewód QSFP+ AOC 100GE o długości 10M – 16 sztuk 41](#_Toc19094744)

[3.13.1.9 Urządzenia bezpieczeństwa 42](#_Toc19094745)

[3.13.1.9.1 MODUŁ ZDALNEGO DOSTĘPU VPN – WYMAGANIA OGÓLNE DLA KONCENTRATORA VPN 42](#_Toc19094746)

[3.13.1.9.2 KONCENTRAROR VPN TYP I – 4 sztuki (dwie pary redundantne) 43](#_Toc19094747)

[3.13.1.9.3 Koncentrator VPN TYP II – 2 sztuki 44](#_Toc19094748)

[3.13.1.9.4 URZĄDZENIA NGFW/NGIOS - WYMAGANIA OGÓLNE DLA URZĄDZEŃ NGFW/NGIPS 45](#_Toc19094749)

[3.13.1.9.5 URZĄDZENIE NGFW/NGIPS TYP I – 2 sztuki 47](#_Toc19094750)

[3.13.1.9.6 URZĄDZENIE NGFW/NGIPS TYP II + 2 sztuki 48](#_Toc19094751)

[3.13.1.9.7 URZĄDZENIE NGFW/NGIPS TYP III – 2 sztuki 49](#_Toc19094752)

[3.13.1.9.8 URZĄDZENIE NGFW/NGIPS TYP IV – 2 sztuki 49](#_Toc19094753)

[3.13.1.9.9 URZĄDZENIE NGFW/NGIPS TYP V – 4 sztuki 51](#_Toc19094754)

[3.13.1.9.10 URZĄDZENIE NGFW/NGIPS TYP VI – 1 sztuka 51](#_Toc19094755)

[3.13.1.9.11 URZĄDZENIE NGFW/NGIPS TYP VII – 5 sztuk 52](#_Toc19094756)

[3.13.1.9.12 URZĄDZENIE NGFW/NGIPS TYP VIII – 2 sztuki 52](#_Toc19094757)

[3.13.1.9.13 URZĄDZENIE NGFW/NGIPS TYP IX – 12 sztuk 53](#_Toc19094758)

[3.13.1.9.14 URZĄDZENIE ANTY-DDOS – WYMAGANIA OGÓLNE 54](#_Toc19094759)

[3.13.1.9.15 URZĄDZENIE ANTY-DDOS TYP I - 2 sztuki 55](#_Toc19094760)

[3.13.1.9.16 URZĄDZENIE ANTY-DDOS TYP II – 2 sztuki 55](#_Toc19094761)

[3.13.1.9.17 SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ - WYMAGANIA OGÓLNE DLA SYSTEMU OCHRONY POCZTY ELEKTRONICZNEJ 56](#_Toc19094762)

[3.13.1.9.18 SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ TYP I – 2 sztuki 58](#_Toc19094763)

[3.13.1.9.19 SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ TYP II – 1 sztuka 58](#_Toc19094764)

[3.13.1.9.20 OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW- WYMAGANIA OGÓLNE DLA OPROGRAMOWANIA ANTYWIRUSOWEGO/EDR DLA SERWERÓW 59](#_Toc19094765)

[3.13.1.9.21 OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP I 61](#_Toc19094766)

[3.13.1.9.22 OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP II 61](#_Toc19094767)

[3.13.1.9.23 OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP III 62](#_Toc19094768)

[3.13.1.9.24 SYSTEM SANDBOX - WYMAGANIA OGÓLNE DLA SYSTEMU SANDBOX 63](#_Toc19094769)

[3.13.1.9.25 SYSTEM SANDBOX TYP I – 2 sztuki 66](#_Toc19094770)

[3.13.1.9.26 SYSTEM SANDBOX TYP II – 2 sztuki 67](#_Toc19094771)

[3.13.1.9.27 SYSTEM SANDBOX TYP III – 2 sztuki 68](#_Toc19094772)

[3.13.1.10 APPLICATIONS DELIVERY CONTROLLERS 69](#_Toc19094773)

[3.13.1.10.1 URZĄDZENIA ADC (APPLICATIONS DELIVERY CONTROLLERS)- WYMAGANIA OGÓLNE DLA URZĄDZEŃ ADC 69](#_Toc19094774)

[3.13.1.10.2 URZĄDZENIA ADC TYP I – 2 sztuki 73](#_Toc19094775)

[3.13.1.10.3 URZĄDZENIA ADC TYP II – 6 sztuk 74](#_Toc19094776)

[3.13.1.10.4 URZĄDZENIA ADC TYP III – 17 sztuk 74](#_Toc19094777)

[3.13.1.11 Inne 76](#_Toc19094778)

[3.13.1.11.1 SZAFA RACK – 3 sztuki 76](#_Toc19094779)

[3.13.1.11.2 SERWER AUTORYZACYJNY – WYMAGANIE OGÓLNE 76](#_Toc19094780)

[3.13.1.11.2.1 SERWER AUTORYZACYJNY TYP I – 2 sztuki 78](#_Toc19094781)

[3.13.1.11.2.2 SERWER AUTORYZACYJNY TYP II – 2 sztuki 79](#_Toc19094782)

[3.13.1.11.2.3 SERWER AUTORYZACYJNY TYP III – 2 sztuki 79](#_Toc19094783)

[3.13.1.12 Oprogramowanie monitorowania I zarządzania 80](#_Toc19094784)

[3.13.1.12.1 SYSTEM ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ - WYMAGANIA OGÓLNE DLA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ 80](#_Toc19094785)

[3.13.1.12.1.1 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP I – 1 sztuka 81](#_Toc19094786)

[3.13.1.12.1.2 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP II – 1 sztuka 82](#_Toc19094787)

[3.13.1.12.1.3 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP III – 1 sztuka 82](#_Toc19094788)

[3.13.1.12.2 SYSTEM ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA- WYMAGANIA OGÓLNE DLA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA 82](#_Toc19094789)

[3.13.1.12.2.1 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP I – 1 sztuka 86](#_Toc19094790)

[3.13.1.12.2.2 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP II – 1 sztuka 86](#_Toc19094791)

[3.13.1.12.2.3 INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP III 86](#_Toc19094792)

[3.13.1.13 System zarządzania logami 88](#_Toc19094793)

[3.13.1.13.1 MODUŁ KORELACJI ZDARZEŃ (SIEM) 88](#_Toc19094794)

[3.14 Spis rysunków 96](#_Toc19094795)

[3.15 Spis tabel 96](#_Toc19094796)

# Słownik pojęć i skrótów.

POPD – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

ZOPD – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

NPOPD – Środowisko nieprodukcyjne w Podstawowym Ośrodku Przetwarzania Danych.

SWE – strefa wewnętrzna środowiska produkcyjnego,

SZE – strefa zewnętrzna środowiska produkcyjnego

SNP – strefa środowiska nieprodukcyjnego.

# Ogólny Opis Przedmiotu Zamówienia

## Kontekst postepowania

Prokuratura Krajowa realizuje projekt „Rozwój Systemu Digitalizacji Akt Postępowań Przygotowawczych w Sprawach Karnych (iSDA-2.0)” współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś priorytetowa nr 2 „E-Administracja i otwarty rząd”, Działanie 2.1.

Projekt iSDA-2.0 został podzielony na cztery komponenty przedstawione na Rysunek 1. Komponenty zostaną zrealizowane w ramach postępowań przetargowych POS-2.1:, POS-04, POS-05, POS-06, POS07 oraz-POS-08. Realizacja poszczególnych komponentów Projektu iSDA-2.0 w ramach postępowań przedstawiony jest poniżej:

1. Komponent - System PROK-SYS w ramach postępowania POS-04.

2. Komponent - Centralne Usługi Infrastrukturalne w ramach postępowania POS-05.

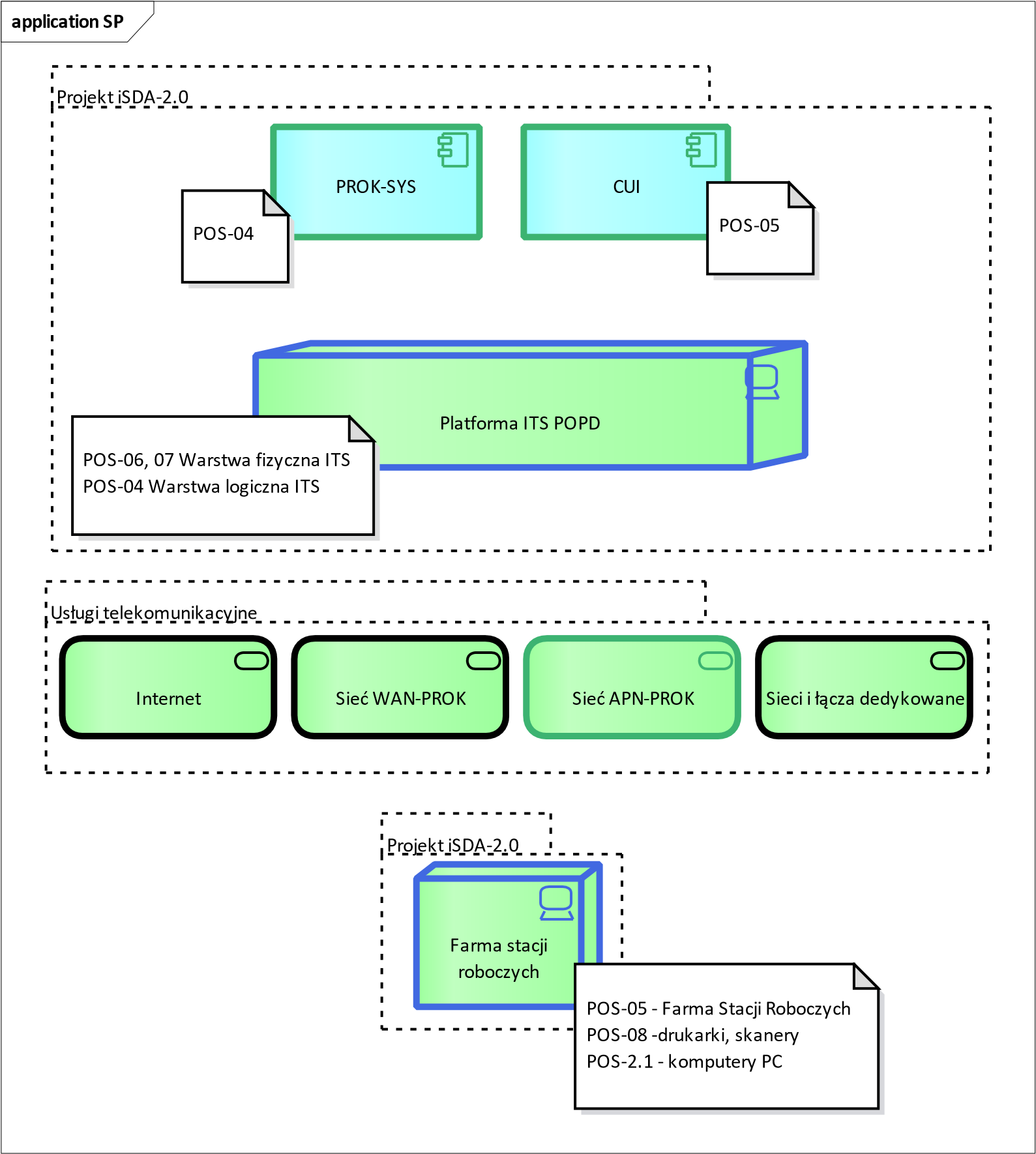
3. Komponent - Platforma ITS POPD wykonana w ramach:

1. Projekt techniczny ITS, dostawa sprzętu komputerowego (serwery, macierze itp.) oprogramowania gotowego i instalacja warstwy fizycznej ITS oraz konfiguracja warstwy logicznej ITS wykonywany w ramach postępowania POS-06,
2. Projekt techniczny ITS, dostawa sprzętu sieci LAN i SAN, oprogramowania gotowego i instalacja na warstwie fizycznej oraz konfiguracja warstwy logicznej ITS w ramach postępowania POS-07,
3. projekt warstwy logicznej ITS w ramach Projektu POS-04.

4. Komponent - Farma Stacji Roboczych wykonana w ramach:

1. dostawa stacji roboczych (komputerów PC) w ramach postępowania POS-2.1,
2. dostawa drukarek, urządzeń skanujących oraz urządzeń wielofunkcyjnych w ramach postępowania POS-08.
3. integracja posiadanych przez Zamawiającego stacji roboczych oraz dostarczonych w ramach POS-2.1 w farmę stacji roboczych w ramach postępowania POS-05.

Wykonawca POS-04 w Projekcie iSDA-2.0 pełni rolę integratora wszystkich komponentów opisanych powyżej.



Rysunek 1 Komponent Projektu iSDA-2.0

## Przedmiot postępowania POS-7

Postępowanie przetargowe POS-7 obejmuje:

1. Dostawę sprzętu i oprogramowania dla Środowiska Produkcyjnego POPD i środowisk nieprodukcyjnych TOPD zgodnie z wymaganiami określonymi w Rozdziale 7.
2. Wykonanie Projektu technicznego ITS dla Środowiska Produkcyjnego w POPD.
3. Wykonanie Projektu technicznego ITS dla Środowisk Nieprodukcyjnych TOPD.
4. Opracowanie Scenariuszy Testów Sprzętu obejmujących:
   1. Scenariusze testów sprzętu dla Środowiska Produkcyjnego POPD
   2. Scenariusze testów sprzętu dla Środowisk Nieprodukcyjnych
5. Montaż sprzętu i konfiguracja dostarczanego ITS zgodnie z opracowanym Projektem Technicznym ITS.
6. Przeprowadzenie testów dostarczanego ITS wg zaakceptowanych przez Zamawiającego scenariuszy testów.
7. Opracowanie dokumentacji powykonawczej.
8. Opracowanie procedur utrzymania warstwy fizycznej i logicznej ITS.
9. Szkolenia.
10. Gwarancja na dostarczony sprzęt oraz oprogramowanie.
11. Wsparcie techniczne.

# SPECYFIKACJA PRODUKTÓW

## Dostawa sprzętu i oprogramowania

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-DOSSPRZ-01 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| POS7-DOSSPRZ-02 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| POS7-DOSSPRZ-03 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| POS7-DOSSPRZ-04 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| POS7-DOSSPRZ-05 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy. |
| POS7-DOSSPRZ-06 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy |
| POS7-DOSSPRZ-07 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego. |
| POS7-DOSSPRZ-08 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| POS7-DOSSPRZ-09 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania lub serwerowni. |
| POS7-DOSSPRZ-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania lub serwerowni. |
| POS7-DOSSPRZ-11 | Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania. Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie i środki transportu umożliwiające wykonanie tych prac. |
| POS7-DOSSPRZ-12 | Dostarczana infrastruktura techniczno-systemowa musi być zgodna z prawem obowiązującym podmioty publiczne. W szczególności wymagana jest zgodność z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych |
| POS7-DOSSPRZ-13 | Wykonawca musi dostarczyć niewyspecyfikowane elementy ITS, które są niezbędne do prawidłowego funkcjonowania wyspecyfikowanych elementów ITS. |
| POS7-DOSSPRZ-14 | Wykonawca musi zapewnić, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca. |
| POS7-DOSSPRZ-15 | Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz |
| POS7-DOSSPRZ-16 | Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, z załączonymi kartami gwarancyjnymi i instrukcjami obsługi w języku polskim (przy czym Zamawiający wymaga, aby urządzenia były rozpakowane i uruchomione wyłącznie przez Wykonawcę, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu). |
| POS7-DOSSPRZ-17 | Wykonawca dostarczy wszystkie licencje i klucze licencyjne wymagane do działania dostarczanych urządzeń i Oprogramowania Gotowego. |
| POS7-DOSSPRZ-18 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania Gotowego. |
| POS7-DOSSPRZ-19 | W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego. |

## Projekt techniczny ITS dla Środowisk Produkcyjnych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-PROITS-01 | Wykonawca opracuje Projekt Techniczny ITS środowisk produkcyjnych umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt będzie oparty o komponenty dostarczone w ramach niniejszego postępowania. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. Zamawiajacy przekaże Wykonawcy wytyczne w zakresie konfiguracji poszczególnych elementów oparte na produkcie typu dokument realizowanym w ramach umowy POS-4. |
| POS7-PROITS-02 | Wykonawca opracuje projekt rozmieszczenia szaf „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń.  Zamawiający dostarczy dokumentację projektową, będącą w jego posiadaniu i istotną dla opracowania Projektu Technicznego ITS, w terminie 3 dni roboczych od dnia podpisania umowy. |
| POS7-PROITS-03 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| POS7-PROITS-04 | Projekt Techniczny ITS środowisk produkcyjnych musi zawierać minimum:   1. Wykaz wykorzystanego sprzętu i licencji oprogramowania, 2. Przyjęte nazewnictwo elementów infrastruktury, 3. Plan ustawienia szaf w pomieszczeniach serwerowni, 4. Plan rozmieszczenia sprzętu w szafach, 5. Wymagania dotyczące zasilania i klimatyzacji oraz wagi poszczególnych szaf rack, 6. Projekt zarządzania infrastrukturą dostarczaną w ramach postępowania z wykorzystaniem dostarczanego oprogramowania do zarządzania i monitorowania. 7. Projekt bezpieczeństwa warstwy logicznej ITS. 8. Projekt konfiguracji infrastruktury sieci LAN. 9. Projekt konfiguracji sieci SAN. 10. Projekt konfiguracji urządzeń bezpieczeństwa. 11. Projekt konfiguracji urządzeń ADC. 12. Projekt konfiguracji serwerów zarządzania. 13. Projekt systemu ochrony antywirusowej. 14. Projekt systemu ochrony poczty elektronicznej. 15. Projekt konfiguracji urządzenia SIEM. |
| POS7-PROITS-05 | Wykonawca opracuje Projekt Techniczny ITS środowisk produkcyjnych ZOPD. |
| POS7-PROITS-06 | Wykonawca opracuje projekt techniczny połączenia POPD-ZOPD umożliwiającego pracę obu ośrodków w trybie Active-Active. W ramach opracowanego dokumentu Wykonawca określi zalecenia konfiguracyjne dla operatorów sieci teletransmisyjnych wykorzystywanych przez Zamawiającego (WAN-PROK oraz Internet) oraz określi ewentualne zasoby niezbędne do wdrożenia proponowanych zmian. |

## Projekt techniczny ITS Środowisk Nieprodukcyjnych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-PROITS-17 | Wykonawca opracuje Projekt Techniczny ITS środowisk nieprodukcyjnych umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. Zamawiajacy przekaże Wykonawcy wytyczne w zakresie konfiguracji poszczególnych elementów oparte na produkcie typu dokument realizowanym w ramach umowy POS-4. |
| POS7-PROITS-18 | Wykonawca opracuje projekt rozmieszczenia szaf „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń.  Zamawiający dostarczy dokumentację projektową, będącą w jego posiadaniu i istotną dla opracowania projektu technicznego montażu i instalacji ITS, w terminie 3 dni roboczych od dnia podpisania umowy. |
| POS7-PROITS-19 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| POS7-PROITS-20 | Projekt Techniczny ITS środowisk nieprodukcyjnych musi zawierać minimum wszystkie elementy analogicznie jak dla wymagania POS7-PROITS-04. Jednocześnie Projekt Techniczny ITS środowisk nieprodukcyjnych musi uwzględniać konieczność uruchowmienia:   1. Środowiska Testów Wstępnych 2. Środowiska Testów Akceptacyjnych 3. Środowiska Szkoleniowego 4. Platformy e-Learningu 5. Środowiska Projektowego 6. Repozytorium Kodów Źródłowych i Środowisk Kompilacji 7. Środowisko Zarządzania Testami |

## Opracowanie Scenariuszy Testów (Dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-TEST-01 | Wykonawca opracuje scenariusze testowe umożliwiające weryfikację spełnienia wymagań, poprawność instalacji i konfiguracji wszystkich komponentów ITS. |
| POS7-TEST-02 | Weryfikacja spełnienia każdego z wymagań będzie przeprowadzana na podstawie wyników Testów Akceptacyjnych |
| POS7-TEST-03 | Zamawiający wymaga, aby dla przeprowadzenia testów zostały przygotowane i przedstawione do akceptacji scenariusze testowe obejmujące wszystkie dostarczane elementy ITS a w szczególności:   1. Elementy infrastruktury serwerowej, 2. Elementy podsystemu dyskowego w tym macierzy obiektowych i deduplikatorów, 3. Elementy dostarczanych urządzeń typu appliance, 4. Testy /ilościowe/ oprogramowania gotowego. |
| POS7-TEST-04 | Testy funkcjonalne sprzętu i oprogramowania powinny obejmować:   1. sprawdzeniu poprawności funkcjonowania Sprzętu poprzez wykonanie testów fabrycznych (producenta) każdego dostarczonego Sprzętu; 2. sprawdzeniu logów w urządzeniach (stwierdzeniu braku błędów w logach); 3. wykonaniu testów sprawdzających poprawność działania poprzez zasymulowanie uszkodzenia dowolnego rodzaju redundantnego elementu w dowolnym urządzeniu oraz zasymulowanie uszkodzenia zasilania zewnętrznego. |
| POS7-TEST-05 | Scenariusze testów muszą być tak przygotowane, aby testy wg scenariuszy mogły być wykonane przez osoby spoza zespołu Wykonawcy. |
| POS7-TEST-06 | Scenariusze testów muszą uwzględniać przeprowadzenie testów wymagań funkcjonalnych i pozafunkcjonalnych wraz z przeprowadzeniem testów procedur eksploatacyjnych. |
| POS7-TEST-07 | Scenariusz testowy musi zawierać:   1. Numer scenariusza – umożliwiający jego łatwą i bezbłędną identyfikację. 2. Wskazanie testowanego zakresu oraz odniesienia do dokumentacji systemu, w szczególności listę weryfikowanych wymagań Zamawiającego oraz realizowanego przypadku użycia. 3. Warunki wejściowe – lista warunków, jakie muszą być spełnione, aby można było rozpocząć wykonanie scenariusza. 4. Wskazanie potrzebnego zakresu danych testowych. 5. Zestaw przypadków testowych składających się na scenariusz. Każdy przypadek testowy musi:    1. zawierać opis działań osoby realizującej przypadek testowy w postaci kolejnych kroków, ze wskazaniem danych, których należy użyć. Opis powinien być wyrażony w sposób prosty, przystępny dla osoby w ograniczonym stopniu zapoznanej z systemem,    2. umożliwiać realizację scenariusza testowego w krótkim czasie, bez konieczności zapoznawania się z dokumentacją Systemu,    3. przedstawiać oczekiwany wynik wykonania – opis pozwalający na jednoznaczną ocenę, czy przypadek testowy zakończył się sukcesem lub czy błędem,    4. jeżeli dla sprawdzenia wyniku przypadku testowego konieczne jest wykonanie pewnej sekwencji działań, to musi być ona również opisana w postaci kolejnych kroków, 6. Klasę błędu, którą należy zgłosić w przypadku wystąpienia błędu (gdy wykonanie przypadku testowego zakończy się niepowodzeniem). |
| POS7-TEST-08 | Każdy scenariusz musi cechować:   1. Prostota opisu – scenariusz powinien być opisany w sposób prosty, zrozumiały dla osoby nie znającej systemu lub zapoznanej z nim w ograniczony sposób, 2. Powtarzalność – powinno być możliwe wielokrotne wykonanie scenariusza w identyczny sposób na podstawie jego opisu, 3. Jednoznaczność – scenariusz przy spełnieniu wymagań wejściowych oraz +realizacji wg opisu przypadków testowych powinien mieć ten sam przebieg oraz identyczny wynik (z dokładnością do istotnych elementów) przy powtórzeniach realizacji scenariusza na tej samej wersji systemu, 4. Możliwość automatyzacji – w przypadku scenariuszy, w których automatyzacja jest możliwa |
| POS7-TEST-09 | Za kompletność i spójność scenariuszy testowych w ramach Testów ITS odpowiada Wykonawca. |

## Montaż sprzętu, instalacja oprogramowania (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-MONTS-01 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty ITS w POPD i TOPD zgodnie z opracowanymi Projektami Technicznymi ITS. |
| POS7-MONTS-02 | Wykonawca dostarczy licencje oprogramowania gotowego, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację systemu w POPD. |
| POS7-MONTS-03 | Wykonawca zainstaluje dostarczane urządzenia w istniejących 3 szafach rack w pomieszczeniach POPD wskazanych przez Zamawiającego dla środowiska produkcyjnego i środowisk nieprodukcyjnych zgodnie z opracowanymi Projektami Technicznymi ITS. |
| POS7-MONTS-04 | **Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, kable Ethernet kat. 6e, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń dostarczanych w ramach przedmiotowego postępowania zgodnie z opracowanymi Projektami Technicznymi ITS. Wykonawca musi uwzględnić konieczność podłączenia wszystkich interfejsów urządzeń określonych w OPZ.** |
| POS7- MONTS-05 | Wykonawca wykona pasywne połączenia pomiędzy dostarczanymi szafami rack w serwerowni Zamawiajacego, w której będą montowane dostarczane urządzenia oraz istniejącymi szafami okablowania strukturalnego budynku i szafami rack będącymi przedmiotem dostawy w ramach postępowania POS-6 (6 sztuk).  Strefa wewnętrzna:  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy dostarczaną szafą rack a szafami przeznaczonymi do montażu urządzeń serwerowych (4 sztuki szaf rack dostarczanych w ramach POS-6).  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy dostarczaną szafą rack a istniejącą szafą IDF w pomieszczeniu serwerowni.  Połączenie za pomocą kabli UTP/STP zakończonych panelami RJ45 pomiędzy dostarczaną szafą rack a szafami przeznaczonymi do montażu urządzeń serwerowych (4 sztuki szaf rack dostarczanych w ramach POS-6).  Strefa zewnętrzna:  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy dostarczaną szafą rack a szafami przeznaczonymi do montażu urządzeń serwerowych (1 sztuka szafy rack dostarczana w ramach POS-6).  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy dostarczaną szafą rack a istniejącą szafą IDF w pomieszczeniu serwerowni.  Połączenie za pomocą kabli UTP/STP zakończonych panelami RJ45 pomiędzy dostarczaną szafą rack a szafami przeznaczonymi do montażu urządzeń serwerowych (1 sztuka szafy rack dostarczana w ramach POS-6).  Środowisko nieprodukcyjne:  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy szafą telekomunikacyjną strefy zewnętrznej (dostarczona w ramch POS-6) a szafą przeznaczoną do montażu urządzeń serwerowych (dostarczane w ramach POS-6).  Połącznie za pomocą kabli światłowodowych min. 48j MM zakończonych na panelach pomiędzy dostarczaną szafą rack a istniejącą szafą IDF w pomieszczeniu serwerowni.  Połączenie za pomocą kabli UTP/STP zakończonych panelami RJ45 pomiędzy dostarczaną szafą rack a szafami przeznaczonymi do montażu urządzeń serwerowych (1 sztuka szafy rack dostarczana w ramach POS-6).  W przypadku zwiększenia ilości szaf lub zmiany rozmieszczenia sprzętu odpowiednie połączenia pasywne pomiędzy szafami zostaną ustalone na etapie Projektu Technicznego. |
| POS7- MONTS-06 | Wykonawca oznaczy każdy kabel w sposób umożliwiający jego jednoznaczną identyfikację zgodnie z przyjętą konwencją nazewniczą. |
| POS7-MONTS-07 | Wykonawca dokona montażu całości sprzętu w szafach RACK w pomieszczeniach POPD wskazanych przez Zamawiającego zgodnie z opracowanymi Projektami Technicznymi ITS. |
| POS7-MONTS-08 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję. |
| POS7-MONTS-09 | Wykonawca wykona odpowiednie przyłącza elektryczne od rozdzielni elektrycznych w budynku do paneli PDU w szafach rack. Każde urządzenie posiadające redundantne zasilacze zostanie podłączone do dwóch niezależnych torów zasilania elektrycznego. W każdej szafie rack pozostanie wolnych co najmniej 5 gniazd elektrycznych z każdego toru zasilania. |
| POS7-MONTS-10 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania. |
| POS7-MONTS-11 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. |
| POS7-MONTS-12 | Wykonawca dla dostarczanych szaf rack dostarczy moduły wentylacyjne podłogi technicznej posiadające regulację kąta nawiewu. Moduł wentylacyjny zostanie zainstalowany przy każdej z szaf rack zgodnie z kierunkiem przepływu powietrza przez urządzenia. |
| POS7-MONTS-13 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware, BIOS) wszystkich urządzeń ITS do najnowszych stabilnych wersji. |
| POS7-MONTS-14 | Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego. Wykonawca dostarczy na płytach CD/DVD komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe i fabryczne. |

## Konfiguracja środowisk zgodnie z projektami technicznymI (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-PRACE-01 | Wykonawca przeprowadzi proces aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowszych dostępnych stabilnych wersji oprogramowania. |
| POS7-PRACE-02 | Wykonawca zainstaluje i skonfiguruje wszystkie dostarczane urządzenia i oprogramowanie zgodnie z opracowanymi Projektami Technicznymi ITS środowiska produkcyjnego oraz środowiska nieprodukcyjnego. |

## Przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-TESTY-01 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| POS7-TESTY-02 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| POS7-TESTY-03 | Testami zostanie objęta cała dostarczona Infrastruktura Techniczno- Systemowa dla środowiska POPD i TOPD. |
| POS7-TESTY-04 | Wykonawca przeprowadzi testy sprawdzające niezawodność ITS na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego. |
| POS7-TESTY-05 | Testy ITS będą wykonane przez Zamawiającego w asyście Wykonawcy, zgodnie z zaakceptowanym przez Zamawiającego Planem Testów i Scenariuszami Testów. |
| POS7-TESTY-06 | Wykonawca przed przeprowadzeniem testów przeprowadzi instruktaż dla testerów Zamawiającego. |
| POS7-TESTY-07 | Testy funkcjonalne weryfikujące poszczególne elementy sprzętowe oraz programowe powinny obejmować co najmniej:   1. sprawdzeniu poprawności funkcjonowania Sprzętu poprzez wykonanie testów fabrycznych (producenta) każdego dostarczonego Sprzętu, 2. sprawdzeniu logów w urządzeniach (stwierdzeniu braku błędów w logach), 3. wykonaniu testów sprawdzających poprawność działania poprzez zasymulowanie uszkodzenia dowolnego rodzaju redundantnego elementu w dowolnym urządzeniu oraz zasymulowanie uszkodzenia zasilania zewnętrznego. |

## Opracowanie dokumentacji powykonawczej (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-DOKPOW-01 | Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów ITS dla POPD i TOPD. |
| POS7-DOKPOW-02 | Dokumentacja powykonawcza ITS będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| POS7-DOKPOW-03 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016 lub wyżej, pliki Visio zawierające rysunki techniczne lub inne uzgodnione z Zamawiajacym) a także w wersji Portable Document Format (zgodny z ISO 32000-1:2008). Na żądanie Zamawiającego lub jeśli wynika to z Umowy Wykonawca dostarczy dokument w wersji drukowanej (wydruk kolorowy) i/lub w wersji stanowiącej skan Dokumentu. |
| POS7-DOKPOW-04 | Wykonawca opracuje „Dokumentację administratora”. |
| POS7-DOKPOW-05 | Dokumentacja administratora powinna zawierać co najmniej:   1. Procedury administracyjne 2. Procedury instalacji i konfiguracji 3. Procedury bieżących działań administracyjnych 4. Procedury okresowych/planowanych działań administracyjnych 5. Procedury aktualizacji standardowych elementów dostarczonego sprzętu 6. Procedury włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych. |
| POS7-DOKPOW-06 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą |
| POS7-DOKPOW-07 | Projekt Techniczny ITS powinien zostać zaktualizowany do postaci dokumentacji powykonawczej w chwili przekazywania infrastruktury Zamawiającemu do akceptacji. |

## Opracowanie procedur utrzymania ITS (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-PROCUT-01 | Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonych komponentów ITS warstwy fizycznej i logicznej.  Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania typu firmware. Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu monitorowania i utrzymania dostarczonych komponentów ITS w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów. |
| POS7-PROCUT-02 | Procedury zostaną przetestowane przez Zamawiającego przy udziale inżyniera Wykonawcy. Procedury będą na bieżąco poprawiane przez Wykonawcę w ramach wdrożenia ITS będącego przedmiotem zamówienia. |

## Przygotowanie materiałów szkoleniowych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-MATSZK-01 | Wykonawca opracuje materiały szkoleniowe dla wdrożonych komponentów ITS, dla których nie będą oferowane szkolenia autoryzowane.  Jako materiał szkoleniowy rozumie się opis zbioru czynności mających na celu zrealizowane określonego zadania np. wykonanie aktualizacji oprogramowania typu firmware. |

## Szkolenia (Usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-SZKOL-01 | Wykonawca zapewni szkolenia i warsztaty z dostarczanych produktów infrastruktury techniczno-systemowej. Przewidywana ilość uczestników warsztatów to maksymalnie 10 osób wskazanych przez Zamawiającego. |
| POS7-SZKOL-02 | Wykonawca opracuje plan warsztatów / szkoleń z zakresu wdrażanej Infrastruktury Techniczno-Systemowej. Warsztaty z zakresu każdego z typów urządzeń dostarczanych w ramach przedmiotowego postępowania powinny trwać przynajmniej 1 dzień roboczy i uwzględniać uwarunkowania montażu i instalacji sprzętu w infrastrukturze Zamawiającego. |
| POS7-SZKOL-03 | Warsztaty odbędą się w siedzibie Zamawiającego. Warsztaty będą prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań. |
| POS7-SZKOL-04 | Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 10 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. |
| POS7-SZKOL-05 | Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy szkoleń i warsztatów. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia. |
| POS7-SZKOL-06 | Program szkoleń i warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów. Zamawiający zastrzega sobie prawo do korekty programu szkoleń / warsztatów w uzgodnionym zakresie. |
| POS7-SZKOL-07 | Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru warsztatu wraz z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem warsztatu. |
| POS7-SZKOL-08 | Szkolenia muszą być autoryzowane przez producenta produktu, którego dotyczą. Szkolenia muszą być prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne i doświadczenie dydaktyczne do prowadzenia szkoleń. |
| POS7-SZKOL-09 | Szkolenia muszą być przeprowadzone w ośrodku szkoleniowym na terenie Warszawy. |
| POS7-SZKOL-10 | Każdy uczestnik szkolenia otrzyma certyfikat jego ukończenia. |
| POS7-SZKOL-11 | Szkolenia zostaną zrealizowane w postaci voucher-ów na autoryzowane szkolenia z zakresu wdrażanych rozwiązań sprzętowych. Vouchery będą ważne co najmniej 18 miesięcy od dnia podpisania Protokołu Odbioru Końcowego. |
| POS7-SZKOL-12 | Wykonawca dostarczy vouchery na szkolenia:   1. Voucher z zakresu dostarczanych przełączników LAN – 4 sztuki 2. Voucher z zakresu dostarczanych urządzeń typu firewall - 4 sztuki 3. Voucher z zakresu dostarczanych urządzeń równoważenia obciążenia ruchem - 4 sztuki 4. Voucher z zakresu dostarczanych przełączników SAN - 4 sztuki 5. Voucher z zakresu modułu ochrony przed malwarem – 4 sztuki 6. Voucher z zakresu modułu ochrony poczty elektronicznej – 4 sztuki 7. Voucher z zakresu modułu zdalnego dostępu VPN – 4 sztuki 8. Voucher z zakresu modułu ochrony aplikacyjnej –WAF – 4 sztuki 9. Voucher z zakresu obsługi systemu klasy SIEM – 6 sztuk 10. Voucher z zakresu rozwiązania do zarządzania elementami bezpieczeństwa – 4 szt 11. Voucher z zakresu rozwiązania do zarządzania elementami infrastruktury sieciowej – 4 sztuki 12. Voucher z zakresu obsługi oprogramowania do zarządzania podatnościami - 4 sztuki |
| POS7-SZKOL-13 | Szkolenia muszą obejmować zagadnienia umożliwiające średniozaawansowane administrowanie oraz bieżące utrzymanie wdrożonych rozwiązań. |
| POS7-SZKOL-14 | W przypadku zaprzestania przez dany ośrodek szkoleniowy prowadzenia szkoleń z danego tematu musi istnieć możliwość zamiany vouchera na szkolenie równoważne. |
| POS7-SZKOL-15 | W ramach warsztatów i szkoleń uczestnicy otrzymają komplet materiałów szkoleniowych w wersji papierowej oraz elektronicznej obejmujących swoim zakresem całe szkolenie. Wszystkie materiały szkoleniowe muszą być w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych |
| POS7-SZKOL-16 | Wykonawca dostarczy wszystkie materiały pomocnicze niezbędne do przeprowadzenia warsztatów i szkoleń, jak np. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć. |
| POS7-SZKOL-17 | Szkolenia powinny odbywać się w formie wykładów i warsztatów praktycznych w proporcji obejmującej co najmniej 75 % warsztatów. |
| POS7-SZKOL-18 | Szkolenia i warsztaty odbywać się będą w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie. Cykl szkolenia nie może być dzielony między tygodniami |
| POS7-SZKOL-19 | Wykonawca zapewni ciepły posiłek, w formie zestawu obiadowego (zupa, drugie danie, napój), dla każdego uczestnika szkolenia, we wszystkie dni szkolenia, podczas przerwy obiadowej. |

## Serwis gwarancyjny, wsparcie eksploatacji

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| POS7-GWAR-SER-01 | Wykonawca udzieli 36-miesięcznej gwarancji na wszystkie elementy systemu (urządzenia i oprogramowanie), dostarczone przez Wykonawcę w ramach niniejszego zamówienia. Okres gwarancji liczony będzie od dnia podpisania Protokołu odbioru w zakresie dostawy urządzeń i oprogramowania. |
| POS7-GWAR-SER-02 | Zamawiający wymaga, aby na całość dostarczanego rozwiązania oraz oprogramowania Wykonawca zaoferował 36 miesięczne wsparcie techniczne. |
| POS7-GWAR-SER-03 | Zgłoszenia awarii następować będzie w trybie 24/7/365 i musi być dokonywane w postaci: zgłoszenia telefonicznego, z wykorzystaniem serwisu www lub za pomocą poczty elektronicznej, wszystkie wymienione kanały komunikacji muszą być świadczone w języku polskim. |
| POS7-GWAR-SER-04 | Wykonawca zobowiązany jest zapewnić wsparcie techniczne dla dostarczanego sprzętu w okresie obowiązywania gwarancji. Wsparcie musi być dostępne w języku polskim poprzez konsultacje w miejscu zainstalowania sprzętu (w lokalizacji Zamawiającego), e-mail oraz połączenia telefoniczne.  Wsparcie techniczne musi obejmować:   1. zdalne wsparcie techniczne (możliwość zgłaszania problemów w trybie 24x7), 2. wsparcie w miejscu instalacji (w trybie 24x7) 3. pozostawienie uszkodzonych dysków u Zamawiającego, 4. części zamienne oraz ich instalację, 5. uaktualnienia oraz instalację oprogramowania firmware nie rzadziej niż raz na 180 dni, jeżeli takie uaktualnienia są rekomendowane przez Producenta sprzętu i oprogramowania 6. dostęp do internetowych narzędzi serwisowych. |
| POS7-GWAR-SER-05 | Wykonawca odpowiada za szkody powstałe po stronie Zamawiającego lub odbiorców usług z przyczyn leżących po stronie Wykonawcy, w szczególności Wykonawca odpowiada za wszelkie szkody powstałe z powodu niewykonania lub nienależytego wykonania przedmiotu Umowy |
| POS7-GWAR-SER-06 | Wykonawca jest zobowiązany do niezwłocznego potwierdzenia przyjęcia zgłoszenia na adres poczty elektronicznej: ………@pk.gov.pl, podany przez Zamawiającego lub telefonicznie - na numer podany podczas rejestracji zgłoszenia (czas reakcji). W przypadku braku potwierdzenia po upływie 4 godzin od zgłoszenia awarii przez Zamawiającego, Zamawiający wdroży procedurę eskalacji zgłoszenia |
| POS7-GWAR-SER-07 | Zgłoszenia awarii będą realizowane w następujący sposób:   1. zgłoszenie o priorytecie wysokim – czas reakcji do 1 godziny, czas przywrócenia funkcjonalności systemu do 7 godzin, przy czym zgłoszenie o priorytecie wysokim to nieprawidłowe działanie urządzeń lub oprogramowania, powodujące albo całkowity brak możliwości korzystania z urządzeń lub oprogramowania albo takie ograniczenie możliwości korzystania z urządzeń lub oprogramowania, że przestają one spełniać swoje podstawowe funkcje. Zgłoszenie o priorytecie wysokim dotyczy w szczególności sytuacji, gdy oprogramowanie jest niedostępne i nie ma możliwości samodzielnego rozwiązania problemu, brak możliwości zalogowania użytkownika, niedostępność krytycznych funkcji urządzeń lub oprogramowania; 2. zgłoszenie o priorytecie średnim – czas reakcji do 4 godzin, czas przywrócenia funkcjonalności systemu do 12 godzin, przy czym zgłoszenie o priorytecie średnim to nieprawidłowe działanie urządzeń lub oprogramowania powodujące ograniczenie korzystania z urządzeń lub oprogramowania przy zachowaniu ich podstawowych funkcji. Podstawowe funkcje oprogramowania działają, ale występują problemy z wydajnością lub pojawiają się błędy mające wpływ na pracę urządzeń lub oprogramowania. Zgłoszenie o priorytecie średnim dotyczy w szczególności ograniczenie działania ważnych elementów oprogramowania, które nie powodują wyłączenia systemu, ale są niedostępne i nie ma możliwości samodzielnego rozwiązania problemu, zmniejszonej wydajności utrudniającej pracę użytkownikom 3. zgłoszenie o priorytecie niskim – czas reakcji w następnym dniu roboczym, czas przywrócenia funkcjonalności systemu do 36 godzin, przy czym zgłoszenie o priorytecie niskim dotyczy rutynowych problemów technicznych, pozyskiwania informacji na temat kompatybilności urządzeń lub oprogramowania, nawigacji w systemie, instalacji i konfiguracji oprogramowania. Zgłoszenie o niskim priorytecie dotyczy w szczególności sytuacji: braku dostępności części środowiska dla niewielkiej liczby użytkowników, zmniejszonej wydajności utrudniającej pracę niewielkiej liczbie użytkowników |
| POS7-GWAR-SER-08 | Na potrzeby niniejszego przedmiotu zamówienia Strony przyjmują, iż dni robocze to dni tygodnia od poniedziałku do piątku od godz. 7:00 do godz. 17:00 z wyłączeniem dni ustawowo wolnych od pracy oraz innych dni wolnych u Zamawiającego. Wykonawca zobowiązany jest do realizowania czasów reakcji i napraw w godzinach roboczych Zamawiającego. |
| POS7-GWAR-SER-09 | Jeżeli dochowanie określonego czasu usunięcia awarii, o którym mowa w wymaganiu POS7-GWAR-SER-07 nie jest możliwe, Zamawiający może, w formie pisemnej lub e-mail, wyrazić zgodę na jego przedłużenie. W takim wypadku Zamawiający może żądać dostarczenia przez Wykonawcę sprzętu zastępczego |
| POS7-GWAR-SER-10 | Zamawiający musi mieć możliwość bezpośredniego zgłaszania awarii do producenta sprzętu (w języku polskim) oraz samodzielnej aktualizacji oprogramowania (szczegółowa instrukcja instalacji/aktualizacji zostanie dostarczona najpóźniej w dniu podpisania Protokołu odbioru). W okresie obowiązywania umowy samodzielna aktualizacja oprogramowania będzie realizowana każdorazowo po uzgodnieniu z Wykonawcą |
| POS7-GWAR-SER-11 | W okresie obowiązywania serwisu gwarancyjnego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Uszkodzone dyski podlegające gwarancji stanowią własność Zamawiającego i pozostają u Zamawiającego, nie podlegają zwrotowi w ramach usługi gwarancyjnej |
| POS7-GWAR-SER-12 | Usługi gwarancyjne muszą być realizowane przez autoryzowany serwis producenta albo przez Wykonawcę na terenie Polski dla każdego urządzenia i oprogramowania na warunkach określonych w Opisie przedmiotu Zamówienia |
| POS7-GWAR-SER-13 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającego do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| POS7-GWAR-SER-14 | **Wykonawca zapewni asystę techniczną, zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera w okresie 36 miesięcy, licząc od dnia podpisania Protokołu odbioru, w wymiarze do 1500 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny).** |
| POS7-GWAR-SER-15 | Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym wsparciem technicznym w ramach udzielonej gwarancji. |
| POS7-GWAR-SER-16 | Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności rozwoju i modyfikacji wdrożonych rozwiązań, wsparciu w zakresie utrzymania. |
| POS7-GWAR-SER-17 | W ramach godzin wsparcia inżynier na wezwanie Zamawiającego ma obowiązek przybyć do siedziby Zamawiającego na terenie Warszawy i tam realizować zgłoszenie. |
| POS7-GWAR-SER-13 | Świadczenie usługi wsparcia technicznego inżyniera (asysty technicznej) jest jednostronnym uprawnieniem Zamawiającego. Nie skorzystanie przez Zamawiającego z tej usługi lub niewykorzystanie wszystkich przewidzianych w Umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń w stosunku do Zamawiającego. |

## Specyfikacja dostarczanego Sprzętu i Oprogramowania Gotowego

## Infrastruktura sieci LAN i SAN

## WYMAGANIA OGÓLNE DLA WSZYSTKICH DOSTARCZANYCH ROZWIĄZAŃ

Tabela 1. Wymagania ogólne dla dostarczanych rozwiązań

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| ***Uwagi ogólne:*** |  |
| POS7-WYMOG-01 | Wszystkie dostarczane rozwiązania muszą umożliwiać współpracę z dostarczanym systemem typu SIEM przez eksport informacji o zdarzeniach, co najmniej za pośrednictwem Syslog, SNMP lub do pliku tekstowego lub XML na współdzielonym zasobie sieciowym. Eksportowane zdarzenia muszą być porawnie przewarzane przez dostarczane rozwiązanie typu SIEM. |
| POS7-WYMOG-02 | Wszystkie systemy muszą zapewniać separację fizyczną urządzeń użytych do budowy stref zewnętrznej i wewnętrznej systemu oraz obszarów w ramach stref. Dopuszczalne jest zastosowanie wspólnych elementów zarządczych (kontrolery, systemy zarządzania, agregacji logów itp.) per strefa (wspólnych dla wszystkich obszarów danej strefy), przy czym każdy system umożliwiający zmianę konfiguracji elementów musi zapewniać możliwość separacji uprawnień administracyjnych, konfiguracji, polityk itp. |
| POS7-WYMOG-03 | Na potrzeby separacji segmentów w ramach strefy wymagane jest wykorzystanie segmentacji logicznej przy zapewnienia przez poszczególne rozwiązania implementujące usługi bezpieczeństwa (NGFW, NGIPS, SSL, WAF, LB, aDDoS) mechanizmów umożliwiających wpływ przeciążenia lub kompromitacji poszczególnych instancji na działanie innych (alokacja zasobów sprzętowych per instancja lub ograniczenie możliwych do wykorzystania zasobów per instancja). |
| POS7-WYMOG-04 | Wszystkie dostarczane rozwiązania muszą zapewniać możliwość wykreowania dedykowanego interfejsu zarządzającego w formie fizycznej lub wirtualnej. Interfejs nie może być wykorzystywany do transmisji ruchu produkcyjnego. |
| POS7-WYMOG-05 | Wszystkie systemy stref produkcyjnych muszą być zrealizowane w sposób zapewniający brak pojedynczego punktu awarii – jako klastry niezawodnościowe. Awaria jakiegokolwiek elementu nie może ograniczać wydajności systemu poniżej określonych w dokumencie wartości minimalnych |
| POS7-WYMOG-06 | Wszystkie dostarczane urządzenia sieciowe (przełączniki, firewalle, platformy NG, ochrony poczty elektronicznej itp.) muszą zapewniać możliwość zarządzania lokalnego i zdalnego:   * 1. linię poleceń (CLI) – dostępną lokalnie przez interfejs szeregowy i zdalnie przez SSHv2   2. graficzny interfejs użytkownika (GUI) dostępny przez standardową przeglądarkę z ochroną kryptograficzną (HTTPS)   3. SNMP v2/v3   4. dostęp do interfejsów administracyjnych musi być możliwy z wykorzystaniem zewnętrznych serwerów autoryzacyjnych (RADIUS lub LDAP) z obsługą zarządzania w oparciu o role (RBAC)   5. możliwość synchronizacji czasu za pomocą protokołu NTP lub SNTP |
| POS7-WYMOG-07 | Wszystkie dostarczane systemy aplikacyjne muszą zapewniać możliwość zarządzania lokalnego i zdalnego:   * 1. graficzny interfejs użytkownika (GUI) dostępny przez standardową przeglądarkę z ochroną kryptograficzną (HTTPS)   2. dostęp do interfejsów administracyjnych musi być możliwy z wykorzystaniem zewnętrznych serwerów autoryzacyjnych (RADIUS lub LDAP) z obsługą zarządzania w oparciu o role (RBAC)   3. możliwość synchronizacji czasu za pomocą protokołu NTP lub SNTP |
| POS7-WYMOG-08 | Wszystkie systemy, o ile wymagania szczegółowe nie określają inaczej, muszą mieć możliwość pracy w obrębie centrum przetwarzania danych – w takim trybie nie jest dopuszczalne odwoływanie się poszczególnych elementów do systemów zewnętrznych, w szczególności umieszczonych w sieci publicznej (chmurze). Wszelkie aktualizacje oprogramowania, baz danych systemów itp. muszą być realizowane poprzez manualne dostarczenie odpowiednich repozytoriów przez administratorów systemu. |
| POS7-WYMOG-09 | Dopuszczalna jest realizacja poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:   * 1. połączenie urządzeń będzie zrealizowane w sposób nieograniczający wydajności zespołu (wydajność poszczególnych elementów nie może być niższa niż wymagana wydajność dla danej grupy funkcjonalnej, połączenie między urządzeniami będzie zrealizowane w sposób redundantny i umożliwiający osiągnięcie wymaganych wydajności), w szczególności przepustowość interfejsów musi zapewniać pasmo umożliwiające bezkolizyjną obsługę wszystkich grup funkcjonalnych   2. dostarczone zostaną wszystkie elementy konieczne do połączenia zespołu   3. wszystkie elementy zestawu będą spełniały wymagania dotyczące zarządzania danej grupy funkcjonalnej,   4. do oferty zostanie dołączony szczegółowy opis zespołu, obejmujący schematy połączeń, określenie które elementy zestawu odpowiadają za poszczególne funkcjonalności itp.   W przypadku oferowania zespołu urządzeń realizujących określoną grupę funkcjonalną należy w formularzu ofertowym w sekcji dla danej grupy wpisać nazwy wszystkich producentów i wszystkich elementów wykorzystanych do zbudowania zespołu. |
| POS7-WYMOG-10 | Wykonawca dostarczy wszystkie elementy niezbędne do funkcjonowania rozwiązania, w tym dodatkowe urządzenia, oprogramowanie, akcesoria niezbędne do prawidłowego, redundantnego połączenia wszystkich elementów, w tym kable, wkładki optyczne, patchpanele itp.  Dodatkowe elementy muszą być ujęte w odpowiednich pozycjach formularza ofertowego. |
| POS7-WYMOG-11 | W przypadku oferowania urządzeń umożliwiających wybór sposobu przepływu powietrza wymagane jest uwzględnienie przepływu typu „front-to-back”. |

## Przełączniki SAN TYP I – 7 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 2. Wymagania dla przełączników SAN TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SAN-01** | **Wymagania funkcjonalne** |
| POS7-SAN-01.01 | Przełączniki FibreChannel obsługujące technoogię 32 Gb/s i zapewniające możliwość pracy portów z prędkościami 32, 16, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP lub QSFP. |
| POS7-SAN-01.02 | Wszystkie porty przełącznika FC muszą umożliwiać działanie bez tzw. nadsubskrypcji (wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika muszą umożliwiać pracę równocześnie z pełną prędkością 32Gb/s) |
| POS7-SAN-01.03 | Obsługa portów co najmniej E oraz F. |
| POS7-SAN-01.04 | Możliwość standardowego przydziału minimum 500 kredytów (FC buffer credits) |
| POS7-SAN-01.05 | Możliwość zwiększenia liczby kredytów (FC buffer credits) do co najmniej 8.000 dla co najmniej czterech portów przełącznika. |
| POS7-SAN-01.06 | Podział sieci SAN na wirtualne fabryki SAN (logiczne przełączniki SAN) – obsługa co najmniej 8 wirtualnych fabryk |
| POS7-SAN-01.07 | Łączenie fabryk SAN poprzez routowanie (routing FC-FC) |
| POS7-SAN-01.08 | Obsługa agregacji nie mniej niż 8 portów fizycznych FC 32G w jedno połączenie logiczne („trunk”, „channel“) – możliwość włączenia w skład zagregowanego połączenia logicznego dowolnego aktywnego portu przełącznika |
| POS7-SAN-01.09 | Jednoczesna obsługa mechanizmów agregowanego połączenia logicznego („trunk”, „channel”) oraz podziału ruchu w oparciu o parametry DID/SID/OXID. |
| POS7-SAN-01.10 | Wykrywanie i eliminacja ramek FC z błędnym kodem CRC na portach we/wy lub obsługa mechanizmu FEC (Forward Error Correction) w celu uniknięcia przesyłania błędnych ramek. |
| POS7-SAN-01.11 | Możliwość aktualizacji oprogramowania bez przerwy w działaniu urządzenia (tzw. nondisruptive software upgrades). |
| POS7-SAN-01.12 | Wsparcie dla mechanizmów gwarancji jakości usług (QoS). |
| **POS7-SAN-02** | **Obsługa mechanizmów FibreChannel:** |
| POS7-SAN-02.01 | sprzętowo implementowany zoning |
| POS7-SAN-02.02 | tryb NPV (N-Port Virtualization) |
| POS7-SAN-02.03 | funkcjonalność N-Port ID Virtualization (NPIV) dla każdego portu, |
| POS7-SAN-02.04 | obsluga NVMe over Fabric |
| **POS7-SAN-03** | **Obsługa mechanizmów zarządzania:** |
| POS7-SAN-03.01 | transfer plików za pomocą SFTP, |
| POS7-SAN-03.02 | standard zarządzający SMI-S. |
| **POS7-SAN-04** | **Obsługa mechanizmów bezpieczeństwa:** |
| POS7-SAN-04.01 | autoryzacja dostępu administracyjnego do przełącznika za pomocą RADIUS i/lub TACACS+, LDAP, Microsoft Active Directory; |
| POS7-SAN-04.02 | mechanizm tzw. Fabric Binding, umożliwiający zdefiniowanie listy przełączników FC mających prawo do uczestnictwa w fabryce FC |
| POS7-SAN-04.03 | definiowanie filtrów IP (list kontroli ACL) dla interfejsu zarządzającego |
| POS7-SAN-04.04 | protokół FC-SP (Fibre Channel Security Protocol) |
| POS7-SAN-04.05 | bezpieczne ładowanie systemu wraz z zapewnieniem że obraz systemu pochodzi z legalnego i wiarygodnego źródła |
| POS7-SAN-04.06 | możliwość sprzętowego szyfrowania danych przesyłanych na wszystkich portach FC 32G z wykorzystaniem kluczy AES minimum 128 bit. |
| **POS7-SAN-05** | **Obsługa mechanizmów monitorowania i analityki:** |
| POS7-SAN-05.01 | sprzętowe monitorowanie połączeń (flows) |
| POS7-SAN-05.02 | inspekcja nagłówków FC i iSCSI z pełną wydajnością (wirespeed) |
| POS7-SAN-05.03 | statystyki ruchu dla iSCSI, co najmniej:   * czas wykonania operacji * opóźnienie dostępu do danych * ilość ramek iSCSI Read I Write * wielkość bloków I/O * ilość operacji I/O na sekundę (IOPS) dla połączenia * liczba niezakończonych transakcji (pending I/O) * ilość odrzuconych ramek ze względu na przekroczony limit czasu * ilość retransmisji * komunikacja między danym hostem i zasobem LUN * Statystyki błędów (Abort, Reject etc) |
| POS7-SAN-05.04 | wykrywanie i eliminowanie problemów zatykania (slow-drain) w sieci SAN |
| **POS7-SAN-06** | **Obsługa narzędzi diagnostycznych:** |
| POS7-SAN-06.01 | rejestrowanie zdarzeń poprzez mechanizm „syslog”, |
| POS7-SAN-06.02 | monitorowanie ruchu na portach przez kopiowanie ruchu z określonego portu na wybrany port monitorujący (np. z dołączonym zewnętrznym analizatorem) – tzw „port mirroring” |
| POS7-SAN-06.03 | narzędzia i metody diagnostyki dla Fibre Channel pozwalające identyfikować ścieżkę przepływu ruchu poprzez fizyczną fabrykę, |
| **POS7-SAN-07** | **Wyposażenie przełącznika SAN TYP 1** |
| POS7-SAN-07.01 | Co najmniej 48 portów FC 8/16/32 Gbps |
| **POS7-SAN-08** | **Nadmiarowe zasilacze zmiennoprądowe** |
| **POS7-SAN-09** | **Obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-SAN-10** | **Dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |

## MODUŁ SAN SFP 16Gb STANDARDU SW – 224 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 3. Wymagania dla modułów SAN SFP 16Gb

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SAN-11** | **Kompatybilność z oferowanymi przełącznikami SAN Typ I** |
| **POS7-SAN-12** | **Zgodność ze standardem FC SFP 16G shortwave** |

## Przełączniki LAN – wymagania ogólne

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 4. Wymagania ogólne dla przełączników LAN

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
|  | *Wymagania funkcjonalne* |
| **POS7-LAN-01** | **Funkcjonalności warstwy L2:** |
| POS7-LAN-01.01 | Trunking IEEE 802.1Q VLAN; |
| POS7-LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| POS7-LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| POS7-LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| POS7-LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| POS7-LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| POS7-LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| POS7-LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree |
| POS7-LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| POS7-LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach |
| POS7-LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| POS7-LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **POS-LAN-02** | **Funkcjonalności warstwy L3** |
| POS7-LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| POS7-LAN-02.02 | Routing w oparciu o trasy statyczne |
| POS7-LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6. |
| POS7-LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| POS7-LAN-02.05 | VRRP v3 |
| POS7-LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| POS7-LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| POS7-LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| POS7-LAN-02.09 | Wsparcie sprzętowe dla minimum 30.000 tras multicastowych |
| POS7-LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| POS7-LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| POS7-LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **POS7-LAN-03** | **Sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit.** |
| **POS7-LAN-04** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| POS7-LAN-04.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| POS7-LAN-04.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| POS7-LAN-04.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| POS7-LAN-04.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| POS7-LAN-04.05 | implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol) |
| POS7-LAN-04.06 | obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). |
| **POS7-LAN-05** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| POS7-LAN-05.01 | layer 2 IEEE 802.1p (CoS); |
| POS7-LAN-05.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| POS7-LAN-05.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p; |
| POS7-LAN-05.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| POS7-LAN-05.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| POS7-LAN-05.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| POS7-LAN-05.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| POS7-LAN-05.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **POS7-LAN-06** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| POS7-LAN-06.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| POS7-LAN-06.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| POS7-LAN-06.03 | standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); |
| POS7-LAN-06.04 | ACL oparte o VLAN-y (VACL); |
| POS7-LAN-06.05 | ACL oparte o porty (PACL); |
| POS7-LAN-06.06 | DHCP Snooping |
| POS7-LAN-06.07 | ARP Inspection |
| POS7-LAN-06.08 | IP Source Guard |
| POS7-LAN-06.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| **POS7-LAN-07** | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| POS7-LAN-07.01 | RMON (przynajmniej grupy Events, Alarms) |
| POS7-LAN-07.02 | Openflow 1.3 |
| POS7-LAN-07.03 | sFlow lub netFlow |
| POS7-LAN-07.04 | IEEE 802.1ab LLDP |
| POS7-LAN-07.05 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| POS7-LAN-07.06 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| POS7-LAN-07.07 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| POS7-LAN-07.08 | Network Time Protocol (NTP); |
| POS7-LAN-07.09 | ping, traceroute |
| **POS7-LAN-08** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| POS7-LAN-08.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **POS7-LAN-09** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **POS7-LAN-10** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |

## Przełącznik LAN TYP I - 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 5. Wymagania dla przełączników LAN TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
|  | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla przełączników LAN”** |
| **POS7-LAN-11** | **Przełącznik posiada:** |
| POS7-LAN-11.01 | minimum 34 porty 10/25/40/100GE definiowanych za pomocą wkładek QSFP |
| POS7-LAN-11.02 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **POS7-LAN-12** | **Parametry wydajnościowe:** |
| POS7-LAN-12.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| POS7-LAN-12.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| POS7-LAN-12.03 | obsługiwana łączna przepływność (pasmo) min. 6,8Tbps |
| POS7-LAN-12.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 2400 Mpps |
| POS7-LAN-12.05 | opóźnienie przełączania pakietów nie większe niż 1 µs |

## Przełącznik LAN TYP II - 15 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 6. Wymagania dla przełączników LAN TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
|  | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla przełączników LAN”** |
| **POS7-LAN-13** | **Przełącznik musi posiadać:** |
| POS7-LAN-13.01 | minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej |
| POS7-LAN-13.02 | minimum 12 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps |
| POS7-LAN-13.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **POS7-LAN-14** | **Parametry wydajnościowe:** |
| POS7-LAN-14.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| POS7-LAN-14.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| POS7-LAN-14.03 | obsługiwana łączna przepływność (pasmo) min. 4,8Tbps |
| POS7-LAN-14.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 1600 Mpps |
| POS7-LAN-14.05 | opóźnienie przełączania pakietów nie większe niż 1 µs |

## Przełącznik LAN TYP III - 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 7. Wymagania dla przełączników LAN TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
|  | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla przełączników LAN”** |
| **POS7-LAN-15** | **Przełącznik posiada:** |
| POS7-LAN-15.01 | minimum 96 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej |
| POS7-LAN-15.02 | minimum 12 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps |
| POS7-LAN-15.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **POS7-LAN-16** | **Parametry wydajnościowe:** |
| POS7-LAN-16.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| POS7-LAN-16.02 | obsługiwana łączna przepływność (pasmo) min. 6,4Tbps |
| POS7-LAN-16.03 | obsługiwana łączna przepustowość pakietowa przełącznika min. 2400 Mpps |
| POS7-LAN-16.04 | opóźnienie przełączania pakietów nie większe niż 1 µs |

## Przełącznik LAN TYP IV - 4 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 8. Wymagania dla przełączników LAN TYP IV

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-17** | ***Wymagania funkcjonalne*** |
| POS7-LAN-17.01 | **Funkcjonalności warstwy L2:** |
| POS7-LAN-17.02 | Trunking IEEE 802.1Q VLAN; |
| POS7-LAN-17.03 | Wsparcie sprzętowe dla obsługi co najmniej 1000 sieci VLAN; |
| POS7-LAN-17.04 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| POS7-LAN-17.05 | Wsparcie sprzętowe dla minimum 80 000 adresów MAC |
| POS7-LAN-17.06 | IEEE 802.1w Rapid Spanning Tree (RST) |
| POS7-LAN-17.07 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 8 instancji |
| POS7-LAN-17.08 | Wsparcie sprzętowe dla tunelowania QinQ |
| POS7-LAN-17.09 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree |
| POS7-LAN-17.10 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| POS7-LAN-17.11 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach |
| POS7-LAN-17.12 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| POS7-LAN-17.13 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| POS7-LAN-17.14 | **Funkcjonalności warstwy L3** |
| POS7-LAN-17.15 | Sprzętowe przełączanie pakietów w warstwie L3 |
| POS7-LAN-17.16 | Routing w oparciu o trasy statyczne |
| POS7-LAN-17.17 | Wsparcie sprzętowe dla minimum 100.000 prefixów / wpisów hosta w tablicy routingu IP |
| POS7-LAN-17.18 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| POS7-LAN-17.19 | Wsparcie dla IGMPv3 oraz MSDP |
| POS7-LAN-17.20 | Wsparcie sprzętowe dla minimum 10.000 tras multicastowych |
| POS7-LAN-17.21 | Wsparcie dla minimum 250 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| POS7-LAN-17.22 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| POS7-LAN-17.23 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| POS7-LAN-17.25 | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| POS7-LAN-17.26 | layer 2 IEEE 802.1p (CoS); |
| POS7-LAN-17.27 | klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4; |
| POS7-LAN-17.28 | kolejkowanie na wyjściu w oparciu o CoS 802.1p; |
| POS7-LAN-17.29 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| POS7-LAN-17.30 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| POS7-LAN-17.31 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| POS7-LAN-17.32 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| POS7-LAN-17.33 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| POS7-LAN-17.34 | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| POS7-LAN-17.35 | wejściowe ACL (standardowe oraz rozszerzone); |
| POS7-LAN-17.36 | Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; |
| POS7-LAN-17.37 | standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); |
| POS7-LAN-17.38 | ACL oparte o VLAN-y (VACL); |
| POS7-LAN-17.39 | ACL oparte o porty (PACL); |
| POS7-LAN-17.40 | DHCP Snooping |
| POS7-LAN-17.41 | ARP Inspection |
| POS7-LAN-17.42 | IP Source Guard |
| POS7-LAN-17.43 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| POS7-LAN-17.44 | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| POS7-LAN-17.45 | RMON (przynajmniej grupy Events, Alarms) |
| POS7-LAN-17.46 | Openflow 1.3 |
| POS7-LAN-17.47 | sFlow lub netFlow |
| POS7-LAN-17.48 | IEEE 802.1ab LLDP |
| POS7-LAN-17.49 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| POS7-LAN-17.50 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| POS7-LAN-17.51 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror) |
| POS7-LAN-17.52 | network Time Protocol (NTP); |
| POS7-LAN-17.53 | ping, traceroute |
| POS7-LAN-17.54 | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| POS7-LAN-17.55 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| POS7-LAN-17.59 | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| POS7-LAN-17.60 | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-LAN-18** | ***Wyposażenie i wymagania wydajnościowe*** |
| POS7-LAN-18.01 | **Przełącznik posiada:** |
| POS7-LAN-18.02 | minimum 48 portów Ethernet 100/1000 |
| POS7-LAN-18.03 | minimum 4 porty 10/25/40/100GE definiowane za pomocą wkładek QSFP |
| POS7-LAN-18.04 | **Parametry wydajnościowe:** |
| POS7-LAN-18.05 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| POS7-LAN-18.06 | obsługiwana łączna przepływność (pasmo) min. 170Gbps |
| POS7-LAN-18.07 | obsługiwana łączna przepustowość pakietowa przełącznika min. 120 Mpps |

## WKŁADKI I KABLE OPTYCZNE DO PRZEŁĄCZNIKÓW LAN

## MODUŁ SFP 1GE STANDARDU 1000Base-T – 52 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 9. Wymagania dla modułów SFP 1000Base-T

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-25** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-26** | **Zgodność ze standardem SFP 1000Base-T** |

## MODUŁ SFP 1GE STANDARDU SX – 142 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 10. Wymagania dla modułów SFP SX

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-19** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-20** | **Zgodność ze standardem SFP 1000Base-SX (IEEE 802.3z)** |

## MODUŁ SFP+ 10GE STANDARDU SR – 274 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 11. Wymagania dla modułów SFP+ SR

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-21** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-22** | **Zgodność ze standardem SFP+ 10GBase-SR (IEEE 802.3ae)** |

## MODUŁ QSFP+ 40GE STANDARDU SR4 – 12 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 12. Wymagania dla modułów QSFP+ SR4

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-23** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-24** | **Zgodność ze standardem QSFP 40GBase-SR4 (IEEE 802.3ba)** |

## Przewód QSFP+ AOC 100GE o długości 3M – 18 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 13. Wymagania dla kabli AOC 100G 3M

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-31** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-32** | **Przepustowość 100Gbps** |
| **POS7-LAN-33** | **Zakończenia QSFP+** |
| **POS7-LAN-34** | **Długość 3m** |

## Przewód QSFP+ AOC 100GE o długości 10M – 16 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 14. Wymagania dla kabli AOC 100G 10M

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-LAN-35** | **Kompatybilność z oferowanymi przełącznikami LAN** |
| **POS7-LAN-36** | **Przepustowość 100Gbps** |
| **POS7-LAN-37** | **Zakończenia QSFP+** |
| **POS7-LAN-38** | **Długość 10m** |

## Urządzenia bezpieczeństwa

## MODUŁ ZDALNEGO DOSTĘPU VPN – WYMAGANIA OGÓLNE DLA KONCENTRATORA VPN

Tabela 15. Wymagania dla ogólne dla koncentratora VPN

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-VPN-01** | **Koncentrator VPN** |
| POS7-VPN-01.01 | Obsługa VPN w trybach zdalnego dostępu (IPSec i VPN) oraz site-to-site (IPSec). |
| POS7-VPN-01.02 | Dla trybu zdalnego dostępu możliwość wykorzystania klienta IPSec/SSL oraz opcji bez klienta (clientless – dostępnej z wykorzystaniem przeglądarki). |
| POS7-VPN-01.03 | Obsługa protokołów IPSec IKEv2, TLS 1.2, DTLS. |
| POS7-VPN-01.04 | Obsługa standardów kryptograficznych AES-256, 3DES-168, NSA Suite-B, ESPv3, SHA2-256 |
| POS7-VPN-01.05 | Obsługa kluczy RSA do 4096b. |
| POS7-VPN-01.06 | Definiowanie reguł dostępu (polityki dostępowej) użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI. |
| POS7-VPN-01.07 | Obsługa uwierzytelnienia klientów VPN opartego o RADIUS oraz AD (ze wsparciem SAML) |
| POS7-VPN-01.08 | Współpraca z serwerami CA |
| POS7-VPN-01.09 | Możliwość inspekcji stanu stacji klienta sprawdzająca co najmniej:   * poprawność pracy aplikacji (antywirus, firewall, backup) * stan określonych procesów * obecność określonych poprawek systemu operacyjnego * możliwość określenia reakcji na wynik inspekcji – zestawienie sesji VPN, blokada sesji, powiadomienie użytkownika, przeniesienie do kwarantanny, wymuszenie korekty stanu. |
| POS7-VPN-01.10 | Obsługa redundancji co najmniej active/standby |
| **POS7-VPN-02** | **Klient VPN obsługujący co najmniej platformy Windows 7 i 10, MacOS 10.8 i nowsze, Linux** |
| POS7-VPN-02.01 | Możliwość automatycznego aktualizowania wersji oprogramowania klienta |
| POS7-VPN-02.02 | Uwierzytelnienie użytkowników przy wykorzystaniu: LDAP, certyfikatów, RADIUS, kart smart |
| POS7-VPN-02.03 | Możliwość definiowania per użytkownik / grupa użytkowników limitu pasma sieciowego |
| POS7-VPN-02.04 | tryb wymuszający nawiązanie połączenia VPN, tzw. tryb always-on |
| POS7-VPN-02.05 | tryb split-tunel (dostęp do zdefiniowanych przez administratora zasobów lokalnych) z możliwością definicji polityki firewall po stronie klienta |

## KONCENTRAROR VPN TYP I – 4 sztuki (dwie pary redundantne)

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 16. Wymagania dla koncentratora VPN TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-VPN-03** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla koncentratorów VPN”** |
| **POS7-VPN-04** | **Koncentrator VPN realizowany jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-VPN-05** | **zasilacze zmiennoprądowe** |
| **POS7-VPN-06** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-VPN-07** | **Co najmniej 4 interfejsy GE SFP, obsadzone wkładkami 1000Base-SX** |
| **POS7-VPN-08** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-VPN-09** | **Wymagania wydajnościowe** |
| POS7-VPN-09.01 | przepustowość co najmniej 500Mbps dla pakietów o średniej wielkości 500B |
| POS7-VPN-09.02 | obsługa co najmniej 2.500 jednoczesnych tuneli VPN (site-to-site, remote access lub ich kombinacji) |
| POS7-VPN-09.03 | obsługa co najmniej 1.250.000 jednoczesnych połączeń |
| POS7-VPN-09.04 | obsługa zestawiania co najmniej 25.000 nowych połączeń na sekundę |
| **POS7-VPN-10** | **Wymagania licencyjne** |
| POS7-VPN-10.01 | obsługa połączeń VPN site-to-site i remote access |
| POS7-VPN-10.02 | obsługa połączeń VPN (klient oraz bez klienta) dla co najmniej 2.000 użytkowników z możliwością instalacji klienta VPN na co najmniej 2.000 stacji końcowych |

## Koncentrator VPN TYP II – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 17. Wymagania dla koncentratora VPN TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-VPN-11** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla koncentratorów VPN”** |
| **POS7-VPN-12** | **Koncentrator VPN realizowany jako maszyna wirtualna działający na wirtualizatorze VMWare vSphere.** |
| **POS7-VPN-13** | **Wymagania wydajnościowe** |
| POS7-VPN-13.01 | przepustowość co najmniej 100Mbps dla pakietów o średniej wielkości 500B |
| POS7-VPN-13.02 | obsługa co najmniej jednoczesnych 20 tuneli VPN (site-to-site, remote access lub ich kombinacji) |
| POS7-VPN-13.03 | obsługa co najmniej 5.000 jednoczesnych połączeń |
| POS7-VPN-13.04 | obsługa zestawiania co najmniej 100 nowych połączeń na sekundę |
| **POS7-VPN-14** | **Wymagania licencyjne** |
| POS7-VPN-14.01 | obsługa połączeń VPN site-to-site i remote access |
| POS7-VPN-14.02 | obsługa połączeń VPN (klient oraz bez klienta) dla co najmniej 10 użytkowników z możliwością instalacji klienta VPN na co najmniej 10 stacji końcowych |

## URZĄDZENIA NGFW/NGIOS - WYMAGANIA OGÓLNE DLA URZĄDZEŃ NGFW/NGIPS

Tabela 18. Wymagania ogólne dla urządzeń NGFW/NGIPS

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-01** | **Urządzenie umożliwiające pełnienie funkcję ściany ogniowej (firewall) typu NGFW, sondy NGIPS z ochroną antymalware i filtrowaniem URL** |
| **POS7-NGFWIPS-02** | **Funkcja ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji (NGFW):** |
| POS7-NGFWIPS-01.01 | firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7) |
| POS7-NGFWIPS-01.02 | polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń |
| POS7-NGFWIPS-01.03 | możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), integrując się z usługą katalogową Microsoft Active Directory |
| POS7-NGFWIPS-01.04 | obsługa funkcjonalności Network Address Translation (NAT oraz PAT) - zarówno dla ruchu wchodzącego, jak i wychodzącego |
| POS7-NGFWIPS-01.05 | obsługa translacji adresów (NAT) dla ruchu multicast |
| POS7-NGFWIPS-01.06 | możliwość konfiguracji reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu |
| POS7-NGFWIPS-01.07 | możliwość uwierzytelnienia użytkowników z wykorzystaniem LDAP, NTLM oraz Kerberos |
| POS7-NGFWIPS-01.08 | współpraca z serwerami autoryzacji w zakresie przypisania polityk dostępowych z granulacją per użytkownik |
| POS7-NGFWIPS-01.09 | współpraca z serwerami CA |
| POS7-NGFWIPS-01.10 | brak ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej |
| POS7-NGFWIPS-01.11 | obsługa trybu pracy jako transparentna ściana ogniowa warstwy drugiej modelu ISO OSI |
| POS7-NGFWIPS-01.12 | mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:   1. Hypertext Transfer Protocol (HTTP), 2. File Transfer Protocol (FTP), 3. Extended Simple Mail Transfer Protocol (ESMTP), 4. Domain Name System (DNS), 5. Simple Network Management Protocol v 1/2/3 (SNMP), 6. Internet Control Message Protocol (ICMP), 7. SQL\*Net, |
| POS7-NGFWIPS-01.13 | funkcjonalności automatycznego wykrywania i klasyfikacji aplikacji:   1. możliwość klasyfikacji ruchu i wykrywania 3.000 aplikacji sieciowych 2. możliwość tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług 3. możliwość wykorzystania informacji geolokacyjnych dotyczących użytkownika lub aplikacji 4. współpraca z otwartym (udokumentowanym i dostępnym dla użytkowników) systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach |
| POS7-NGFWIPS-01.14 | obsługa routingu statycznego i dynamicznego (min. dla protokołów RIP, OSPF i BGP) |
| POS7-NGFWIPS-01.15 | możliwość zbierania informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL) |
| **PT02-NGFWIPS-02** | **Funkcja wykrywania i zapobiegania włamaniom** |
| POS7-NGFWIPS-02.01 | Możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) |
| POS7-NGFWIPS-02.02 | Możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu) |
| POS7-NGFWIPS-02.03 | Możliwość wykrywania i eliminowania szerokiej gamy zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.) |
| POS7-NGFWIPS-02.04 | Możliwość wykrywania modyfikacji znanych ataków, jak i tych nowo powstałych, które nie zostały jeszcze dogłębnie opisane |
| POS7-NGFWIPS-02.05 | Zapewnienie co najmniej następujących sposobów wykrywania zagrożeń:   1. sygnatury ataków opartych na exploitach, 2. reguły oparte na zagrożeniach, 3. mechanizm wykrywania anomalii w protokołach |
| POS7-NGFWIPS-02.06 | Możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu |
| POS7-NGFWIPS-02.07 | Możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń |
| POS7-NGFWIPS-02.08 | Zróżnicowane możliwości reakcji na zdarzenia, takich jak monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastępowanie zawartość pakietów oraz zapisywanie pakietów |
| POS7-NGFWIPS-02.09 | Możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji |
| POS7-NGFWIPS-02.10 | Możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS |
| POS7-NGFWIPS-02.11 | Mechanizm bezpiecznej aktualizacji sygnatur - zestawy sygnatur/reguł zabezpieczone przed modyfikacją przez osoby postronne |
| POS7-NGFWIPS-02.12 | Możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie |
| POS7-NGFWIPS-02.13 | Obsługa importu reguł Snort |
| POS7-NGFWIPS-02.14 | Możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS |
| POS7-NGFWIPS-02.15 | Mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (tzw. Indication of Compromise) |
| POS7-NGFWIPS-02.19 | Jeżeli funkcjonalność wykrywania i zapobiegania włamaniom wymaga dodatkowej licencji lub subskrypcji, wymagane jest jej dostarczenie dla typów określonych w kolejnych sekcjach |
| **POS7-NGFWIPS-03** | **Funkcje ochrony przed malware:** |
| POS7-NGFWIPS-03.01 | weryfikacja reputacji plików względem bazy zagrożeń |
| POS7-NGFWIPS-03.02 | sprawdzanie plików w oferowanym systemie sandbox |
| POS7-NGFWIPS-03.03 | jeżeli funkcjonalność ochrony przed malware wymaga dodatkowej licencji lub subskrypcji, wymagane jest jej dostarczenie dla typów określonych w kolejnych sekcjach |
| **POS7-NGFWIPS-04** | **Funkcje filtracji URL** |
| POS7-NGFWIPS-04.01 | obsługa co najmniej 70 kategorii stron |
| POS7-NGFWIPS-04.02 | baza o wielkości co najmniej 250 mln URL |
| POS7-NGFWIPS-04.03 | mechanizmy filtrowania w oparciu o reputację domeny |
| POS7-NGFWIPS-04.04 | obsługa białych i czarnych list URL |
| POS7-NGFWIPS-04.05 | jeżeli funkcjonalność filtracji URL wymaga dodatkowej licencji lub subskrypcji, wymagane jest jej dostarczenie dla typów określonych w kolejnych sekcjach |
| **POS7-NGFWIPS-05** | **Zarządzanie** |
| POS7-NGFWIPS-05.01 | obsługa eksportu zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub równoważnego |
| POS7-NGFWIPS-05.02 | możliwość eksportu aktualnego stanu (tzw. coredump) dla potrzeb diagnostycznych |
| POS7-NGFWIPS-05.03 | obsługa protokołu NTP |

## URZĄDZENIE NGFW/NGIPS TYP I – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 19. Wymagania urządzeń NGFW/NGIPS TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-08** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-09** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-NGFWIPS-10** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-NGFWIPS-11** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-NGFWIPS-12** | **co najmniej 4 interfejsy 10GE SFP+ obsadzone wkładkami 10GBase-SR** |
| **POS7-NGFWIPS-13** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-NGFWIPS-14** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-14.01 | przepustowość na poziomie co najmniej 10 Gbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-14.02 | przepustowość na poziomie co najmniej 2 Gbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-14.03 | obsługa co najmniej 8.000.000 jednoczesnych połączeń |
| POS7-NGFWIPS-14.04 | obsługa zestawiania co najmniej 50.000 nowych połączeń na sekundę |
| POS7-NGFWIPS-14.05 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej trzech wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |
| **POS7-NGFWIPS-15** | **Wymagania licencyjne** |
| POS7-NGFWIPS-15.01 | obsługa funkcjonalności NGFW |
| POS7-NGFWIPS-15.02 | obsługa funkcjonalności NGIPS |
| POS7-NGFWIPS-15.03 | obsługa funkcjonalności ochrony przed malware |
| POS7-NGFWIPS-15.04 | obsługa funkcjonalności filtracji URL |

## URZĄDZENIE NGFW/NGIPS TYP II + 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 20. Wymagania urządzeń NGFW/NGIPS TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-17** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-18** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-NGFWIPS-19** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-NGFWIPS-20** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-NGFWIPS-21** | **co najmniej 4 interfejsy 10GE SFP+ obsadzone wkładkami 10GBase-SR** |
| **POS7-NGFWIPS-22** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-NGFWIPS-23** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-23.01 | maksymalna przepustowość na poziomie co najmniej 10 Gbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-23.02 | przepustowość na poziomie co najmniej 2 Gbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-23.03 | obsługa co najmniej 8.000.000 jednoczesnych połączeń |
| POS7-NGFWIPS-23.04 | obsługa zestawiania co najmniej 50.000 nowych połączeń na sekundę |
| POS7-NGFWIPS-23.05 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej trzech wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |
| **POS7-NGFWIPS-24** | **Wymagania licencyjne** |
| POS7-NGFWIPS-24.01 | obsługa funkcjonalności NGFW |

## URZĄDZENIE NGFW/NGIPS TYP III – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 21. Wymagania urządzeń NGFW/NGIPS TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-25** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-26** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-NGFWIPS-27** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-NGFWIPS-28** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-NGFWIPS-29** | **co najmniej 8 interfejsów 10GE SFP+ obsadzonych wkładkami 10GBase-SR** |
| **POS7-NGFWIPS-30** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-NGFWIPS-31** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-31.01 | maksymalna przepustowość na poziomie co najmniej 25 Gbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-31.02 | przepustowość na poziomie co najmniej 6 Gbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-31.03 | obsługa co najmniej 12.500.000 jednoczesnych połączeń |
| POS7-NGFWIPS-31.04 | obsługa zestawiania co najmniej 150.000 nowych połączeń na sekundę |
| POS7-NGFWIPS-31.05 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej sześciu wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |
| **POS7-NGFWIPS-32** | **Wymagania licencyjne** |
| POS7-NGFWIPS-32.01 | obsługa funkcjonalności NGFW |
| POS7-NGFWIPS-32.02 | obsługa funkcjonalności NGIPS |
| POS7-NGFWIPS-32.03 | obsługa funkcjonalności ochrony przed malware |

## URZĄDZENIE NGFW/NGIPS TYP IV – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 22. Wymagania urządzeń NGFW/NGIPS TYP IV

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-34** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-35** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-NGFWIPS-36** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-NGFWIPS-37** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-NGFWIPS-38** | **co najmniej 8 interfejsów 10GE SFP+ obsadzonych wkładkami 10GBase-SR** |
| **POS7-NGFWIPS-39** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-NGFWIPS-40** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-40.01 | maksymalna przepustowość na poziomie co najmniej 25 Gbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-40.02 | przepustowość na poziomie co najmniej 6 Gbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-40.03 | obsługa co najmniej 12.500.000 jednoczesnych połączeń |
| POS7-NGFWIPS-40.04 | obsługa zestawiania co najmniej 150.000 nowych połączeń na sekundę |
| POS7-NGFWIPS-40.05 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej sześciu wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |
| **POS7-NGFWIPS-41** | **Wymagania licencyjne** |
| POS7-NGFWIPS-42.01 | obsługa funkcjonalności NGFW |

## URZĄDZENIE NGFW/NGIPS TYP V – 4 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 23. Wymagania urządzeń NGFW/NGIPS TYP V

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-42** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-43** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-NGFWIPS-44** | **zasilacze zmiennoprądowe** |
| **POS7-NGFWIPS-45** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-NGFWIPS-46** | **co najmniej 4 interfejsy GE SFP obsadzone wkładkami 1000Base-SX** |
| **POS7-NGFWIPS-47** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-NGFWIPS-48** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-48.01 | maksymalna przepustowość na poziomie co najmniej 2 Gbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-48.02 | przepustowość na poziomie co najmniej 500 Mbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-48.03 | obsługa co najmniej 200.000 jednoczesnych połączeń |
| POS7-NGFWIPS-48.04 | obsługa zestawiania co najmniej 15.000 nowych połączeń na sekundę |
| POS7-NGFWIPS-48.05 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej sześciu wirtualnych instancji   każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |
| **POS7-NGFWIPS-49** | **Wymagania licencyjne** |
| POS7-NGFWIPS-49.01 | obsługa funkcjonalności NGFW |
| POS7-NGFWIPS-49.02 | obsługa funkcjonalności NGIPS |

## URZĄDZENIE NGFW/NGIPS TYP VI – 1 sztuka

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 24. Wymagania urządzeń NGFW/NGIPS TYP VI

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-50** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-51** | **Urządzenie realizowane jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** |
| **POS7-NGFWIPS-52** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-52.01 | maksymalna przepustowość na poziomie co najmniej 500 Mbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-52.02 | przepustowość na poziomie co najmniej 200 Mbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-52.03 | obsługa co najmniej 10.000 jednoczesnych połączeń |
| POS7-NGFWIPS-52.04 | obsługa zestawiania co najmniej 200 nowych połączeń na sekundę |
| **POS7-NGFWIPS-53** | **Wymagania licencyjne** |
| POS7-NGFWIPS-53.01 | obsługa funkcjonalności NGFW |
| POS7-NGFWIPS-53.02 | obsługa funkcjonalności NGIPS |
| POS7-NGFWIPS-53.03 | obsługa funkcjonalności ochrony przed malware |
| POS7-NGFWIPS-53.04 | obsługa funkcjonalności filtracji URL |

## URZĄDZENIE NGFW/NGIPS TYP VII – 5 sztuk

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 25. Wymagania urządzeń NGFW/NGIPS TYP VII

|  |  |  |
| --- | --- | --- |
| ***Identyfikator wymagania*** | ***Wymaganie*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-54** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** | |
| **POS7-NGFWIPS-55** | **Urządzenie realizowane jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** | |
| **POS7-NGFWIPS-56** | **Wymagania wydajnościowe** | |
| POS7-NGFWIPS-56.01 | maksymalna przepustowość na poziomie co najmniej 500 Mbps dla usługi NGFW z kontrolą aplikacji | |
| POS7-NGFWIPS-56.02 | przepustowość na poziomie co najmniej 200 Mbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware | |
| POS7-NGFWIPS-56.03 | obsługa co najmniej 10.000 jednoczesnych połączeń | |
| POS7-NGFWIPS-56.04 | obsługa zestawiania co najmniej 200 nowych połączeń na sekundę | |
| **POS7-NGFWIPS-57** | **Wymagania licencyjne** | |
| POS7-NGFWIPS-57.01 | obsługa funkcjonalności NGFW | |
| POS7-NGFWIPS-57.02 | obsługa funkcjonalności NGIPS | |
| POS7-NGFWIPS-57.03 | obsługa funkcjonalności ochrony przed malware | |

## URZĄDZENIE NGFW/NGIPS TYP VIII – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 26. Wymagania urządzeń NGFW/NGIPS TYP VIII

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-58** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-59** | **Urządzenie realizowane jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** |
| **POS7-NGFWIPS-60** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-60.01 | maksymalna przepustowość na poziomie co najmniej 500 Mbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-60.02 | przepustowość na poziomie co najmniej 200 Mbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-60.03 | obsługa co najmniej 10.000 jednoczesnych połączeń |
| POS7-NGFWIPS-60.04 | obsługa zestawiania co najmniej 200 nowych połączeń na sekundę |
| **POS7-NGFWIPS-61** | **Wymagania licencyjne** |
| POS7-NGFWIPS-61.01 | obsługa funkcjonalności NGFW |
| POS7-NGFWIPS-61.02 | obsługa funkcjonalności NGIPS |

## URZĄDZENIE NGFW/NGIPS TYP IX – 12 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 27. Wymagania urządzeń NGFW/NGIPS TYP IX

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-NGFWIPS-62** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń NGFW/NGIPS”** |
| **POS7-NGFWIPS-63** | **Urządzenie realizowane jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** |
| **POS7-NGFWIPS-64** | **Wymagania wydajnościowe** |
| POS7-NGFWIPS-64.01 | maksymalna przepustowość na poziomie co najmniej 500 Mbps dla usługi NGFW z kontrolą aplikacji |
| POS7-NGFWIPS-64.02 | przepustowość na poziomie co najmniej 200 Mbps dla pakietów o średniej wielkości 500B przy kombinacji usług NGFW, NGIPS i anty-malware |
| POS7-NGFWIPS-64.03 | obsługa co najmniej 10.000 jednoczesnych połączeń |
| POS7-NGFWIPS-64.04 | obsługa zestawiania co najmniej 200 nowych połączeń na sekundę |
| **POS7-NGFWIPS-65** | **Wymagania licencyjne** |
| POS7-NGFWIPS-65.01 | obsługa funkcjonalności NGFW |

## URZĄDZENIE ANTY-DDOS – WYMAGANIA OGÓLNE

Tabela 28. Wymagania ogólne urządzeń Anty-DDoS

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-DDoS-01** | **System wykrywania anomalii ruchu przynajmniej za pomocą sygnatur, przekroczenia zdefiniowanych progów ruchu dla określonego typu pakietów i protokołów, analizy profilu ruchu w oparciu o profil standardowego ruchu, analizy behawioralnej ruchu** |
| **POS7-DDoS-01** | **System usuwania ataku (filtrowania) przy możliwie jak najmniejszym wpływie na pozostały ruch w kierunkach od i do sieci;** |
| **POS7-DDoS-02** | **Możliwość implementacji w trybie inline** |
| **POS7-DDoS-03** | **Możliwość wykrywania i automatyzacji blokowania ataków typu zero-day** |
| **POS7-DDoS-04** | **Możliwość współpracy z centrami ochrony producenta rozwiązania, co najmniej w zakresie przekierowania ruchu za pomocą mechanizmów GRE, BGP i DNS** |
| **POS7-DDoS-05** | **System wykrywania anomalii ruchu musi obejmować przynajmniej:** |
| POS7-DDoS-05.01 | wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu w sieci Internet, w szczególności pakietów TCP SYN, TCP RST, ICMP, IP Fragmented, DNS; |
| POS7-DDoS-05.02 | wyznaczanie oczekiwanej wartości ruchu w kierunkach do i od Zamawiającego, o danej porze dnia w danym dniu tygodnia; |
| POS7-DDoS-05.03 | wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych tego ruchu. |
| **POS7-DDoS-06** | **System wykrywania ataków aplikacyjnych musi obejmować przynajmniej:** |
| POS7-DDoS-06.01 | wykrywanie ataków mających na celu wysycenie zasobów aplikacyjnych (ataki flood L3/L4 niezależnie od liczby atakujących, skanowanie aplikacji) |
| POS7-DDoS-06.02 | wykrywanie ataków mających na celu wykorzystanie podatności serwerów web, mail, DNS, SQL |
| POS7-DDoS-06.03 | wykrywanie ataków na serwery DNS |
| POS7-DDoS-06.04 | wykrywanie ataków na SSL |
| POS7-DDoS-06.05 | wsparcie dla de-obfuskacji kodu |
| POS7-DDoS-06.06 | ochrona behawioralna z wykorzystaniem dynamicznie tworzonych sygnatur opartych o parametry nagłówków L3 - L7 |
| POS7-DDoS-06.07 | ochrona behawioralna http, DNS, |
| **POS7-DDoS-07** | **System usuwania ataku musi obejmować przynajmniej:** |
| POS7-DDoS-07.01 | filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP; |
| POS7-DDoS-07.02 | odrzucanie lub przepuszczanie na bazie zdefiniowanych przez administratora filtrów operujących na informacjach w nagłówkach L3 i L4 modelu ISO/OSI; |
| POS7-DDoS-07.03 | filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne; |
| POS7-DDoS-07.04 | filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne; |
| POS7-DDoS-07.05 | ochronę przed atakami z udawanymi adresami źródłowymi IP (spoofing) poprzez autentykację sesji TCP, zapytań DNS oraz zapytań http; |
| POS7-DDoS-07.06 | filtrowanie nieprawidłowych zapytań DNS; |
| POS7-DDoS-07.07 | ograniczenie zapytań DNS do zadanej wartości zapytań na sekundę; |
| POS7-DDoS-07.08 | filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS; |
| POS7-DDoS-07.09 | filtrowanie nieprawidłowych zapytań HTTP; |
| POS7-DDoS-07.10 | filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP; |
| POS7-DDoS-07.11 | ochronę przez atakami typu Slow Lories |
| POS7-DDoS-07.12 | wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją; |
| POS7-DDoS-07.13 | monitorowanie negocjacji SSL dla różnych portów, na których można stosować aplikacje zabezpieczone protokołem TLS |

## URZĄDZENIE ANTY-DDOS TYP I - 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 29. Wymagania urządzeń Anty-DDoS TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-DDoS-08** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń anty-DDoS”** |
| **POS7-DDoS-09** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-DDoS-10** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-DDoS-11** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-DDoS-12** | **co najmniej 4 interfejsy 10GE SFP+ obsadzone wkładkami 10GBase-SR** |
| **POS7-DDoS-13** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-DDoS-14** | **Wymagania wydajnościowe** |
| POS7-DDoS-14.01 | przepustowość na poziomie co najmniej 5 Gbps (łączna dla ruchu „czystego” i „brudnego”) |
| POS7-DDoS-14.02 | wydajność pozwalająca na powstrzymanie ataków typu flood na poziomie co najmniej 1 Mpps |
| POS7-DDoS-14.03 | przepustowość na poziomie co najmniej 1 Gbps dla ruchu „czystego” |

## URZĄDZENIE ANTY-DDOS TYP II – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 30. Wymagania urządzeń Anty-DDoS TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-DDoS-16** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń anty-DDoS”** |
| **POS7-DDoS-17** | **Urządzenie realizowane jako maszyna wirtualna działające na wirtualizatorze VMWare vSphere.** |
| **POS7-DDoS-18** | **Wymagania wydajnościowe** |
| POS7-DDoS-18.01 | przepustowość na poziomie co najmniej 200 Mbps (łączna dla ruchu „czystego” i „brudnego”) |
| POS7-DDoS-18.02 | przepustowość na poziomie co najmniej 100 Mbps dla ruchu „czystego” |

## SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ - WYMAGANIA OGÓLNE DLA SYSTEMU OCHRONY POCZTY ELEKTRONICZNEJ

Tabela 31. Wymagania ogólne systemu ochrony poczty elektronicznej

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-EMAIL-01** | **Rozwiązanie ochrony poczty elektronicznej zapewniające:** |
| POS7-EMAIL-01.01 | ochronę przed szkodliwą treścią (m.in. malware, wirusy etc.) |
| POS7-EMAIL-01.02 | ochronę przed spamem |
| POS7-EMAIL-01.03 | filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki) |
| **POS7-EMAIL-02** | **Kontrola protokołu SMTP w tym szyfrowanych wersji: SSL i TLS.** |
| **POS7-EMAIL-03** | **Filtrowanie poczty przychodzącej i wychodzącej, przy czym istnieje możliwość przypisania odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej.** |
| **POS7-EMAIL-04** | **Ochrona dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6** |
| **POS7-EMAIL-05** | **Rozwiązanie pracujące jako brama dla poczty elektronicznej (jako MTA - Mail Transfer Agent).** |
| **POS7-EMAIL-06** | **Architektura rozwiązania** |
| POS7-EMAIL-06.01 | MTA (Mail Transfer Agent) pracujący w trybie bramy dla ruchu przychodzącego z możliwością rozbudowy o opcję bramy dla ruchu wychodzącego |
| POS7-EMAIL-06.02 | obsługa protokołów SMTP, ESMTP, Secure SMTP over TLS |
| POS7-EMAIL-06.03 | obsługa mechanizmów kryptograficznych   1. TLS: 56-bit DES, 168-bit 3DES, 128-bit RC4, 128-bit AES i 256-bit-AES 2. Domain Keys Signing: 512-, 768-, 1024-, 1536- i 2048-bit RSA |
| **POS7-EMAIL-07** | **Ochrona antyspamowa** |
| POS7-EMAIL-07.01 | narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. Mechanizmy ochrony oparte co najmniej o:   * sygnatury * słowniki * heurystykę, dla której jest możliwa regulacja czułości (kontrola ilości False-Positives) |
| POS7-EMAIL-07.02 | wbudowane mechanizmy metody wykrywania wiadomości komercyjnych typu „Newsletters” i umożliwia traktowanie tych wiadomości w zależności od ustalonej polityki organizacji jako SPAM lub jako wiadomość dopuszczona |
| POS7-EMAIL-07.03 | opcja definiowania wyjątków od stosowanych polityk |
| POS7-EMAIL-07.04 | mechanizm antyspamowy realizowany dwufazowo:   * + 1. sprawdzenie reputacji adresu IP nadawcy w ogólnoświatowej bazie reputacji:        - dane z co najmniej 100.000 źródeł danych z całego świata        - wynik reputacji dla adresu IP w skali co najmniej 20-stopniowej        - rezultat reputacji zwracany jedynie na podstawie zbieranych danych, nie dopuszczając jednorazowych interwencji ze strony wysyłających pocztę mających na celu manualne podwyższenie ich reputacji        - możliwość wykorzystania co najmniej dwóch systemów badania reputacji nadawców dla poczty przychodzącej. Jeden z nich oparty o publiczny serwis Real-Time Blackhole List (RBL), drugi np. będący systemem własnym producenta zaimplementowanym w rozwiązaniu     2. jeżeli wiadomość przejdzie pomyślnie fazę pierwszą – analiza oparta się na silniku antyspamowym, korzystającym z reguł producenta        - reguły tworzone dynamicznie na podstawie informacji z co najmniej trzech źródeł:          * bazy danych reputacji o parametrach jak w fazie pierwszej,          * informacji zwrotnych od użytkowników rozwiązania          * informacji od dedykowanych analityków bezpieczeństwa producenta rozwiązania        - reguły weryfikują informację na temat adresów IP pojawiających się w mailach jako linki do stron, strukturę wiadomości, sposób w jaki została wysłana, treść wiadomości i reputację nadawcy. |
| POS7-EMAIL-07.05 | możliwość skorzystania z funkcji reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie weryfikacji oraz odrzucenie połączenia w przypadku:   * braku rekordu PTR w DNS * niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS, * niezgodności rekordu reverse DNS (PTR) z rekordem forward DNS (A) |
| POS7-EMAIL-07.06 | możliwość:   * + 1. monitorowania i ograniczania ilości połączeń z jednego adresu IP w określonym przedziale czasu:        - możliwość definicji przedziału czasowego        - opcja ograniczenia maksymalnej ilości połączeń i wiadomości.     2. ograniczanie maksymalnej liczby wiadomości przekazywanych za pomocą pojedynczego połączenia SMTP     3. wskazanie timeout’u dla niewykorzystywanego połączenia |
| POS7-EMAIL-07.07 | możliwość blokowania na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z chronionej domeny |
| **POS7-EMAIL-08** | **Ochrona antywirusowa** |
| POS7-EMAIL-08.01 | co najmniej dwa niezależne, komercyjne silniki antywirusowe |
| POS7-EMAIL-08.02 | blokowanie złośliwej treści z wykorzystaniem tradycyjnego skanowania antywirusowego opartego o co najmniej dwa komercyjne silniki antywirusowe oraz bazę sygnatur kodów złośliwych |
| POS7-EMAIL-08.03 | silnik antywirusowy musi korzystać z co najmniej następujących metod skanowania wiadomości:   1. dopasowanie wzorców binarnych do sygnatur antywirusowych 2. analiza heurystyczna 3. emulacja uruchomienia kodu (w celu zapobiegania infekcji wirusami polimorficznymi) |
| POS7-EMAIL-08.04 | mechanizmy dynamicznej ochrony przed epidemią złośliwego kodu (ang. Outbreak)   1. technologia umożliwiająca automatyczną kwarantannę wiadomości, które pomimo, że nie są wskazane przez powyższe metody skanowania (z powodu np. braku odpowiednich sygnatur antywirusowych), mogą jednak zawierać złośliwy kod 2. podejrzane wiadomości mogą pozostać w kwarantannie, aż do wypuszczenia przez producentów silników antywirusowych odpowiednich sygnatur i automatycznie wypuszczane i skanowane ponownie po ściągnięciu odpowiednich sygnatur |
| **POS7-EMAIL-09** | **Ochrona anty-malware** |
| POS7-EMAIL-09.01 | weryfikacja reputacji plików względem bazy zagrożeń |
| POS7-EMAIL-09.02 | sprawdzanie plików w oferowanym systemie sandbox |

## SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ TYP I – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 32. Wymagania systemu ochrony poczty elektronicznej TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-EMAIL-10** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu ochrony poczty elektronicznej”** |
| **POS7-EMAIL-11** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-EMAIL-12** | **zasilacze zmiennoprądowe** |
| **POS7-EMAIL-13** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-EMAIL-14** | **co najmniej 2 interfejsy GE 100/1000** |
| **POS7-EMAIL-15** | **Wymagania licencyjne** |
| POS7-EMAIL-15.01 | ochrona co najmniej 600 skrzynek poczty elektronicznej |

## SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ TYP II – 1 sztuka

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 33. Wymagania systemu ochrony poczty elektronicznej TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-EMAIL-17** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu ochrony poczty elektronicznej”** |
| **POS7-EMAIL-18** | **Urządzenie realizowane jako maszyna wirtualna działające na wirtualizatorze VMWare vSphere.** |
| **POS7-EMAIL-19** | **Wymagania licencyjne** |
| POS7-EMAIL-19.01 | ochrona co najmniej 10 skrzynek poczty elektronicznej |

## OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW- WYMAGANIA OGÓLNE DLA OPROGRAMOWANIA ANTYWIRUSOWEGO/EDR DLA SERWERÓW

Tabela 34. Wymagania ogólne oprogramowania antywirusowego/EDR dla serwerów

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ANTYVIR-01** | **System bezpieczeństwa, umożliwiający ochronę systemów serwerowych (fizycznych oraz wirtualnych) w zakresie anty-malware, reputacji sieciowej, wykrywania i przeciwdziałania włamaniom oraz monitorowania integralności systemu plików.** |
| **POS7-ANTYVIR-02** | **System musi posiadać architekturę dwu-warstwową, tzn. musi składać się z centralnej konsoli zarządzania oraz agentów zainstalowanych na serwerach. Centralna konsola zarządzania musi umożliwiać definiowanie polityk bezpieczeństwa (także ich przypisywanie do konkretnych maszyn oraz ich grup), zbieranie logów oraz generowanie raportów, a także zarządzanie agentami (ich aktualizacje, dystrybucja, konfiguracja). Agent odpowiada za faktyczną ochronę systemu na którym został zainstalowany.** |
| **POS7-ANTYVIR-03** | **Współpraca z oferowanym systemem sandbox w zakresie weryfikacji nieznanych plików** |
| **POS7-ANTYVIR-04** | **Agent ochrony serwerów obsługujący systemy operacyjne:** |
| POS7-ANTVIR-04.01 | Windows Server 2016, 2019 |
| POS7-ANTVIR-04.02 | Linux Red Hat Enterprise, CentOS 7.x |
| **POS7-ANTYVIR-05** | **Agent ochrony stacji końcowej/serwera musi zapewniać (poprzez centralną konsolę) następujące narzędzia i funkcje wspierające proces wykrywania oraz eliminacji zdarzeń naruszenia polityki bezpieczeństwa poprzez złośliwe lub niechciane oprogramowanie:** |
| POS7-ANTVIR-05.01 | wskaźniki przełamania zabezpieczeń – poszczególne zdarzenia dotyczące plików oraz pojedyncze zachowania elementów systemu operacyjnego/procesów/aplikacji muszą być korelowane w incydenty i otrzymywać odpowiednie priorytety w celu zwrócenia uwagi administratora systemu na te najważniejsze |
| POS7-ANTVIR-05.02 | ochrona przed znanymi oraz nieznanymi zagrożeniami. System zabezpieczeń serwerów powinien chronić przed znanymi oraz nieznanymi zagrożeniami przy pomocy różnych silników skanujących. Ochrona powinna wykorzystywać najnowocześniejsze mechanizmy, w tym algorytmy uczenia maszynowego, korelację przepływów sieciowych. |
| POS7-ANTVIR-05.03 | wbudowany klasyczny silnik antywiusowy oparty na sygnaturach |
| POS7-ANTVIR-05.04 | weryfikacja reputacji plików względem bazy zagrożeń |
| POS7-ANTVIR-05.05 | sprawdzanie plików w oferowanym systemie sandbox |
| POS7-ANTVIR-05.06 | możliwość wymuszenia skanowania „na żądanie” w każdej chwili |
| POS7-ANTVIR-05.07 | reputacja plików - zaawansowane metody analizy zbieranych informacji przez agenta o plikach umożliwiające określenie ich dyspozycji – czy są złośliwe, neutralne czy czyste |
| POS7-ANTVIR-05.08 | wizualizacja zachowania systemu operacyjnego – ciągła analiza zachowania monitorowanego systemu operacyjnego pod kątem aktywności na plikach oraz procesów w połączeniach sieciowych dająca możliwość ich wizualizacji w celu szybszego wykrycia przyczyny infekcji złośliwym oprogramowaniem |
| POS7-ANTVIR-05.09 | elastyczne wyszukiwanie – proste i nieograniczone wyszukiwanie szczegółowych informacji o wykrytych zdarzeniach pozwalające w szybki sposób   1. zrozumieć formę wykrytego ataku 2. wskazać powiązane ze sobą zdarzenia 3. pomóc w szybki sposób usunąć zagrożenia z monitorowanego środowiska dzięki korelacji wyszukiwania na wielu warstwach zbieranych informacji |
| POS7-ANTVIR-05.10 | rozpowszechnianie – funkcja pozwalająca na wyświetlenie wszystkich plików, które zostały uruchomione na wszystkich monitorowanych systemach w danej organizacji i posortowanie ich według ilości wykryć |
| POS7-ANTVIR-05.11 | wsparcie dla sygnatur „OpenIOC” – w celu wykrycia celowych ataków administrator bezpieczeństwa musi mieć możliwość wykorzystania mechanizmu OpenIOC. W szczególności musi on umożliwiać wczytanie przygotowanych wcześniej szablonów opisujących prawidłowości występujące w skompromitowanych hostach i uruchomić skanowanie na żądanie - przeszukać wszystkie monitorowane stacje robocze pod kątem tych prawidłowości. Funkcja ta musi pozwalać na import ogólnie dostępnych szablonów OpenIOC, jak i posiadać narzędzie edytora ułatwiającego pisanie własnych szablonów |
| POS7-ANTVIR-05.12 | spis podatności musi pokazywać listę podatnego oprogramowania wykrytego na monitorowanych stacjach końcowych i serwerach oraz sortować wyświetlane informacje według poziomu zagrożenia, jakie te podatności ze sobą niosą. Narzędzie musi wspierać administratora w eliminowaniu z monitorowanych systemów operacyjnych znanych podatności typowo wykorzystywanych przez malware |
| POS7-ANTVIR-05.13 | kontrola rozpowszechniania infekcji – funkcja pozwalająca uzyskać kontrolę nad podejrzanymi plikami i zatrzymać ich rozpowszechnianie się bez zwłoki związanej z zebraniem większej ilości dokładniejszych informacji. Funkcja musi umożliwiać:   1. zablokowanie konkretnego pliku/aplikacji rezydującej na wskazanych lub wszystkich monitorowanych systemach operacyjnych 2. opisanie zaawansowaną sygnaturą pliku, którego część zmienia się wraz z mutującym polimorficznym kodem i jego blokowanie bez względu na jego aktualną formę 3. blokowanie niechcianych aplikacji – w szczególności lista niechcianych aplikacji musi umożliwiać wymuszenie polityki bezpieczeństwa blokującej zainfekowane aplikacje, będące „bramą” dla malware i musi zatrzymywać proces nawracającej się infekcji 4. zdefiniowanie listy niezbędnych aplikacji – w szczególności musi pozwalać na określenie listy dopuszczonych aplikacji i zezwalać na ich funkcjonowanie bez względu na poziom zagrożenia jaki ze sobą wnoszą 5. blokowanie komunikacji zwrotnej złośliwego oprogramowanie C&C poprzez wykorzystanie reputacji adresów IP, przy czym baza reputacyjna utrzymywana ma być przez dostawcę rozwiązania |
| POS7-ANTVIR-05.14 | funkcja definiowania wyjątków w politykach skanowania i monitorowania |

## OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP I

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Ilość:

• Konsola zarządzająca: 2 szt., stanowiące parę redundantną

• Licencje dla serwerów: 50 szt., każda umożliwiająca instalację agenta na serwerze wirtualnym lub fizycznym

Tabela 35. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ANTYVIR-06** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-ANTYVIR-07** | **Konsola zarządzająca realizowana jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważny).** |
| POS7-ANTVIR-07.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-ANTVIR-07.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-ANTVIR-07.03 | obudowa przeznaczona do instalacji w szafie rack 19” |

## OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP II

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Ilość:

• Konsola zarządzająca: 2 szt., stanowiące parę redundantną

• Licencje dla serwerów: 300 szt., każda umożliwiająca instalację agenta na serwerze wirtualnym lub fizycznym

Tabela 36. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ANTYVIR-08** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-ANTYVIR-09** | **Konsola zarządzająca realizowana jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-ANTVIR-09.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-ANTVIR-09.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-ANTVIR-09.03 | obudowa przeznaczona do instalacji w szafie rack 19” |

## OPROGRAMOWANIE ANTYWIRUSOWE/EDR DLA SERWERÓW TYP III

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Ilość:

• Konsola zarządzająca: 1 szt.,

• Licencje dla serwerów: 185 szt., każda umożliwiająca instalację agenta na serwerze wirtualnym lub fizycznym

Tabela 37. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ANTYVIR-10** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-ANTYVIR-11** | **Konsola zarządzająca realizowana jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere lub rozwiązanie typu appliance.** |

## SYSTEM SANDBOX - WYMAGANIA OGÓLNE DLA SYSTEMU SANDBOX

Tabela 38. Wymagania ogólne systemu SANDBOX

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SANDBOX-01** | **System ochrony przed malware:** |
| POS7-SANDBOX-01.01 | sprawdzanie reputacji plików w systemie globalnym |
| POS7-SANDBOX-01.02 | sprawdzanie plików w sandbox (realizowanym lokalnie) |
| POS7-SANDBOX-01.03 | zapewnia wykrywanie ataków typu Zero-Day |
| POS7-SANDBOX-01.04 | system musi objąć pliki przesyłane co najmniej przez moduły NGIPS i ochrony poczty elektronicznej – realizowany w oparciu o funkcjonalności modułów lub dedykowane elementy sieciowe |
| **POS7-SANDBOX-02** | **System klasy sandbox:** |
| POS7-SANDBOX-02.01 | ruch administracyjny oraz ruch generowany podczas detonacji analizowanych plików logicznie rozdzielony na co najmniej dwa interfejsy fizyczne |
| POS7-SANDBOX-02.02 | zachowanie prywatności informacji zawartych w analizowanych plikach |
| POS7-SANDBOX-02.03 | oparte na niestandardowym silniku wirtualizacji w celu utrudnienia możliwości jego wykrycia przez złośliwe oprogramowanie |
| POS7-SANDBOX-02.04 | maszyny wirtualne z obrazami systemu operacyjnego nie mogą mieć żadnych mechanizmów analitycznych wewnątrz maszyn wirtualnych, aby wykrywanie prób analiz przez złośliwe oprogramowanie było trudniejsze. Wszystkie analizy przeprowadzane poza maszynami wirtualnymi |
| POS7-SANDBOX-02.05 | wsparcie co najmniej następujących systemów operacyjnych: Windows 7 x64, Windows 10 |
| POS7-SANDBOX-02.06 | dostępna lista zainstalowanych pakietów oprogramowania na każdej z dostępnych maszyn wirtualnych. Lista musi zawierać co najmniej całkowitą liczbę programów, ich nazwy i konkretne wersje. Dobór zainstalowanych programów wynikający z analiz aktualnych standardów oprogramowania obserwowanych w środowiskach produkcyjnych |
| POS7-SANDBOX-02.07 | obsługa co najmniej następujących typów plików:   1. .BAT - Batch 2. .BZ2 – skompresowany bzip2 3. .CHM – skompilowany plik pomocy - Microsoft Compiled HTML Help 4. .DLL – biblioteki 5. PE32 i PE32+ - pliki wykonywalne 6. .EML - Wiadomości email zapisane w postaci pliku. 7. .EXE – plik wykonywalny PE32 8. .GZ – skompresowany gzip 9. .HTA – aplikacja HTML 10. .ISO - obraz ISO 11. .JAR – archiwum Java 12. .JS - JavaScript 13. .JSE - encoded JavaScripts 14. .LNK - Windows shortcut 15. .MSI - Microsoft Installer 16. .MHTML - Mime HTML 17. Pliki MSOffice: w tym .DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX 18. .PDF - Portable Document Format (razem z skryptami Java) 19. .PS1 - Powershell 20. .SEP - Tagged Image File Format 21. .SLK - Microsoft Symbolic Link (SYLK) 22. .SWF - Flash Files 23. .TAR - tar 24. Podawanie URLi do obiektów znajdujących się na Internecie 25. .VBE - Encoded Visual 26. .VBN - Virus Bin 27. .VBS - Visual Basic Script 28. .WSF - Windows Script File 29. .XML - XML Based Office Document Types (.DOCX, .XLSX, .PPTX) oraz Extensible Markup Language (.XML) 30. .XZ – skompresowany xz 31. .ZIP – skompresowane archiwa oraz pliki tzw. kwarantanny |
| POS7-SANDBOX-02.08 | identyfikacja plików i powiązanie wyników analizy z bazą danych zawierającą wyniki poprzednich analiz innych próbek oraz globalne informacje o zagrożeniach. Poszukiwanymi elementami są co najmniej:   1. adresy IP wykorzystywane w komunikacji podczas detonacji 2. domeny wykorzystywane w komunikacji podczas detonacji 3. adresy URL wykorzystywane w komunikacji podczas detonacji 4. wskazania behawioralne 5. ścieżka 6. nazwa pliku 7. suma kontrolna: SHA256, SHA1, MD5 8. unikalny identyfikator przypisany podczas przesyłania plików do urządzenia sandboxingu 9. tagi 10. mutex 11. artefakty pobrane podczas analizy 12. rejestrowanie zdarzeń związanych z analizą plików |
| POS7-SANDBOX-02.09 | możliwość przeszukiwania pobranych artefaktów podczas analizy złośliwego oprogramowania. Dostępne opcje wyszukiwania co najmniej:   1. rodzaj pliku rozpoznany po tzw. „file magic” a nie tylko rozszerzeniu 2. źródło 3. sygnatura AV |
| POS7-SANDBOX-02.10 | raport z analizy zawierający następujące dane:   1. nazwa pliku 2. jego sumy kontrolne (SHA-256, SHA-1 oraz MD5) 3. typ pliku przy wykrytym wykorzystaniu tzw. „file magic” oraz zastosowany odpowiedni profil analizy 4. znaczniki czasu procesu detonacji i jej zakończenia 5. szczegółowy raport z aktywowanych wskaźników szkodliwego zachowania 6. szczegółowy raport z zachowania ruchu sieciowego podczas detonacji 7. zestawienie aktywowanych procesów systemu operacyjnego oraz możliwość wizualizacji wszystkich procesów i odzwierciedlania ich wzajemnych relacji, a także zaznaczania ich działalności 8. lista użytych dodatkowych artefaktów (plików), których nie było w oryginalnej maszynie wirtualnej a powstały podczas detonacji 9. aktywności w rejestrach systemowych 10. aktywności systemu plików |
| POS7-SANDBOX-02.11 | każdy moduł wykrywania behawioralnego odpowiedzialny za wykrycie szkodliwego działania podczas procesu detonacji (Indication of Compromise) musi być oznaczany co najmniej dwoma markerami: poziom zagrożenia z nim związanego oraz pewność systemu co do prawidłowości detekcji |
| POS7-SANDBOX-02.12 | każdy mechanizm opisujący szkodliwe zachowanie lub typową dla szkodliwego kodu charakterystykę struktur w danym pliku musi być opisany w kilku zdaniach tak, aby w łatwy i przyjazny sposób można było zrozumieć na czym polega dane zagrożenie. Dodatkowo każde wykrycie powinno zawierać fragmenty pliku lub kodu, które by potwierdzały wykorzystanie danego mechanizmu w analizowanej próbce |
| POS7-SANDBOX-02.13 | możliwość interakcji ze środowiskiem analizy, podczas gdy detonacja pliku odbywa się za pomocą klawiatury i myszy |
| POS7-SANDBOX-02.14 | możliwość wyboru czasu detonacji próbek w zakresie od 5 do 30 minut |
| POS7-SANDBOX-02.15 | możliwość pobrania nagrania ekranu wideo z procesu detonacji plików w celu sprawdzenia aktywności pulpitu |
| POS7-SANDBOX-02.16 | każdy raport musi zawierać link do pobrania co najmniej: oryginalnej próbki pliku, plików powstałych w procesie detonacji, raportu, szczegółowej analizy, przechwytywanych pakietów ruchu sieciowego w formacie pcap oraz harmonogramu aktywności procesów |
| POS7-SANDBOX-02.17 | możliwość ponownego przesłania pliku, który jest już obecny w systemie w celu próby ujawnienia nowych informacje o złośliwym kodzie i jego zachowaniu |
| POS7-SANDBOX-02.18 | wszystkie informacje dotyczące analizy zagrożeń muszą być dostępne i przeszukiwalne we wszystkich raportach z dostępnych analiz. Przeszukiwanie danych o zagrożeniach musi być możliwe co najmniej za pomocą następujących elementów:   1. domeny 2. adresy IP 3. klucze rejestru 4. adresy URL 5. wskaźniki zagrożeń (Indication of Compromise) |
| POS7-SANDBOX-02.19 | możliwość integracji z rozwiązaniami firm trzecich (bram sieciowych, serwerów proxy, systemy SIEM, itp.) na wielu poziomach dostępu do informacji poprzez moduły API:   1. możliwość przesyłania plików 2. udostępnianie informacji o zagrożeniach przychodzących w formie subskrypcji 3. dostarczanie raportów z analizy pliku |

## SYSTEM SANDBOX TYP I – 2 sztuki

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 39. Wymagania systemu SANDBOX TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SANDBOX-03** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-SANDBOX-04** | **Współpraca z oferowanymi urządzeniami NGFW/NGIPS, oprogramowaniem antywirusowym/EDR dla serwerów. Dopuszczalne jest przy tym, zgodnie z wymaganiami ogólnymi oferowanie zarówno pojedynczego rozwiązania sandbox zintegrowanego z poszczególnymi systemami, jak też zespołu rozwiązań obsługujących poszczególne systemy.** |
| **POS7-SANDBOX-05** | **Rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-SANDBOX-05.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-SANDBOX-05.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-SANDBOX-05.03 | obudowa przeznaczona do instalacji w szafie rack 19” |
| **POS7-SANDBOX-06** | **Wymagania licencyjne** |
| POS7-SANDBOX-06.01 | możliwość analizy co najmniej 1000 plików dziennie, niezależnie od źródła pliku |

## SYSTEM SANDBOX TYP II – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 40. Wymagania systemu SANDBOX TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SANDBOX-07** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-SANDBOX-08** | **Współpraca z oferowanymi urządzeniami NGFW/NGIPS, oprogramowaniem antywirusowym/EDR dla serwerów, systemem ochrony poczty elektronicznej. Dopuszczalne jest przy tym, zgodnie z wymaganiami ogólnymi oferowanie zarówno pojedynczego rozwiązania sandbox zintegrowanego z poszczególnymi systemami, jak też zespołu rozwiązań obsługujących poszczególne systemy.** |
| **POS7-SANDBOX-09** | **Rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-SANDBOX-09.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-SANDBOX-09.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-SANDBOX-09.03 | obudowa przeznaczona do instalacji w szafie rack 19” |
| **POS7-SANDBOX-10** | **Wymagania licencyjne** |
| POS7-SANDBOX-10.01 | możliwość analizy co najmniej 5000 plików dziennie, niezależnie od źródła pliku |

## SYSTEM SANDBOX TYP III – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 41. Wymagania systemu SANDBOX TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SANDBOX-11** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla oprogramowania antywirusowego/EDR dla serwerów”** |
| **POS7-SANDBOX-12** | **Współpraca z of urządzeniami oferowanymi NGFW/NGIPS, oprogramowaniem antywirusowym/EDR dla serwerów, systeme ochrony poczty elektronicznej. Dopuszczalne jest przy tym, zgodnie z wymaganiami ogólnymi oferowanie zarówno pojedynczego rozwiązania sandbox zintegrowanego z poszczególnymi systemami, jak też zespołu rozwiązań obsługujących poszczególne systemy.** |
| **POS7-SANDBOX-13** | **Rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-SANDBOX-13.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-SANDBOX-13.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-SANDBOX-13.03 | obudowa przeznaczona do instalacji w szafie rack 19” |
| **POS7-SANDBOX-14** | **Wymagania licencyjne** |
| POS7-SANDBOX-14.01 | możliwość analizy co najmniej 200 plików dziennie, niezależnie od źródła pliku |

## APPLICATIONS DELIVERY CONTROLLERS

## URZĄDZENIA ADC (APPLICATIONS DELIVERY CONTROLLERS)- WYMAGANIA OGÓLNE DLA URZĄDZEŃ ADC

Tabela 42. Wymagania ogólne dla urządzeń ADC

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ADC-01** | **Urządzenie realizujące funkcjonalności równoważenia obciążenia (load balancing), firewalla aplikacji web (web application firewall) oraz terminowania i deszyfracji SSL (SSL offload / termination)** |
| **POS7-ADC-02** | ***Funkcjonalności równoważenia obciążenia (load balancing)*** |
| **POS7-ADC-03** | **Metody równoważenia obciążenia:** |
| POS7-ADC-01.01 | cykliczna |
| POS7-ADC-01.02 | ważona |
| POS7-ADC-01.03 | najmniejsza liczba połączeń |
| POS7-ADC-01.04 | najszybsza odpowiedź serwera |
| POS7-ADC-01.05 | definiowana na podstawie grupy priorytetów dla serwerów |
| **POS7-ADC-04** | **Możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego** |
| **POS7-ADC-05** | **Wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:** |
| POS7-ADC-05.01 | analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów |
| POS7-ADC-05.02 | obsługa protokołów: http, tcp. |
| POS7-ADC-05.03 | funkcja inspekcji protokołu RADIUS |
| POS7-ADC-05.04 | musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami |
| **POS7-ADC-06** | **Wbudowane lub dostarczone szablony skryptów** |
| **POS7-ADC-07** | **Funkcjonalność lokalnego równoważenia obciążenia** |
| POS7-ADC-07.01 | Wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP), najmniejsza liczba połączeń, najszybsza odpowiedź, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego |
| POS7-ADC-07.02 | Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług |
| POS7-ADC-07.03 | Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID |
| POS7-ADC-07.04 | Wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP |
| **POS7-ADC-08** | **Funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów:** |
| POS7-ADC-08.01 | Cookie (hash, rewrite, custom, insert, passive) |
| POS7-ADC-08.02 | Adres źródła |
| POS7-ADC-08.03 | SIP call ID |
| POS7-ADC-08.04 | Identyfikator sesji SSL |
| POS7-ADC-08.05 | Microsoft Terminal Services (RDP) – nazwa użytkownika |
| POS7-ADC-08.06 | Adres docelowy |
| POS7-ADC-08.07 | Tworzone przez administratora systemu przy wykorzystaniu języka skryptowego |
| POS7-ADC-08.08 | Funkcja definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer. |
| POS7-ADC-08.09 | Możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS. |
| POS7-ADC-08.10 | Moduł analizy ruchu http. |
| POS7-ADC-08.11 | Możliwość przekierowywania zapytań do innych adresów URL |
| **POS7-ADC-09** | **Co najmniej następujące usługi w warstwach 4-7:** |
| POS7-ADC-09.01 | inspekcja warstwy aplikacji, w tym inspekcja nagłówka http |
| POS7-ADC-09.02 | ukrywanie zasobów |
| POS7-ADC-09.03 | zmiana odpowiedzi serwera |
| POS7-ADC-09.04 | przepisywanie odpowiedzi (response rewriting) |
| POS7-ADC-09.05 | ochrona przed atakami typu DoS/DDoS |
| POS7-ADC-09.06 | ochrona przed atakami typu SYN Flood |
| POS7-ADC-09.07 | multipleksowanie połączeń http |
| POS7-ADC-09.08 | Optymalizacja i akceleracja aplikacji |
| POS7-ADC-09.09 | optymalizacja protokołu TCP |
| POS7-ADC-09.10 | TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta |
| POS7-ADC-09.11 | możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control) |
| POS7-ADC-09.12 | multipleksacja wielu zapytań http w tej samej sesji TCP |
| POS7-ADC-09.13 | kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:   1. listy dozwolonych URI 2. listy wykluczonych URI 3. listy kompresowalnych Content-Type 4. listy wykluczonych Content-Type |
| **POS7-ADC-10** | ***Funkcjonalności firewalla aplikacji web (web application firewall)*** |
| POS7-ADC-10.01 | Rozwiązanie musi umożliwić terminowanie sesji SSL oraz przekazywanie zapytań oraz odpowiedzi dla co najmniej 200 domen, przy założeniu, że każda domena korzysta z własnego certyfikatu SSL. |
| POS7-ADC-10.02 | Obsługa certyfikatów z kluczami typu RSA oraz ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów. |
| POS7-ADC-10.03 | Wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy. |
| POS7-ADC-10.04 | Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów. |
| POS7-ADC-10.05 | Obsługa certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów. |
| POS7-ADC-10.06 | Funkcja walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL. |
| **POS7-ADC-11** | ***Funkcjonalności terminowania i deszyfracji SSL (SSL offload / termination)*** |
| **POS7-ADC-12** | **WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji na bazie ruchu sieciowego.** |
| **POS7-ADC-13** | **Pozytywny model bezpieczeństwa musi kontrolować co najmniej:** |
| POS7-ADC-13.01 | wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a. |
| POS7-ADC-13.02 | typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT) oraz dopuszczalne parametry w danym serwlecie |
| POS7-ADC-13.03 | dopuszczalne metody http, |
| POS7-ADC-13.04 | dopuszczalne cookie, |
| POS7-ADC-13.05 | dopuszczalne parametry w polityce, |
| POS7-ADC-13.06 | parametry dynamiczne, |
| POS7-ADC-13.07 | typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany) |
| POS7-ADC-13.08 | długość zapytań |
| POS7-ADC-13.09 | nazwy hosta |
| POS7-ADC-13.10 | wystąpienia i długość parametrów (per każdy parametr) |
| POS7-ADC-13.11 | wystąpienia i długości nagłówków |
| POS7-ADC-13.12 | wystąpienia i długości cookies |
| POS7-ADC-13.13 | oczekiwane typy znaków per każdy parametr |
| POS7-ADC-13.14 | typy rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku |
| **POS7-ADC-14** | **Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń)** |
| **POS7-ADC-15** | **Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać nadużycia w procesie nauki.** |
| **POS7-ADC-16** | **Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.** |
| **POS7-ADC-17** | **Musi istnieć możliwość ręcznego konfigurowania i modyfikacji reguł polityki bezpieczeństwa** |
| **POS7-ADC-18** | **Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http** |
| **POS7-ADC-19** | **WAF musi posiadać mechanizmy ochrony przed atakami:** |
| POS7-ADC-19.01 | SQL Injection, |
| POS7-ADC-19.02 | Cross-Site Scripting, |
| POS7-ADC-19.03 | Cross-Site Request Forgery, |
| POS7-ADC-19.04 | Session hijacking, |
| POS7-ADC-19.05 | Command Injection, |
| POS7-ADC-19.06 | Cookie/Session Poisoning, |
| POS7-ADC-19.07 | Parameter/Form Tampering, |
| POS7-ADC-19.08 | Forceful Browsing, |
| POS7-ADC-19.09 | Brute Force Login, |
| POS7-ADC-19.10 | Web Scraping |
| POS7-ADC-19.11 | Cookie manipulation/poisoning |
| POS7-ADC-19.12 | Dynamic Parameter tampering |
| POS7-ADC-19.13 | Buffer Overflow |
| POS7-ADC-19.14 | Stealth Commanding |
| POS7-ADC-19.15 | Unused HTTP Methods |
| POS7-ADC-19.16 | Malicious File Uploads |
| POS7-ADC-19.17 | Hidden Field Manipulation |
| **POS7-ADC-20** | **Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego musi być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.** |
| **POS7-ADC-21** | **Wstrzykiwanie przez WAF dodatkowych informacji (cookie, tokeny, JavaScript, itp.), nie może powodować degradacji wydajności oferowanego urządzenia.** |
| **POS7-ADC-22** | **Wstrzykiwanie przez WAF dodatkowych informacji (cookie, tokeny, JavaScript, itp.), nie może wpływać na działanie oraz funkcjonowanie ochranianej aplikacji/serwisu.** |
| **POS7-ADC-23** | **WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http)** |
| **POS7-ADC-24** | **WAF musi blokować ataki typu Slow Loris** |
| **POS7-ADC-25** | **WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:** |
| POS7-ADC-25.01 | Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania |
| POS7-ADC-25.02 | Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser |
| POS7-ADC-25.03 | Sygnatur botów |
| **POS7-ADC-26** | **System musi umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub brute force.** |
| **POS7-ADC-27** | **System musi kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.** |
| **POS7-ADC-28** | **Musi istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia** |
| **POS7-ADC-29** | **WAF musi umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a.** |
| **POS7-ADC-30** | **WAF musi umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem** |
| **POS7-ADC-31** | **WAF musi umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a** |
| **POS7-ADC-32** | **W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu http.** |
| **POS7-ADC-33** | **WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON.** |
| **POS7-ADC-34** | **WAF musi wyświetlać stronę blokowania (błędu).** |
| **POS7-ADC-35** | **WAF musi posiadać możliwość ochrony komunikacji XML** |
| **POS7-ADC-36** | **WAF musi posiadać mechanizmy do obrony przed technikami ukrywania ataku. Muszą one wspierać/wykrywać:** |
| POS7-ADC-36.01 | Directory traversal |
| POS7-ADC-36.02 | Kodowanie typu %u |
| POS7-ADC-36.03 | Kodowanie typu IIS backslash |
| POS7-ADC-36.04 | IIS Unicode codepoints |
| POS7-ADC-36.05 | Bare byte decoding |
| POS7-ADC-36.06 | Apache whitespace |
| POS7-ADC-36.07 | Bad unescape |
| POS7-ADC-36.08 | Wstrzykiwanie komentarzy (np. <!-- -->) |
| **POS7-ADC-37** | **Urządzenie musi wspierać następujące tryby pracy:** |
| POS7-ADC-37.01 | Tryb wykrywania, logowania i blokowania ataków |
| POS7-ADC-37.02 | Tryb wykrywania i logowania ataków bez blokowania |
| POS7-ADC-37.03 | Tryb uczenia się bez blokowania |
| POS7-ADC-37.04 | Tryb uczenia się z blokowaniem i logowaniem |
| **POS7-ADC-38** | **WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach.** |
| **POS7-ADC-39** | **Narzędzia optymalizacji Web** |
| POS7-ADC-39.01 | Optymalizacja dostępu do stron web, obejmująca akcelerację przepływów, konsolidację obrazów, kompresję itp. |
| POS7-ADC-39.02 | Wykrywanie typów urządzeń i przeglądarek i dostosowywanie mechanizmów optymalizacji |
| POS7-ADC-39.03 | Optymalizacja obrazów, w tym co najmniej progresywny rendering, kompresja stratna i bezstratna |
| POS7-ADC-39.04 | Minimalizacja kodu co najmniej CSS i Javascript |
| POS7-ADC-39.05 | Optymalizacja stron startowych |
| **POS7-ADC-40** | **Zarządzanie:** |
| POS7-ADC-40.01 | SOAP-SSL |
| POS7-ADC-40.02 | API REST - programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji |
| **POS7-ADC-41** | **Rozwiązanie musi być dojrzałym, uznanym na rynku – jako potwierdzenie tej pozycji uznane będzie jego uwzględnienie w zestawieniach Gartner Magic Quadrant for Application Delivery Controllers i Web Application Firewall w ostatnich 3 latach** |

## URZĄDZENIA ADC TYP I – 2 sztuki

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 43. Wymagania dla urządzeń ADC TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ADC-42** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń ADC”** |
| **POS7-ADC-43** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-ADC-44** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-ADC-45** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-ADC-46** | **co najmniej 4 interfejsy 10GE SFP+ obsadzone wkładkami 10GBase-SR** |
| **POS7-ADC-47** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-ADC-48** | **Wymagania wydajnościowe** |
| POS7-ADC-48.01 | przepustowość L4 na poziomie co najmniej 40 Gbps |
| POS7-ADC-48.02 | przepustowość L7 na poziomie co najmniej 30 Gbps |
| POS7-ADC-48.03 | obsługa co najmniej 40.000.000 jednoczesnych połączeń L4 |
| POS7-ADC-48.04 | przepustowość szyfrowania SSL na poziomie co najmniej 8 Gbps |
| **POS7-ADC-49** | **Wymagania licencyjne** |
| POS7-ADC-49.01 | Licencja pozwalająca na uzyskanie rzeczywistej przepustowości na poziomie co najmniej 10 Gbps |
| POS7-ADC-49.02 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej trzech wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |

## URZĄDZENIA ADC TYP II – 6 sztuk

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 44. Wymagania dla urządzeń ADC TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-ADC-50** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń ADC”** |
| **POS7-ADC-51** | **Urządzenie realizowane jako rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| **POS7-ADC-52** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **POS7-ADC-53** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **POS7-ADC-54** | **co najmniej 8 interfejsów 10GE SFP+ obsadzonych wkładkami 10GBase-SR** |
| **POS7-ADC-55** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **POS7-ADC-56** | **Wymagania wydajnościowe** |
| POS7-ADC-56.01 | przepustowość L4 na poziomie co najmniej 60 Gbps |
| POS7-ADC-56.02 | przepustowość L7 na poziomie co najmniej 30 Gbps |
| POS7-ADC-56.03 | obsługa co najmniej 40.000.000 jednoczesnych połączeń L4 |
| POS7-ADC-56.04 | przepustowość szyfrowania SSL na poziomie co najmniej 20 Gbps |
| **POS7-ADC-57** | **Wymagania licencyjne** |
| POS7-ADC-57.01 | Licencja pozwalająca na uzyskanie rzeczywistej przepustowości na poziomie co najmniej 30 Gbps |
| POS7-ADC-57.02 | Obsługa logicznej segmentacji urządzenia:   * możliwość wykreowania co najmniej ośmiu wirtualnych instancji * każda instancja musi obsługiwać wszystkie dostępne usługi i zapewniać osobną konfigurację polityk i innych parametrów |

## URZĄDZENIA ADC TYP III – 17 sztuk

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 45. Wymagania dla urządzeń ADC TYP III

|  |  |  |
| --- | --- | --- |
| ***Identyfikator wymagania*** | ***Wymaganie*** | ***Opis wymagania*** |
| **POS7-ADC-58** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla urządzeń ADC”** | |
| **POS7-ADC-59** | **Urządzenie realizowane jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** | |
| **POS7-ADC-60** | **Wymagania wydajnościowe** | |
| POS7-ADC-60.01 | przepustowość L4 na poziomie co najmniej 200 Mbps | |
| POS7-ADC-60.02 | przepustowość L7 na poziomie co najmniej 100 Mbps | |
| POS7-ADC-60.03 | obsługa co najmniej 100.000 jednoczesnych połączeń L4 | |
| POS7-ADC-60.04 | przepustowość szyfrowania SSL na poziomie co najmniej 50 Mbps | |
| **POS7-ADC-61** | **Wymagania licencyjne** | |
| POS7-ADC-61.01 | Licencja pozwalająca na uzyskanie rzeczywistej przepustowości na poziomie co najmniej 200 Mbps | |

## Inne

## SZAFA RACK – 3 sztuki

| ***Identyfikator wymagania*** | ***Wymaganie*** | ***Opis wymagania*** |
| --- | --- | --- |
| RACK-01 | Wysokość | Wysokość (podana w jednostkach EIA) - 42U |
| RACK-02 | Wyposażenie | Szafa wyposażona w zdejmowane drzwi przednie i tylne zamykane na klucz, zdejmowane panele boczne oraz elementy stabilizujące, zabezpieczające szafę przed wywróceniem. Drzwi tylne dzielone. Dodatkowo wymagane jest uziemienie szafy, panele chroniące przed mieszaniem powietrza gorącego z zimnym oraz elementy ułatwiające organizację kabli w szafie. Zestaw elementów do organizacji kabli: 10 mocowań typu D (D-rings), przedni panel szczotkowy 1U, przedni panel szczotkowy 2U. |
| RACK-03 | Wymiary (wysokość x głębokość x szerokość) | 2010 mm x 1075 mm x 800 mm |
| RACK-04 | Obciążenie | Możliwe obciążenie - 1130kg |
| RACK-05 | Dodatkowe | Wymagania dodatkowe:   1. 80% perforacji drzwi przednich szafy 2. 10 lat gwarancji |
| RACK-06 | Normy | 1. Zgodność z normami EIA-310 2. Zgodność z normami RoHS |

## SERWER AUTORYZACYJNY – WYMAGANIE OGÓLNE

Tabela 46. Wymagania ogólne dla serwera autoryzacyjnego

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-AAA-01** | **Podstawowe cechy systemu** |
| POS7-AAA-01.01 | Serwer autoryzacyjny umożliwiający realizację uwierzytelnienia użytkowników i administratorów elementów infrastruktury sieciowej i bezpieczeństwa |
| POS7-AAA-01.02 | System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, w tym:   1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu 2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych |
| POS7-AAA-01.03 | System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback). |
| POS7-AAA-01.04 | System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled). |
| POS7-AAA-01.05 | System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników. |
| POS7-AAA-01.06 | System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni |
| POS7-AAA-01.07 | System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:   * dostęp do interfejsu konfiguracji urządzeń sieciowych * dostęp do interfejsu konfiguracji polityk * dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania |
| POS7-AAA-01.08 | System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP. |
| **POS7-AAA-02** | **Mechanizmy uwierzytelniania** |
| POS7-AAA-02.01 | System musi wspierać następujące protokoły uwierzytelniania i standardy:   * RADIUS, zgodnie z dokumentami:   + RFC 2865 — Remote Authentication Dial In User Service (RADIUS)   + RFC 2866 — RADIUS Accounting   + RFC 2867 — RADIUS Accounting for Tunnel Protocol Support   + RFC 2868 — RADIUS Attributes for Tunnel Protocol Support   + RFC 2869 — RADIUS Extensions   + RADIUS Proxy dla zewnętrznego serwera RADIUS * TACACS+ |
| POS7-AAA-02.02 | System musi wspierać Windows Active Directory, w tym co najmniej następujące repozytoria AD:   * Microsoft Windows Active Directory 2012 * Microsoft Windows Active Directory 2012 R2 * Microsoft Windows Active Directory 2016 |
| POS7-AAA-02.03 | System musi wspierać protokół Lightweight Directory Access Protocol (LDAP) |
| POS7-AAA-02.04 | System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym) |
| POS7-AAA-02.05 | System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC. |
| **POS7-AAA-03** | **Profilowanie urządzeń** |
| POS7-AAA-03.01 | System musi umożliwiać profilowanie (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu. |
| POS7-AAA-03.02 | System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc. |
| POS7-AAA-03.03 | System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:   * DHCP * HTTP * RADIUS * DNS * SNMP * Network Scan (NMAP lub inne narzędzie profilowania aktywnego) |
| POS7-AAA-03.04 | System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji. |
| POS7-AAA-03.05 | System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy. |
| POS7-AAA-03.06 | System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:   * Stacji robocznych pracujących z systemami Linux, MacOS, Microsoft Windows * Urządzeń mobilnych: Android, Apple, * Routerów |
| POS7-AAA-03.07 | System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń, w tym następujących informacji:   * reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci * reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt |
| **POS7-AAA-04** | **Obsługa serwerów certyfikatów CA.** |
| POS7-AAA-04.01 | System musi posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA. |
| POS7-AAA-04.02 | Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS. |
| POS7-AAA-04.03 | System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów. |
| POS7-AAA-04.04 | Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności:   * Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS * Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym * Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji * Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA |

## SERWER AUTORYZACYJNY TYP I – 2 sztuki

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 47. Wymagania dla serwera autoryzacyjnego TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-AAA-04** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla serwera autoryzacyjnego”** |
| **POS7-AAA-05** | **Rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-AAA-05.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-AAA-05.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-AAA-05.03 | obudowa przeznaczona do instalacji w szafie rack 19” |
| **POS7-AAA-06** | **Wymagania licencyjne** |
| POS7-AAA-06.01 | obsługa co najmniej 50 użytkowników |

## SERWER AUTORYZACYJNY TYP II – 2 sztuki

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 48. Wymagania dla serwera autoryzacyjnego TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-AAA-05** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla serwera autoryzacyjnego”** |
| **POS7-AAA-08** | **Rozwiązanie klasy appliance (dedykowane połączenie sprzętu i oprogramowania – niedopuszczalne maszyny wirtualne działające na ogólnodostępnym wirtualizatorze typu VMWare vSphere, Microsoft Hyper-V, Linux KVM lub równoważnych).** |
| POS7-AAA-08.01 | co najmniej dwa interfejsy GE 100/1000 |
| POS7-AAA-08.02 | zasilacz zmiennoprądowy AC 230V |
| POS7-AAA-08.03 | obudowa przeznaczona do instalacji w szafie rack 19” |
| **POS7-AAA-09** | **Wymagania licencyjne** |
| POS7-AAA-09.01 | obsługa co najmniej 2050 użytkowników |

## SERWER AUTORYZACYJNY TYP III – 2 sztuki

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 49. Wymagania dla serwera autoryzacyjnego TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-AAA-10** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla serwera autoryzacyjnego”** |
| **POS7-AAA-11** | **Realizowany jako maszyna wirtualna działająca na wirtualizatorze VMWare vSphere.** |
| **POS7-AAA-12** | **Wymagania licencyjne** |
| POS7-AAA-12.01 | obsługa co najmniej 20 użytkowników |

## Oprogramowanie monitorowania I zarządzania

## SYSTEM ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ - WYMAGANIA OGÓLNE DLA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ

Tabela 50. Wymagania ogólne dla systemu zarządzania elementami infrastruktury sieciowej

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNT-01** | **Zestaw oprogramowania do zarządzania siecią LAN i SAN** |
| **POS7-MGNT-02** | **Zarządzanie elementami sieci SAN (funkcjonalność dla każdego z elementów i całej fabryki):** |
| POS7-MGNT-03.01 | wizualizacja topologii sieci SAN |
| POS7-MGNT-03.02 | konfiguracja całej sieci (fabryki) SAN oraz poszczególnych przełączników i ich portów |
| POS7-MGNT-03.03 | uproszczone narzędzia konfiguracyjne (wizards) |
| POS7-MGNT-03.04 | narzędzia diagnostyczne łącznie analizą działania (fabryki) SAN |
| POS7-MGNT-03.05 | wizualizacja wydajności działania |
| POS7-MGNT-03.06 | wizualizacja błędów i alarmów |
| POS7-MGNT-03.07 | jednoczesne zarządzanie wieloma oddzielnymi fizycznie sieciami SAN |
| POS7-MGNT-03.08 | centralny serwer web zapewniający dostęp do informacji nt sieci SAN bez konieczności instalacji oprogramowania klienckiego |
| POS7-MGNT-03.09 | zbieranie i raportowanie danych historycznych |
| POS7-MGNT-03.10 | przekazywanie zdarzeń (events) do zdalnych kolektorów |
| POS7-MGNT-03.11 | wizualizacja połączeń SAN dla maszyn wirtualnych VM w środowisku VMWare ESXi |
| **POS7-MGNT-04** | **Zarządzanie elementami sieci LAN (funkcjonalności dla każdego z elementów i całej sieci):** |
| POS7-MGNT-04.01 | automatyczny proces rozpoznawania środowiska i topologii sieci LAN |
| POS7-MGNT-04.02 | uproszczone narzędzia konfiguracyjne (wizards) |
| POS7-MGNT-04.03 | wizualizacja topologii sieci LAN |
| POS7-MGNT-04.04 | szczegółowe informacje dla poszczególnych przełączników, w tym co najmniej:   * nazwa przełącznika * model przełącznika * adres IP interfejsu zarządzającego przełącznika * numer seryjny przełącznika * wersja firmware przełącznika * wykorzystanie CPU przełącznika * wykorzystanie pamięci przełącznika |
| POS7-MGNT-04.05 | szczegółowe informacje dla fizycznych i zagregowanych interfejsów przełącznika, w tym co najmniej:   * stan administracyjny i operacyjny interfejsu * prędkość interfejsu * MTU interfejsu * adres IP interfejsu * informacja nt. konfiguracji interfejsu |
| POS7-MGNT-04.06 | wyszukiwanie przełączników na podstawie:   * nazwy przełącznika * adresu IP * adresu MAC * numeru seryjnego |
| POS7-MGNT-04.07 | wizualizacja topologii środowiska wirtualnego VMWare dołączonego do przełączników LAN, w tym hostów, przełączników wirtualnych i maszyn wirtualnych VM |
| POS7-MGNT-04.08 | wizualizacja danych dla przełączników w formie wykresów dla co najmniej:   * wykorzystania CPU * wykorzystania pamięci * statystyk ruchu dla indywidualnych oraz agregowanych interfejsów * wykorzystania zasobów sprzętowych dla przełączników * temperatury przełącznika |
| POS7-MGNT-04.09 | konfiguracja funkcjonalności przełączników:   * PortChannel oraz wirtualny PortChannel * dodawanie, usuwanie i modyfikowanie VLAN-ów 802.1Q |
| POS7-MGNT-04.10 | definiowanie i uruchamianie samodzielnie definiowanych zadań konfiguracyjnych |
| POS7-MGNT-04.11 | zarządzanie aktualizacją firmware na przełącznikach, w tym co najmniej:   * implementacja serwera FTP/SCP z repozytorium dla poszczególnych wersji firmware * możliwość uruchamiania indywidualnego oraz grupowego procesu aktualizacji firmware na wybranych przełącznikach oraz grupach przełączników * możliwość uruchomienia aktualizacji natychmiastowo lub w zaplanowanym czasie |
| POS7-MGNT-04.12 | identyfikowanie anomalii w działaniu przełączników sieciowych LAN poprzez wskazanie:   * przełączników z wysokim stopniem wykorzystania zasobów sprzętowych i logicznych takich jak: porty fizyczne, adresy MAC, sieci VLAN, wpisy w tablicy routingu, tablice VRF, listy kontroli dostępu ACL, itp. * przełączników z alarmującym stanem środowiskowym i sprzętowym w tym:   + wysokim poziomem wykorzystania pamięci RAM   + wysokim poziomem wykorzystania pamięci Flash * przełączników z interfejsami nadającymi i odbierającymi najwięcej ruchu sieciowego oraz generującymi największą ilość błędów |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP I – 1 sztuka

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 51. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNT-05** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami infrastruktury sieciowej”** |
| **POS7-MGNT-06** | **Zarządzanie wszystkimi przełącznikami sieci LAN (6 przełączników)** |
| **POS7-MGNT-07** | **Zarządzanie wszystkimi przełącznikami sieci SAN (2 przełączniki)** |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP II – 1 sztuka

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 52. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNT-08** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami infrastruktury sieciowej”** |
| **POS7-MGNT-09** | **Zarządzanie wszystkimi przełącznikami sieci LAN (10 przełączników)** |
| **POS7-MGNT-010** | **Zarządzanie wszystkimi przełącznikami sieci SAN (4 przełączniki)** |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI INFRASTRUKTURY SIECIOWEJ TYP III – 1 sztuka

**Producent …………………..…………………………….……………….….**

**Model …………………….………………………………………………**

Tabela 53. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNT-08** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami infrastruktury sieciowej”** |
| **POS7-MGNT-09** | **Zarządzanie wszystkimi przełącznikami sieci LAN (1 przełącznik)** |
| **POS7-MGNT-010** | **Zarządzanie wszystkimi przełącznikami sieci SAN (1 przełączniki)** |

## SYSTEM ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA- WYMAGANIA OGÓLNE DLA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA

Tabela 54. Wymagania ogólne dla systemu zarządzania elementami bezpieczeństwa

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNTSEC-01** | **Zestaw urządzeń i oprogramowania do zarządzania elementami bezpieczeństwa** |
| **POS7-MGNTSEC-02** | **Zarządzanie funkcjonalnościami urządzeń realizujących funkcjonalności NGFW, NGIPS, SSL, WAF, LB, anty-malware i ochrony poczty elektronicznej – dopuszczalne jest oferowanie w ramach systemu zestawu urządzeń typu appliance i/lub elementów oprogramowania (uruchamianych na serwerach obszaru zarządzania) odpowiedzialnych za zarządzanie poszczeglnymi funkcjonalnościami (NGFW, NGIPS, SSL, WAF, LB, anty-malware, ochrony poczty elektronicznej, …). W takim przypadu należy wymienić wszystkie elementy wchodzące w skład zestawu oraz ich producentów.** |
| **POS7-MGNTSEC-03** | **Interfejs graficzny (GUI) dostępny przez standardową przeglądarkę, chroniony kryptograficznie (HTTPS).** |
| **POS7-MGNTSEC-04** | **Zarządzanie funkcjonalnościami NGFW:** |
| POS7-MGNTSEC-04.01 | definiowanie polityk dostępu i autoryzacji |
| POS7-MGNTSEC-04.02 | monitorowanie i diagnostyka elementów |
| POS7-MGNTSEC-04.03 | zarządzanie i korelacja zdarzeń |
| **POS7-MGNTSEC-05** | **Zarządzanie funkcjonalnościami NGIPS:** |
| POS7-MGNTSEC-05.01 | definiowanie polityk ochrony |
| POS7-MGNTSEC-05.02 | monitorowanie i diagnostyka elementów |
| POS7-MGNTSEC-05.03 | zarządzanie zdarzeniami |
| POS7-MGNTSEC-05.04 | informacje ogólne i szczegółowe o:   1. wykrytych hostach 2. aplikacjach 3. zagrożeniach i atakach 4. wskazaniach kompromitacji (tzw. Indication of Compromise) na podstawie:    1. zdarzeń z IPS    2. malware backdoors    3. exploit kits    4. ataków na aplikacje webowe    5. połączeń do serwerów Command'n'Control    6. wskazań eskalacji uprawnień    7. zdarzeń sieciowych    8. połączeń do znanych adresów IP Command'n'Control    9. zdarzeń związanych z malware    10. wykrytego malware    11. wykrytej infekcji dropperów |
| **POS7-MGNTSEC-06** | **Zarządzanie funkcjonalnościami sieciowego anty malware:** |
| POS7-MGNTSEC-06.01 | narzędzia szybkiej reakcji na zdarzenia - co najmniej w postaci możliwości zweryfikowania reputacji danego pliku, jeśli był on już wcześniej widziany w sieci, i określenie jego statusu w trzech stanach (czysty, neutralny, złośliwy). |
| POS7-MGNTSEC-06.02 | możliwość wysłania do globalnego centrum informacji o plikach w sposób zanonimizowany np. poprzez sumy kontrolne (SHA-256) lub inne rozwiązanie oferowane przez producenta |
| POS7-MGNTSEC-06.03 | możliwość automatycznej propagacji do systemów ochrony przed malware informacji o widzianych plikach oraz ich statusie celem ich blokowania |
| POS7-MGNTSEC-06.04 | automatyczne i niezwłoczne przesyłanie do systemów ochrony informacji o plikach, które podczas początkowej analizy otrzymały status „czysty” lub „neutralny”, a których status został obniżony do statusu „złośliwy” – tzw. blokowanie wsteczne |
| POS7-MGNTSEC-06.05 | interfejs graficzny do analizy zdarzeń i dokonywania zmian konfiguracji polityk bezpieczeństwa |
| POS7-MGNTSEC-06.06 | interfejs graficzny służący do administracji funkcji utrzymaniowych w tym:   1. ilość dostępnych zasobów 2. analiza wydajności 3. kopie zapasowe |
| **POS7-MGNTSEC-07** | **Zarządzanie funkcjonalnościami ochrony poczty elektronicznej:** |
| POS7-MGNTSEC-07.01 | definiowanie polityk   1. wielokrotne wykorzystywanie w regułach predefiniowanych elementów takich jak filtry i akcje 2. definiowanie co najmniej następujących akcji (w ramach polityki): 3. dostarczenie wiadomości z wykonaniem dodatkowych akcji:    * zmodyfikowanie tematu przesyłki    * usunięcie i/lub dodanie nagłówka X-header    * wysłanie kopii wiadomości pod wskazany adres lub adresy email    * zablokowanie wiadomości    * zapisanie wiadomości do wskazanej kolejki    * wysłanie powiadomienia, 4. budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu, niezależnie dla ruchu wychodzącego i przychodzącego z zastosowaniem co najmniej:    * domen email    * obiektów z Microsoft AD    * adresów pojedynczych użytkowników 5. tworzenie odrębnych polityk i wyjątków dla różnych użytkowników 6. tworzenie dedykowanych polityk dla tzw. „greymail” (wiadomości, które nie są kwalifikowane jako spam) |
| POS7-MGNTSEC-07.02 | generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem |
| POS7-MGNTSEC-07.03 | możliwość dostarczanie raportów w postaci plików pdf i csv |
| POS7-MGNTSEC-07.04 | możliwość dostosowania tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty |
| POS7-MGNTSEC-07.05 | zarządzanie, przeglądanie aktywności użytkowników |
| POS7-MGNTSEC-07.06 | prezentacja sumarycznej aktywności z ostatnich 24 godzin oraz podstawowych statystyk |
| POS7-MGNTSEC-07.07 | mechanizm pozwalający na przeglądanie przez chronionych użytkowników wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości z kwarantanny |
| **POS7-MGNTSEC-08** | **Zarządzanie funkcjonalnościami WAF** |
| POS7-MGNTSEC-08.01 | definiowanie polityk ochrony |
| POS7-MGNTSEC-08.02 | monitorowanie i diagnostyka elementów |
| POS7-MGNTSEC-08.03 | zarządzanie zdarzeniami |
| **POS7-MGNTSEC-09** | **Zarządzanie funkcjonalnościami Load Balancer** |
| POS7-MGNTSEC-09.01 | definiowanie polityk równoważenia ruchu |
| POS7-MGNTSEC-09.02 | monitorowanie i diagnostyka elementów |
| POS7-MGNTSEC-09.03 | zarządzanie zdarzeniami |
| **POS7-MGNTSEC-10** | **Zarządzanie funkcjonalnościami terminowania i deszyfracji SSL** |
| POS7-MGNTSEC-10.01 | definiowanie polityk terminowania i deszyfracji SSL |
| POS7-MGNTSEC-10.02 | dystrybucja certyfikatów |
| POS7-MGNTSEC-10.03 | monitorowanie i diagnostyka elementów |
| POS7-MGNTSEC-10.04 | zarządzanie zdarzeniami |
| **POS7-MGNTSEC-11** | **Funkcje modelowania aplikacji i budowy polityk bezpieczeństwa:** |
| POS7-MGNTSEC-11.01 | system na bazie zebranych danych z różnych źródeł, co najmniej przełączników CPD, firewalli musi dokonywać analizy ruchu sieciowego między usługami |
| POS7-MGNTSEC-11.02 | możliwość wykorzystywanie własnych lub zewnętrznych etykiet/tagów, które można następnie wykorzystać w budowaniu polityk (typu zakaz ruchu pomiędzy elementami oznaczonymi etykietą DEV a tymi oznaczonymi PROD) |
| POS7-MGNTSEC-11.03 | rekomendacje polityki segmentacji opartej o tzw. „white-listing”, czyli otwarcie do komunikacji tylko wymaganych i wykorzystywanych portów wymaganych do działania aplikacji |
| POS7-MGNTSEC-11.04 | wizualizacja topologii aplikacji w danym obszarze (podział na warstwy/segmenty) w przystępnej formie (application dashboard) |
| POS7-MGNTSEC-11.05 | wizualizacja mapy polityk (przepływy pomiędzy segmentami/workload z dokładnością do informacji dla warstwy L4 |
| POS7-MGNTSEC-11.06 | wsparcie dla analizy aplikacji usług opartych o maszyny wirtualne VM |
| POS7-MGNTSEC-11.07 | **Funkcje analizy i monitorowania przepływu danych dla aplikacji** |
| POS7-MGNTSEC-11.08 | możliwość monitorowania przepływu danych (network flow) pomiędzy usługami opartymi o maszyny wirtualne VM |
| POS7-MGNTSEC-11.09 | możliwość mapowania przepływu poprzez sieć fizyczną w centrum przetwarzania |
| POS7-MGNTSEC-11.10 | możliwość wskazania usług, które charakteryzują się najwyższym poziomem generowanego ruchu (top talkers) w oparciu o co najmniej:   * ilość przepływów * wolumen ruchu |
| POS7-MGNTSEC-11.11 | identyfikacja sytuacji nietypowych, statystycznie odbiegających od standardowego wzorca pracy (tzw. outliers), np. przepływy o nietypowo dużym lub małym wolumenie danych w ramach danej aplikacji |
| POS7-MGNTSEC-11.12 | możliwość przeszukiwania bazy wiedzy, z dokładnością do nazw maszyn VM, adresów IP, ilości przepływów, wolumenu ruchu, etykiet/tagów itp. |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP I – 1 sztuka

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 55. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP I

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNTSEC-13** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami bezpieczeństwa”** |
| **POS7-MGNTSEC-14** | **Zarządzanie wszystkimi urządzeniami NGFW/NGIPS strefy zewnętrznej** |
| **POS7-MGNTSEC-15** | **Zarządzanie wszystkimi urządzeniami ADC strefy zewnętrznej** |
| **POS7-MGNTSEC-16** | **Obsługa co najmniej 75 serwerów lub maszyn wirtualnych oraz wszystkich przełączników LAN w zakresie funkcji modelowania aplikacji i budowy polityk bezpieczeństwa, funkcji analizy i monitorowania przepływu danych dla aplikacji** |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP II – 1 sztuka

**Producent …………………..…………………………….……………….…**

**Model …………………….………………………………………………**

Tabela 56. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP II

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNTSEC-17** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami bezpieczeństwa”** |
| **POS7-MGNTSEC-18** | **Zarządzanie wszystkimi urządzeniami NGFW/NGIPS strefy zewnętrznej** |
| **POS7-MGNTSEC-19** | **Zarządzanie wszystkimi urządzeniami ADC strefy zewnętrznej** |
| **POS7-MGNTSEC-20** | **Obsługa co najmniej 300 serwerów lub maszyn wirtualnych oraz wszystkich przełączników LAN w zakresie funkcji modelowania aplikacji i budowy polityk bezpieczeństwa, funkcji analizy i monitorowania przepływu danych dla aplikacji** |

## INSTANCJA SYSTEMU ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA TYP III

**Producent …………………..…………………………….……………….…**

**Model …………………….………………………………………………**

Tabela 57. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP III

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-MGNTSEC-22** | **Spełnienie wszystkich wymagań określonych w sekcji „Wymagania ogólne dla systemu zarządzania elementami bezpieczeństwa”** |
| **POS7-MGNTSEC-23** | **Zarządzanie wszystkimi urządzeniami NGFW/NGIPS strefy zewnętrznej** |
| **POS7-MGNTSEC-24** | **Zarządzanie wszystkimi urządzeniami ADC strefy zewnętrznej** |
| **POS7-MGNTSEC-25** | **Obsługa co najmniej 185 serwerów lub maszyn wirtualnych oraz wszystkich przełączników LAN w zakresie funkcji modelowania aplikacji i budowy polityk bezpieczeństwa, funkcji analizy i monitorowania przepływu danych dla aplikacji** |

## System zarządzania logami

## MODUŁ KORELACJI ZDARZEŃ (SIEM)

Ilości:

* Dla strefy zewnętrznej – konsola agregująca dane, umożliwiająca obsługę co najmniej 7.500 zdarzeń na sekundę, dzienny przyrost danych na poziomie 200GB i 90-dniową retencję oraz przechowywanie danych w archiwum przez okres 21 miesięcy , konektor umożliwiający import danych ze strefy zewnętrznej za pośrednictwem jednokierunkowego (tylko odczyt) zasobu dyskowego.
* Dla strefy wewnętrznej – konektor systemu umożliwiający zbieranie i agregację danych ze strefy i ich eksport za pośrednictwem jednokierunkowego (tylko zapis) zasobu dyskowego do strefy zewnętrznej.
* Dla strefy nieprodukcyjnej – system umożliwiający odzwierciedlenie struktury stref produkcyjnych.

**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

Tabela 58. Wymagania dla modułu korelacji zdarzeń (SIEM)

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **POS7-SIEM-01** | **Platforma SIEM ma zapewnić mechanizmy nadzoru nad funkcjonowaniem systemów przetwarzania informacji w zakresie bezpieczeństwa informacji, ciągłości działania, wykrywania awarii, wykrywania anomalii i rozwiązywania problemów. Podstawowymi zadaniami dla systemu SIEM są m.in.:** |
| POS7-SIEM-01.01 | wykrywanie awarii i innych problemów na podstawie logów i metryk pozyskiwanych z urządzeń i systemów informatycznych. |
| POS7-SIEM-01.02 | weryfikacja funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych, |
| POS7-SIEM-01.03 | zapewnienie mechanizmów monitorujących pracowników i innych użytkowników infrastruktury teleinformatycznej, |
| POS7-SIEM-01.04 | podział obowiązków w zakresie monitorowania i rozliczania użytkowników uprzywilejowanych, |
| POS7-SIEM-01.05 | monitorowanie funkcjonowania aplikacji i urządzeń w celu szybszego reagowania na możliwe problemy i awarie, |
| POS7-SIEM-01.06 | zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów bezpieczenstwa, |
| POS7-SIEM-01.07 | zbieranie, zapisywania i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne. Dane muszą być́ przechowywane w sposób zapewniający ochronę ich integralności, |
| POS7-SIEM-01.08 | korelacji informacji pochodzących z różnych źródeł w celu wykrycia zaawansowanych zagrożeń i/lub eliminacji fałszywych alarmów. |
| **POS7-SIEM-02** | **Wymagania ogólne** |
| POS7-SIEM-02.01 | System musi realizować funkcjonalność systemu zarządzania informacją i zdarzeniami bezpieczeństwa SIEM. |
| POS7-SIEM-02.02 | System musi umożliwiać wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie monitorowania usług IT, wydajności aplikacji, monitorowania usług. |
| POS7-SIEM-02.03 | System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych za analizą danych obejmujące:   1. mechanizmy pobierania danych, 2. raporty, dashboardy i formularze, 3. nowe funkcje analityczne, 4. nowe sposoby wizualizacji, 5. mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent.   Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta i nie może naruszać praw autorskich. |
| POS7-SIEM-02.04 | Architektura rozwiązania musi umożliwiać rozdzielenie na osobne serwery funkcji:   1. pobierania danych, 2. przechowywania, wyszukiwania i zarządzania bazą zebranych logów, 3. warstwy analitycznej i interfejsu użytkownika. |
| **POS7-SIEM-03** | **Wymagania funkcjonalne – pozyskiwanie danych** |
| POS7-SIEM-03.01 | System musi umożliwiać pobieranie logów/zdarzeń z co najmniej z następujących systemów i aplikacji:   1. Windows 2003/2008/2012 oraz XP/7/8.x/10. 2. Linux 3. Urządzanie sieciowe Cisco, Juniper, Fortinet   Przez pozyskiwanie logów rozumie się:   1. pobranie logów i zapisanie w bazie systemu SIEM, 2. klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.) 3. normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source\_ip itp. |
| POS7-SIEM-03.02 | Rozwiązanie musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji. |
| POS7-SIEM-03.03 | System SIEM musi umożliwiać pobieranie logów co najmniej następującymi protokołami:   1. syslog UDP/TCP, 2. trap SNMP, 3. logi i informacje przechowywane w bazach danych co najmniej Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie), 4. pliki tekstowe, 5. WMI, 6. NetFlow v5 i v9, sFlow, jFlow, IPFIX,   Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów. |
| POS7-SIEM-03.04 | System SIEM musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów:   1. DHCP, 2. DNS, 3. HTTP, 4. IMAP, 5. SMTP.   Prowadzenie nasłuch musi być możliwe z dedykowanego serwera oraz z agenta zainstalowanego na stacji roboczej lub serwerze. |
| POS7-SIEM-03.05 | System musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie. |
| POS7-SIEM-03.06 | Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym. |
| POS7-SIEM-03.07 | Musi istnieć możliwość ograniczenia przepustowości wykorzystywanej przez agenta do transmisji danych. |
| POS7-SIEM-03.08 | Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie |
| POS7-SIEM-03.09 | System musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych. |
| POS7-SIEM-03.10 | Oprócz źródeł wymienionych wyżej system musi umożliwiać pobierania informacji z wykorzystaniem poniższych mechanizmów:   1. parametry życiowe urządzeń pobierane z wykorzystaniem SNMP v2c/3, 2. dane wydajnościowe Windows Performance Monitor, 3. dowolne dane WMI, 4. wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym, 5. zmiany w zawartości plików i kluczy rejestrów. 6. pliki tekstowe na zdalnych serwerach poprzez SSH, CIFS i NFS. |
| POS7-SIEM-03.11 | Rozwiązanie musi umożliwiać analizowanie logów wielolinijkowych. Maksymalny wspierany rozmiar pojedynczego logu nie może być mniejszy niż 256kB. |
| **POS7-SIEM-04** | **Wymagania funkcjonalne – normalizacja danych** |
| POS7-SIEM-04.01 | System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych. System SIEM musi pozwalać na równoległe używanie różnych sposobów normalizacji logów. |
| POS7-SIEM-04.02 | System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą XML |
| POS7-SIEM-04.03 | System musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą CEF. |
| POS7-SIEM-04.04 | System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON. |
| POS7-SIEM-04.05 | System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp. ) oraz wartości pól w cudzysłowach. |
| POS7-SIEM-04.06 | System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski” powinno tworzyć pole „user” o wartości „jkowalski”. |
| POS7-SIEM-04.07 | Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach:   1. Katalogi LDAP, 2. Bazy danych, 3. Bazy noSQL 4. Hadoop. 5. Dane geolokalizacyjne.   W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami, a wzbogacanie powinno odbywać w locie w trakcie odczytu danych z źródeł zewnętrznych. |
| POS7-SIEM-04.08 | System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót. |
| POS7-SIEM-04.09 | System musi umożliwiać analizę logów różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych muszą być konwertowane do wspólnego kodowania (UTF8 lub UTF16). |
| POS7-SIEM-04.10 | Licencja nie może ograniczać w żaden sposób liczby podłączonych urządzeń. |
| **POS7-SIEM-05** | **Wymagania funkcjonalne – wyszukiwanie i przechowywanie danych** |
| POS7-SIEM-05.01 | System SIEM musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie surowej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwe w oparciu o te same narzędzia. |
| POS7-SIEM-05.02 | System SIEM musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celi spełnienia wymagać dot. wydajności lub dostępności (zwiększenie liczby kopii danych). Klastry muszą umożliwiać funkcjonowanie w środowiskach złożonych z wielu lokalizacji, przy czym konfiguracja replikacji danych musi pozwalać na określenie, w której lokalizacji dostępne są kopie zebranych informacji |
| POS7-SIEM-05.03 | System musi samodzielnie zarządzać retencją danych. Wymagana jest obsługa co najmniej dwóch etapów życia danych: WARM i COLD. Z każdym etapem związane jest miejsce przechowywania danych. Migracja danych musi następować automatycznie po określonym czasie (wiek danych) lub osiągnięciu określonej objętości. Musi istnieć możliwość stworzenie różnych schematów retencji dla różnych typów danych. Dane COLD muszą być dostępne w ten sam sposób co dane WARM, w szczególności nie jest dopuszczalne wymaganie jakichkolwiek czynności związanych z odtwarzaniem danych COLD. |
| POS7-SIEM-05.04 | System SIEM musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych i danych COLD. Dane COLD powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością. |
| POS7-SIEM-05.05 | Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem. |
| **POS7-SIEM-06** | **Wymaganie funkcjonalne – narzędzia analityczne danych** |
| POS7-SIEM-06.01 | Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól. |
| POS7-SIEM-06.02 | System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach, jeśli są dostępne. System musi uwzględniać przy prezentacji wyniku możliwość pozyskiwania logów z urządzeń skonfigurowanych w innych strefach czasowych. |
| POS7-SIEM-06.03 | System musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być dostępne w wielu formatach – co najmniej PDF, CSV, JPG. |
| POS7-SIEM-06.04 | Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:   1. Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego), 2. Funkcje wykrywania anomalii danych liczbowych. Rozwiązania musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego. 3. Rozwiązanie musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze, 4. Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól. 5. Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%). |
| POS7-SIEM-06.05 | System SIEM musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia czy dnia tygodnia). |
| POS7-SIEM-06.06 | System SIEM musi pozwalać na akcelerację zapytań i raportów, które wykonywane są często, tak by automatycznie budował agregaty pozwalające na szybkie wykonania raportu obejmującego dowolnie długie okresy czasu. Akceleracja musi być dostępna zarówno dla raportów wbudowanych jak i własnych definiowanych przez użytkownika. Raporty takie powinny być dostępne w czasie nie przekraczającym kilku sekund od ich uruchomienia dla dowolnego okresu czasu. |
| POS7-SIEM-06.07 | System SIEM musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem:   1. tabel, 2. list zdarzeń, 3. wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), 4. map. |
| POS7-SIEM-06.08 | Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na standardowych dashboardach systemu. |
| POS7-SIEM-06.09 | Musi istnieć możliwość tworzenie interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenie ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych). |
| POS7-SIEM-06.10 | Musi istnieć możliwość definiowania akcji typu drill down związanych powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól, których dotyczy akcja drilldown. Musi istnieć możliwość przekazania parametrów metodami GET i POST. |
| POS7-SIEM-06.11 | Musi istnieć możliwość tworzenia na podstawie tego samego zapytania do bazy systemu zarówno alarmów jak i raportów. Musi istnieć możliwość utworzenia panelu dashboardu na podstawie dowolnego raportu. |
| **POS7-SIEM-07** | **Wymagania funkcjonalne – analiza zdarzeń bezpieczeństwa** |
| POS7-SIEM-07.01 | System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach) |
| POS7-SIEM-07.02 | System SIEM musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danego systemu SIEM. |
| POS7-SIEM-07.03 | Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości. |
| POS7-SIEM-07.04 | System SIEM musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie. |
| POS7-SIEM-07.05 | Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.). |
| POS7-SIEM-07.06 | System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:   1. Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych, 2. Możliwość przypisania incydentu do osoby, 3. Możliwość zmiany statusu i priorytetu incydentu, 4. Możliwość tworzenia komentarzy, 5. Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy. 6. Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki. 7. Możliwość raportowania wydajności obsługi incydentów. |
| POS7-SIEM-07.07 | System SIEM musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu. |
| POS7-SIEM-07.08 | System SIEM musi umożliwiać wzbogacanie informacji o incydentach poprzez automatyczne uruchomienie dodatkowych zapytań i raportów, które pozwolą na automatyczną ocenę wpływu lub potwierdzenie istnienie incydentu. |
| POS7-SIEM-07.09 | Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto. |
| POS7-SIEM-07.10 | Musi istnieć możliwość prezentacji opisu zasobu w postaci serwera lub stacji roboczej obejmującego: nazwę, istotność, właściciela, funkcję, kontakt do administratora nawet, jeżeli w samym logu występuje wyłączenie adres IP lub MAC tego zasobu. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane. |
| POS7-SIEM-07.11 | System SIEM musi klasyfikować ryzyko związane ze zdarzeń z uwzględnieniem danych priorytetu hosta celu zdarzenia. |
| POS7-SIEM-07.12 | System musi umożliwiać prezentację zdarzeń związanych z użytkownikiem niezależnie od tego z jakiego konta korzystał. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane. |
| POS7-SIEM-07.13 | System SIEM musi umożliwiać korzystanie z zewnętrznych subskrypcji tzw. wskaźników kompromitacji (ang. IOC). System musi wspierać dowolne subskrypcje zgodne z protokołami:   1. http, 2. ftp, 3. system musi również interpretować pliki w formacie CSV, OpenIOC, tekstowym interpretowanym z wykorzystaniem REGEX. |
| POS7-SIEM-07.14 | System SIEM musi wspierać ww. wskaźniki wobec pól reprezentujących:   1. certyfikat X509, 2. adres email, 3. nazwa pliku, 4. suma kontrolna pliku, 5. URL, 6. adres hosta lub domena, 7. adres IP, 8. nazwa procesu, 9. suma kontrolna procesu, 10. klucze rejestru, 11. nazwa usługi systemowej, 12. nazwa użytkownika. 13. musi istnieć możliwość rozbudowy funkcjonalności o nowe typy wskaźników samodzielnie przez administratora. |
| POS7-SIEM-07.15 | Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach. |
| POS7-SIEM-07.16 | System SIEM musi posiadać predefiniowane raporty raporty/dashboardy związane z zarządzaniem bezpieczeństwem, co najmniej uwzględniające następujące zagadnienia:   1. istotne zdarzenia bezpieczeństwa uwzględniające istotność zasobu informatycznego, 2. aktywność złośliwego oprogramowania, 3. aktywność użytkowników i wykorzystanie kont, 4. zmiany w zawartości krytycznych obiektów systemowych, 5. stan zainstalowanych poprawek/patchy dla oprogramowania systemowego, 6. informacje o ruchu sieciowym, 7. informacje dotyczące ataków sieciowych, 8. wykorzystanie dostępu do Internetu przez pracowników, 9. wykryte podatności na podstawie raportów skanerów podatności, 10. zmiany w konfiguracji urządzeń sieciowych, 11. aktywność użytkowników (na podstawie tożsamości), 12. raporty dotyczące obsługi incydentów przez operatorów systemu, 13. raporty dotyczące wykrycia wskaźników kompromitacji. |
| POS7-SIEM-07.17 | System SIEM musi pozwalać na definiowanie własnych i modyfikację raportów, zapytań i dashboardów dostarczonych przez producenta. |
| POS7-SIEM-07.18 | System musi umożliwiać podejmowanie automatycznych akcji lub alarmowanie. Dostępne akcje muszą obejmować:   1. utworzenie incydentu, 2. wysłanie email, 3. uruchomienie skryptu i przekazanie parametrów wywoławczych, 4. integrację z systemami klasy service-desk, 5. modyfikacja list kontrolnych, 6. rozwiązanie musi zawiera API pozwalająca na budowanie nowych akcji w tym przekazanie wybranych pól zdarzenia jako parametrów akcji. |
| **POS7-SIEM-08** | **Wymagania techniczne i bezpieczeństwa** |
| POS7-SIEM-08.01 | Komunikacja użytkownika z systemem SIEM musi odbywać się przy użyciu przeglądarki internetowej. Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight. |
| POS7-SIEM-08.02 | System nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników. |
| POS7-SIEM-08.03 | System SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu. |
| POS7-SIEM-08.04 | Rozwiązanie musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck). |
| POS7-SIEM-08.05 | Rozwiązanie musi umożliwiać uwierzytelniać i szyfrować połączenia między komponentami systemu. |
| POS7-SIEM-08.06 | Rozwiązanie musi być dojrzałym, uznanym na rynku – jako potwierdzenie tej pozycji uznane będzie jego uwzględnienie w zestawieniach Gartner Magic Quadrant for Security Information and Event Management (SIEM) w ostatnich 3 latach |

## Spis rysunków

[Rysunek 1 Komponent Projektu iSDA-2.0 7](#_Toc19024734)

## Spis tabel

[Tabela 1. Wymagania ogólne dla dostarczanych rozwiązań 29](#_Toc19094653)

[Tabela 2. Wymagania dla przełączników SAN TYP I 31](#_Toc19094654)

[Tabela 3. Wymagania dla modułów SAN SFP 16Gb 33](#_Toc19094655)

[Tabela 4. Wymagania ogólne dla przełączników LAN 33](#_Toc19094656)

[Tabela 5. Wymagania dla przełączników LAN TYP I 35](#_Toc19094657)

[Tabela 6. Wymagania dla przełączników LAN TYP II 36](#_Toc19094658)

[Tabela 7. Wymagania dla przełączników LAN TYP III 36](#_Toc19094659)

[Tabela 8. Wymagania dla przełączników LAN TYP IV 37](#_Toc19094660)

[Tabela 9. Wymagania dla modułów SFP 1000Base-T 40](#_Toc19094661)

[Tabela 10. Wymagania dla modułów SFP SX 40](#_Toc19094662)

[Tabela 11. Wymagania dla modułów SFP+ SR 40](#_Toc19094663)

[Tabela 12. Wymagania dla modułów QSFP+ SR4 40](#_Toc19094664)

[Tabela 13. Wymagania dla kabli AOC 100G 3M 41](#_Toc19094665)

[Tabela 14. Wymagania dla kabli AOC 100G 10M 41](#_Toc19094666)

[Tabela 15. Wymagania dla ogólne dla koncentratora VPN 42](#_Toc19094667)

[Tabela 16. Wymagania dla koncentratora VPN TYP I 43](#_Toc19094668)

[Tabela 17. Wymagania dla koncentratora VPN TYP II 44](#_Toc19094669)

[Tabela 18. Wymagania ogólne dla urządzeń NGFW/NGIPS 45](#_Toc19094670)

[Tabela 19. Wymagania urządzeń NGFW/NGIPS TYP I 47](#_Toc19094671)

[Tabela 20. Wymagania urządzeń NGFW/NGIPS TYP II 48](#_Toc19094672)

[Tabela 21. Wymagania urządzeń NGFW/NGIPS TYP III 49](#_Toc19094673)

[Tabela 22. Wymagania urządzeń NGFW/NGIPS TYP IV 50](#_Toc19094674)

[Tabela 23. Wymagania urządzeń NGFW/NGIPS TYP V 51](#_Toc19094675)

[Tabela 24. Wymagania urządzeń NGFW/NGIPS TYP VI 51](#_Toc19094676)

[Tabela 25. Wymagania urządzeń NGFW/NGIPS TYP VII 52](#_Toc19094677)

[Tabela 26. Wymagania urządzeń NGFW/NGIPS TYP VIII 53](#_Toc19094678)

[Tabela 27. Wymagania urządzeń NGFW/NGIPS TYP IX 53](#_Toc19094679)

[Tabela 28. Wymagania ogólne urządzeń Anty-DDoS 54](#_Toc19094680)

[Tabela 29. Wymagania urządzeń Anty-DDoS TYP I 55](#_Toc19094681)

[Tabela 30. Wymagania urządzeń Anty-DDoS TYP II 55](#_Toc19094682)

[Tabela 31. Wymagania ogólne systemu ochrony poczty elektronicznej 56](#_Toc19094683)

[Tabela 32. Wymagania systemu ochrony poczty elektronicznej TYP I 58](#_Toc19094684)

[Tabela 33. Wymagania systemu ochrony poczty elektronicznej TYP II 59](#_Toc19094685)

[Tabela 34. Wymagania ogólne oprogramowania antywirusowego/EDR dla serwerów 59](#_Toc19094686)

[Tabela 35. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP I 61](#_Toc19094687)

[Tabela 36. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP II 62](#_Toc19094688)

[Tabela 37. Wymagania oprogramowania antywirusowego/EDR dla serwerów TYP III 62](#_Toc19094689)

[Tabela 38. Wymagania ogólne systemu SANDBOX 63](#_Toc19094690)

[Tabela 39. Wymagania systemu SANDBOX TYP I 66](#_Toc19094691)

[Tabela 40. Wymagania systemu SANDBOX TYP II 67](#_Toc19094692)

[Tabela 41. Wymagania systemu SANDBOX TYP III 68](#_Toc19094693)

[Tabela 42. Wymagania ogólne dla urządzeń ADC 69](#_Toc19094694)

[Tabela 43. Wymagania dla urządzeń ADC TYP I 73](#_Toc19094695)

[Tabela 44. Wymagania dla urządzeń ADC TYP II 74](#_Toc19094696)

[Tabela 45. Wymagania dla urządzeń ADC TYP III 74](#_Toc19094697)

[Tabela 46. Wymagania ogólne dla serwera autoryzacyjnego 76](#_Toc19094698)

[Tabela 47. Wymagania dla serwera autoryzacyjnego TYP I 78](#_Toc19094699)

[Tabela 48. Wymagania dla serwera autoryzacyjnego TYP II 79](#_Toc19094700)

[Tabela 49. Wymagania dla serwera autoryzacyjnego TYP III 79](#_Toc19094701)

[Tabela 50. Wymagania ogólne dla systemu zarządzania elementami infrastruktury sieciowej 80](#_Toc19094702)

[Tabela 51. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP I 81](#_Toc19094703)

[Tabela 52. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP II 82](#_Toc19094704)

[Tabela 53. Wymagania dla systemu zarządzania elementami infrastruktury sieciowej TYP III 82](#_Toc19094705)

[Tabela 54. Wymagania ogólne dla systemu zarządzania elementami bezpieczeństwa 82](#_Toc19094706)

[Tabela 55. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP I 86](#_Toc19094707)

[Tabela 56. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP II 86](#_Toc19094708)

[Tabela 57. Wymagania dla systemu zarządzania elementami bezpieczeństwa TYP III 87](#_Toc19094709)

[Tabela 58. Wymagania dla modułu korelacji zdarzeń (SIEM) 88](#_Toc19094710)