Znak sprawy: PK XII BIA 0470.23.2021

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**CZĘŚĆ I**

***Rozbudowa posiadanego przez Zamawiającego systemu ochrony poczty oraz system sandbox opartego na rozwiązaniach firmy Fortinet oraz zabezpieczenie centralnego styku z siecią Internet***

# Słownik pojęć i skrótów

**POPD** – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

**ZOPD** – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

**OPD** – Ośrodek Przetwarzania Danych

**CPD** – Centrum Przetwarzania Danych

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania

**ITS** – infrastruktura techniczno-systemowa

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny dostarczany w ramach przedmiotowego postępowania

# Opis stanu aktualnego

## Lokalizacje centrów przetwarzania danych

Zamawiający udostępnia na potrzeby wdrożenia dwa centra przetwarzania danych:

POPD PK – centrum podstawowe zlokalizowane w Warszawie przy ulicy Postępu 3

ZOPD PK – centrum zapasowe zlokalizowane w Warszawie przy ulicy Czerniakowskiej 100

## Łącza pomiędzy centrami przetwarzania danych

Zamawiający obecnie posiada łącze pomiędzy centrami przetwarzania danych o przepustowości 2x10Gbps wykonane w technologii CWDM. Docelowo Zamawiający dokona zwiększenia przepustowości połączenia do poziomu 2x40Gbps.

Dostęp do sieci WAN-PROK i Internet jest obecnie zrealizowany w POPD. ZOPD łączy się z tymi sieciami poprzez POPD za pośrednictwem wspomnianego wyżej łącza.

## Dostęp do sieci Internet

Zamawiający udostępnia zbiorcze łącze dostępowe (punkty styku dla wszystkich jednostek organizacyjnych Prokuratury) do sieci Internet o przepustowości 2048Mbps.

## Zegar

W celu synchronizacji czasu wszystkich dostarczanych Urządzeń, Zamawiający udostępnia serwer czasu ELPROMA NTS-3000.

# Przedmiot i zakres zamówienia

## Kontekst postepowania

Zamawiający planuje stworzenie na potrzeby własne oraz podległych jednostek wysokodostępnego styku POPD, ZOPD oraz wszystkich jednostek organizacyjnych Prokuratury z siecią Internet. Rozwiązanie to będzie służyć udostępnianiu centralnych usług i systemów informatycznych dla wszystkich jednostek organizacyjnych Prokuratury oraz dla podmiotów zewnętrznych uzyskujących dostęp do udostępnianych przez Prokuraturę zasobów za pośrednictwem sieci publicznej. Obecnie Zamawiający posiada system bezpieczeństwa składający się z poniższych elementów:

1. System do zarządzania urządzeniami Fortinet - FortiManager
2. Firewalle NGFW FortiGate
3. Urządzenia FortiSandbox
4. Urządzenia FortiMail
5. Urządzenia FortiAuthenticator
6. Urządzenia FortiAnalyzer
7. Oprogramowanie FortiEDR

## Przedmiot postępowania

Przedmiotem zamówienia jest rekonfiguracja posiadanego przez Zamawiającego systemu bezpieczeństwa styku z siecią Internet poprzez:

1. Rozbudowę oraz rekonfigurację system sandbox,
2. Rozbudowę oraz rekonfigurację systemu ochrony poczty elektronicznej,
3. Dostarczenie oraz konfigurację urządzeń do ochrony styku z Internetem typu NGFW,
4. Dostarczenie oraz konfigurację urządzeń do autoryzacji użytkowników zdalnych,
5. Dostarczenie oraz konfigurację systemu centralnego zarządzania urządzeniami NGFW,
6. Dostarczenie oraz konfigurację systemu logowania,
7. Dostarczenie oraz konfigurację systemu zarządzania zdalnym dostępem VPN,
8. Dostarczenie oraz konfigurację oprogramowania EDR przeznaczonego na stacje końcowe użytkowników;

W ramach realizacji projektu zostaną zrealizowane następujące usługi:

1. Dostawa Urządzeń do lokalizacji POPD;
2. Dostawa Urządzeń do lokalizacji ZOPD;
3. Wykonanie Projektu technicznego ITS dla Środowiska Produkcyjnego w POPD i ZOPD
4. Opracowanie Scenariuszy Testów Sprzętu obejmujących scenariusze testów sprzętu dla Środowiska Produkcyjnego POPD/ZOPD
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. Warsztaty i Szkolenia.
10. Gwarancja na dostarczony sprzęt oraz oprogramowanie.
11. Wsparcie techniczne.

## Architektura warstwy fizycznej ITS

Zamawiający koncentruje usługi informatyczne udostępniane jednostkom organizacyjnym oraz obywatelom w ramach dwóch ośrodków:

* Podstawowego Ośrodka Przetwarzania Danych (POPD).
* Zapasowego Ośrodka Przetwarzania Danych (ZOPD).

W stanie docelowym architektura obu ośrodków będzie identyczna, zbudowana w oparciu o rozwiązanie chmury prywatnej. Obydwa ośrodki będą połączone łączem zapewniającym wymianę danych niezbędnych dla spełnienia wymagań niezawodnościowych oraz przełączenia eksploatacji w przypadku awarii elementów OPD. Planowane jest umożliwienie dostępu do sieci WAN-PROK i Internet niezależnie z POPD i ZOPD. W ramach przedmiotowego projektu nastąpi dostawa oraz konfiguracja urządzeń stanowiących klastry umożliwiające niezawodny i bezprzerwowy dostęp do/z sieci Internet poprzez punkty styku zlokalizowane w POPD i ZOPD wykreowane przez operatora telekomunikacyjnego.

W POPD (analogicznie w ZOPD) będą wydzielone dwie strefy bezpieczeństwa:

* + - Strefa Wewnętrzna – będą w niej umieszczone wyłącznie elementy zainstalowane w POPD/ZOPD do której będą miały dostęp wszystkie jednostki prokuratury połączone poprzez dedykowaną sieć WAN-PROK. Rozwiązania bezpieczeństwa Strefy Wewnętrznej pozwolą również na wymianę danych z instytucjami współpracującymi z prokuraturą poprzez specjalne dedykowane łącza.
		- Strefa Zewnętrzna – w której będą elementy zainstalowane w POPD/ZOPD udostępniające usługi w sieci Internet oraz umożliwiajace dostęp zdalny do wskazanych zasobów wewnętrznych dla pracowników Prokuratury.

Zrealizowane w ramach przedmiotowego projektu klastry Urządzeń w POPD i ZOPD będą stanowić uzupełniającą się i wzajemnie zabezpieczającą się parę (Active/Active, HA/DR (High Availability and DisasterRecovery)), gwarantując utrzymanie działania wszystkich usług przy braku dostępności jednego z dwóch ośrodków niezależnie od usług udostępnianych z poziomu danego OPD.

Dodatkowo Wykonawca dostarczy oraz skonfiguruje system bezpiecznego dostępu zdalnego VPN do zasobów Zamawiającego dla urzędników i prokuratorów wszystkich jednostek organizacyjnych prokuratury oraz wdroży oprogramowanie typu EDR na komputerach stacjonarnych oraz przenośnych wszystkich pracowników Prokuratury.

Całość prowadzonych prac i wdrażanych rozwiązań będzie realizowana w architekturze dwuośrodkowej – POPD i ZOPD.

# Specyfikacja produktów

## SZAFA RACK- 1 sztuka

**Producent …………………………………**

**Model …………………………………**

| ***Identyfikator wymagania*** | ***Wymaganie*** | ***Opis wymagania*** |
| --- | --- | --- |
| SZA-RACK-01 | Wysokość | Wysokość (podana w jednostkach EIA) - 42U |
| SZA-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 okablowania w szafie. Zestaw elementów do organizacji kabli: 10 mocowań typu D (D-rings), przedni panel szczotkowy 1U, przedni panel szczotkowy 2U. |
| SZA-RACK-03 | Wymiary (wysokość x głębokość x szerokość) | Wysokość : nie więcej niż 202cm Szerokość: min. 59cm , maksymalnie 61cmGłębokość: min. 118cm , maksymalnie 131cm |
| SZA-RACK-04 | Obciążenie | Możliwe obciążenie - 1130kg |
| SZA-RACK-05 | Dodatkowe | Wymagania dodatkowe:1. 80% perforacji drzwi przednich szafy
2. 10 lat gwarancji
 |
| SZA-RACK-06 | Normy | 1. Zgodność z normami EIA-310
2. Zgodność z normami RoHS
 |
| SZA-RACK-07 | Wykorzystanie | Szafa musi umożliwiać zamontowanie urządzeń, które będą dostarczone w ramach zamówienia. Wyjątkiem są urządzenia dostarczane razem z własnymi szafami. |
| SZA-RACK-08 | Kable zasilające | W przypadku, kiedy urządzenie montowane w szafie nie jest wyposażone w przewód zasilający, lub przewód zasilający ma inną wtyczkę niż gniazda w oferowanej szafie, muszą zostać dostarczone odpowiednie przewody zasilające. |
| SZA-RACK-09 | Listwy zasilające | Każda szafa wyposażona w dwie listwy zasilające, parametry listwy zasilającej przedstawione poniżej:1. Natężenie prądu - 32A/ moc nominalna 7,3kVA
2. Rodzaj wejścia - IEC 309-32A
3. Minimalna ilość i rodzaj gniazd wyjściowych:
	1. 6 gniazd IEC C-19
	2. 36 gniazd IEC C-13
 |

## URZĄDZENIA SANDBOX – 2 klastry HA

**Producent …………………………………**

**Model …………………………………**

Obecnie w sieci POPD znajdują się dwa urządzenia sandbox firmy Fortinet - FortSandbox1000F.

W ramach wdrożenia należy rozbudować klaster urządzeń w taki sposób żeby uzyskać dwa niezależne klastry zlokalizowane w POPD i ZOPD, każdy posiadający następującą wydajność (w każdej lokalizacji wykorzystać jedno urządzenie FortiSandbox1000F oraz dostarczyć dodatkowe urządzenia w celu osiągnięcia wymaganej wydajności analizy plików):

* 1. W serwerowni podstawowej klaster urządzeń powinien obsłużyć następującą wydajność:
1. Ilość maszyn wirtualnych - 150
2. Wydajność analizy plików przez system sandbox (pliki/godzina) - 3000
	1. W serwerowni zapasowej klaster urządzeń powinien obsłużyć następującą wydajność:
3. Ilość maszyn wirtualnych 75
4. Wydajność analizy plików przez system sandbox (pliki/godzina) – 1500

Jeżeli do zapewnienia poprawnej działalności klastra wymagane jest dodatkowe oprogramowanie lub urządzenie fizyczne to należy je dostarczyć i wdrożyć.

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego poniższe wymagania:

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **SANDBOX-01** | **Architektura systemu** |
| SANDBOX-01.01 | Dwa klastry urządzeń, przy czym każdy klaster (System) musi spełnić wymagania opisane poniżej. Jeżeli do zapewnienia poprawnej działalności klastra wymagane jest dodatkowe oprogramowanie lub urządzenie fizyczne to należy je dostarczyć i wdrożyć. |
| SANDBOX-01.02 | Elementy systemu powinny zostać dostarczone w postaci komercyjnej platformy (lub komercyjnych platform) sprzętowej. |
| SANDBOX-01.02 | System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji.  |
| SANDBOX-01.02 | System musi umożliwiać lokalne logowanie i raportowanie oraz współpracować z systemem centralnego logowania i raportowania. |
| SANDBOX-01.02 | Musi istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń klasy NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway), aplikacjami typu agent instalowanymi na stacjach roboczych/serwerach oraz w oparciu o interfejsy programistyczne API. W przypadku rozwiązań NGFW, SWG, SEG oraz agent system sandbox ma zapewniać aktualizację ich baz antywirusowych oraz URL. |
| SANDBOX-01.02 | System musi współpracować z dostarczanymi w ramach postępowania systemami ochrony poczty, systemami zabezpieczeń NGFW oraz agentami w tym agentami oprogramowania EDR instalowanymi na stacjach roboczych. W przypadku dostarczenia systemów różnych producentów oraz braku możliwości integracji jednego systemu sandbox ze wszystkimi wymienionymi systemami, wykonawca może dostarczyć oddzielny system sandbox do poszczególnych systemów (system ochrony poczty, system zabezpieczeń NGFW oraz agenci instalowani na stacjach roboczych). |
| SANDBOX-01.02 | W celu zapewnienia szybkiego wsparcia technicznego ze strony producenta wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcie i aktualizacje oprogramowania. |
| SANDBOX-01.02 | System musi mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia (Load Balancing). |
| **SANDBOX-02** | **System operacyjny** |
| SANDBOX-02.01 | W celu zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. |
| **SANDBOX-03** | **Parametry fizyczne systemu** |
| SANDBOX-03.01 | System musi dysponować minimum: 1. 4 portami Gigabit Ethernet RJ-45.
2. 2 gniazdami SFP+ 10 Gbps (porty wyposażone we wkładki SFP+ 10GE SR)
 |
| SANDBOX-03.02 | Redundantne zasilanie z sieci 230V/50Hz. |
| **SANDBOX-04** | **Parametry wydajnościowe** |
| SANDBOX-04.01 | System musi pozwalać na analizę w maszynach wirtualnych min. 3160 plików na godzinę. |
| SANDBOX-04.02 | System musi zapewniać możliwość uruchomienia min. 158 jednoczesnych instancji (jednoczesna analiza 158 różnych próbek w ramach „pełnego sandboxingu”) maszyn wirtualnych. |
| SANDBOX-04.03 | System musi realizować jednoczesną analizę próbek na obrazach/maszynach wirtualnych następujących systemów operacyjnych: 1. MS Office
2. Windows 7
3. Windows 8
4. Windows 10
 |
| SANDBOX-04.04 | Licencje na powyższe systemy mają być dostarczone wraz z rozwiązaniem. |
| **SANDBOX-05** | **Funkcje podstawowe i uzupełniające** |
| SANDBOX-05.01 | System musi umożliwiać „pełny sanboxing”, tzn. wykonanie w maszynie wirtualnej dla następujących rodzajów próbek znajdujących się w wiadomościach pocztowych: adres URL, dokumenty Microsoft Office, pliki wykonywalne (w tym języki skryptowe JavaScript, Visual Basic, PowerShell, bat), pliki PDF (Adobe Acrobat), pliki SWF (Adobe Flash). |
| SANDBOX-05.02 | System musi umożliwiać wgrywanie własnych obrazów systemów operacyjnych.  |
| SANDBOX-05.03 | Funkcjonalność Sandbox dla instancji Windows musi realizować co najmniej sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.  |
| SANDBOX-05.04 | System musi umożliwiać procesowanie plików o rozmiarze większym niż 200 MB.  |
| SANDBOX-05.05 | System musi umożliwiać sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR). |
| SANDBOX-05.06 | System musi umożliwiać sandboxing plików multimedialnych: .avi, .mpeg, .mp3, .mp4. |
| SANDBOX-05.07 | System musi umożliwiać skanowanie stron www z linkami URL. |
| SANDBOX-05.08 | System musi umożliwiać konfigurację czarnych i białych list dla sum kontrolnych plików. |
| SANDBOX-05.09 | System musi umożliwiać szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM. Administrator musi mieć możliwość definiowania cyklicznych raportów.  |
| SANDBOX-05.10 | System musi umożliwiać dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap. |
| SANDBOX-05.11 | System musi umożliwiać generowanie alertów podczas wykrywania zagrożeń i raportowanie ich za pomocą: Syslog, SNMP, SMTP w celu integracji z posiadanym przez Zamawiającego rozwiązaniem SIEM. |
| SANDBOX-05.12 | System musi umożliwiać zarządzanie min. przez panel WebUI za pomocą przeglądarki internetowej. |
| SANDBOX-05.13 | System musi umożliwiać skanowanie zasobów sieciowych SMB/NFS oraz kwarantanny podejrzanych plików.  |
| SANDBOX-05.14 | System musi mieć możliwość integracja z regułami YARA firm trzecich.  |
| **SANDBOX-06** | **Sygnatury, subskrypcje** |
| SANDBOX-06.01 | Bazy sygnatur wykorzystywanych przez funkcje skanujące muszą być systematycznie aktualizowane. |
| SANDBOX-06.02 | W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych w okresie obowiązywania gwarancji. |
| SANDBOX-06.03 | W ramach postępowania muszą zostać dostarczone licencje niezbędne do uruchomienia wszystkich wymaganych maszyn wirtualnych. |

## SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ – 2 klastry HA

**Producent …………………………………**

**Model …………………………………**

Obecnie w sieci prokuratury znajdują się dwa urządzenia do ochrony poczty firmy Fortinet FortMail900F.

W ramach wdrożenia należy rozbudować klaster urządzeń w taki sposób żeby uzyskać dwa niezależne klastry zlokalizowane w POPD i ZOPD, każdy posiadający następującą wydajność (w każdej lokalizacji wykorzystać jedno urządzenie FortiMail9000F oraz dostarczyć dodatkowe urządzenia w celu osiągnięcia wymaganej przepustowości):

* 1. W serwerowni podstawowej klaster urządzeń powinien obsłużyć następującą wydajność:
1. Obsługa wiadomości/godz. – 3 800 000
2. Analiza ATP wiadomości/godz. – 1 800 000
	1. W serwerowni zapasowej klaster urządzeń powinien obsłużyć następującą wydajność:
3. Obsługa wiadomości/godz. – 1 900 000
4. Analiza ATP wiadomości/godz. – 900 000

Jeżeli do zapewnienia poprawnej działalności klastra wymagane jest dodatkowe oprogramowanie lub urządzenie fizyczne to należy je dostarczyć i wdrożyć.

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego poniższe wymagania:

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **MAIL-01** | **Wymagania ogólne** |
| MAIL-01.01 | Dwa klastry urządzeń, przy czym każdy klaster (System) musi spełnić wymagania opisane poniżej. Jeżeli do zapewnienia poprawnej działalności klastra wymagane jest dodatkowe oprogramowanie lub urządzenie fizyczne to należy je dostarczyć i wdrożyć. |
| MAIL-01.02 | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników. |
| MAIL-01.03 | System musi być dostarczony pod postacią komercyjnej platformy sprzętowej (lub platform, jeśli jest to wymagane ze względu na wydajność i/lub niezawodność). Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  |
| MAIL-01.04 | Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
 |
| **MAIL-02** | **Parametry fizyczne systemu antyspamowego** |
| MAIL-02.01 | System musi być wyposażony w interfejsy:1. 4 porty Gigabit Ethernet RJ-45.
2. 2 gniazda SFP 1 Gbps (porty wyposażone we wkładki SFP 1GE SX)
 |
| MAIL-02.02 | System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 4 TB z możliwością obsługi mechanizmu RAID: 1, 5, 10, 50. |
| MAIL-02.03 | System musi posiadać wbudowany port konsoli szeregowej. |
| MAIL-02.04 | Redundantne zasilanie z sieci 230V/50Hz. |
| **MAIL-03** | **Ogólne funkcje systemu ochrony poczty** |
| MAIL-03.01 | Wsparcie dla co najmniej 800 domen pocztowych. |
| MAIL-03.02 | System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 3800000 wiadomości/godzinę w ośrodku podstawowym oraz 1900 000 w ośrodku zapasowym. |
| MAIL-03.03 | Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). |
| MAIL-03.04 | Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. |
| MAIL-03.05 | Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). |
| MAIL-03.06 | Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. |
| MAIL-03.07 | Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. |
| MAIL-03.08 | Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. |
| MAIL-03.09 | Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. |
| MAIL-03.10 | Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. |
| MAIL-03.11 | Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. |
| MAIL-03.12 | Dostęp do kwarantanny użytkownika możliwy poprzez WebMail lub IMAP. |
| MAIL-03.13 | Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. |
| MAIL-03.14 | Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. |
| MAIL-03.15 | Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. |
| MAIL-03.16 | Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. |
| MAIL-03.17 | Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention). |
| MAIL-03.18 | Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |
| MAIL-03.19 | Możliwość integracji z Microsoft 365 z wykorzystaniem API. Ochrona ma być możliwa do skonfigurowania w czasie rzeczywistym w taki sposób aby po zastosowaniu mechanizmów ochronnych (antywirusowych, antyspamowych, kontroli treści) możliwe było umieszczenie przeanalizowanego maila w odpowiednim katalogu w oparciu o werdykt (np. inbox, spam, bulk, etc.) |
| **MAIL-04** | **Kontrola antywirusowa i ochrona przed malware** |
| MAIL-04.01 | Skanowanie antywirusowe wiadomości SMTP. |
| MAIL-04.02 | Kwarantannę dla zainfekowanych plików. |
| MAIL-04.03 | Skanowanie załączników skompresowanych.  |
| MAIL-04.04 | Definiowanie komunikatów powiadomień w języku polskim. |
| MAIL-04.05 | Blokowanie załączników w oparciu o typ pliku. |
| MAIL-04.06 | Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antywirusowej. |
| MAIL-04.07 | Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (lub platformami) typu sandbox dostarczoną w ramach postępowania. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. |
| MAIL-04.08 | Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| MAIL-04.09 | Ochronę typu virus outbrake.  |
| MAIL-04.10 | Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości. |
| **MAIL-05** | **Kontrola antyspamowa** |
| MAIL-05.01 | Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. |
| MAIL-05.02 | Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. |
| MAIL-05.03 | Szczegółowa kontrola nagłówka wiadomości.  |
| MAIL-05.04 | Analiza Heurystyczna. |
| MAIL-05.05 | Współpraca z zewnętrznymi serwerami RBL, SURBL. |
| MAIL-05.06 | Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. |
| MAIL-05.07 | Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. |
| MAIL-05.08 | Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.  |
| MAIL-05.09 | Kontrola w oparciu o Greylisting oraz SPF. |
| MAIL-05.10 | Filtrowanie treści wiadomości i załączników. |
| MAIL-05.11 | Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. |
| MAIL-05.12 | Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antyspamowej. |
| MAIL-05.13 | Ochrona typu outbrake. |
| MAIL-05.14 | Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).  |
| MAIL-05.15 | Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. |
| MAIL-05.16 | Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level). |
| MAIL-05.17 | Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| **MAIL-06** | **Ochrona przed atakami na usługę poczty** |
| MAIL-06.01 | Ochrona przed atakami na adres odbiorcy (m.in. email bombing). |
| MAIL-06.02 | Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.  |
| MAIL-06.03 | Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. |
| MAIL-06.04 | Kontrola Reverse DNS (ochrona przed Anty-Spoofing). |
| MAIL-06.05 | Weryfikacja poprawności adresu e-mail nadawcy. |
| **MAIL-07** | **Funkcje logowania i raportowania** |
| MAIL-07.01 | Logowanie do zewnętrznego serwera SYSLOG. |
| MAIL-07.02 | Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. |
| MAIL-07.03 | Logowanie informacji na temat spamu oraz niedozwolonych załączników. |
| MAIL-07.04 | Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. |
| MAIL-07.05 | Możliwość analizy przebiegu sesji SMTP. |
| MAIL-07.06 | Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. |
| MAIL-07.07 | Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.  |
| MAIL-07.08 | Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.  |
| **MAIL-08** | **Funkcje pracy w trybie wysokiej dostępności (HA)** |
| MAIL-08.01 | Konfigurację HA w każdym z trybów: gateway, transparent. |
| MAIL-08.02 | Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. |
| MAIL-08.03 | Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. |
| MAIL-08.04 | Monitorowanie stanu pracy klastra. |
| MAIL-08.05 | W ramach postępowania wymaganym jest dostarczenie systemu w formie klastra realizującego funkcje podstawowe, gdzie każdy jego element charakteryzuje się parametrami fizycznymi i funkcjonalnymi opisanymi w tym dokumencie. |
| **MAIL-09** | **Aktualizacje sygnatur, dostęp do bazy spamu** |
| MAIL-09.01 | Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. |
| MAIL-09.02 | Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |
| **MAIL-10** | **Zarządzanie** |
| MAIL-10.01 | System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. |
| MAIL-10.02 | Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. |
| MAIL-10.03 | Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |
| **MAIL-11** | **Serwisy i licencje** |
| MAIL-11.01 | Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise w okresie obowiązywania gwarancji. |
| MAIL-11.02 | Usługa analizy treści typu Dynamic Adult Image w okresie obowiązywania gwarancji. |
| MAIL-11.03 | Usługa integracji z Office 365 po API w okresie obowiązywania gwarancji. |
| **MAIL-12** | **Gwarancja oraz wsparcie** |

## URZĄDZENIA NGFW – 3 sztuki urządzeń

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **NGFW-01** | **Dwa z dostarczanych urządzeń będą tworzyły klaster w POPD natomiast jedno urządzenie będzie zainstalowane w ZOPD.** |
| **NGFW-02** | **Wymagania Ogólne** |
| NGFW-02.01 | Urządzenie NGFW (System) zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7) |
| NGFW-02.02 | System musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| NGFW-02.03 | W ramach dostarczonego Systemu musi być zapewniona możliwość budowy minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. |
| NGFW-02.04 | System musi wspierać IPv4 oraz IPv6 w zakresie:1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
 |
| **NGFW-03** | **Redundancja, monitoring i wykrywanie awarii** |
| NGFW-03.01 | W przypadku Systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. |
| NGFW-03.02 | W ramach postępowania system musi zostać dostarczony w postaci redundantnej. |
| NGFW-03.03 | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
| NGFW-03.04 | Monitoring stanu realizowanych połączeń VPN.  |
| NGFW-03.05 | System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| **NGFW-04** | **Interfejsy, Dysk, Zasilanie:** |
| NGFW-04.01 | System realizujący funkcję Firewall musi dysponować minimum: 1. 12 gniazdami 10/25GE SFP+/SFP28 (8 portów obsadzone wkładkami 10GE SR)
2. 4 gniazdami 40GE QSFP+ (4 porty obsadzone wkładkami 40GE SR4)
3. 4 porty 1GE RJ45
 |
| NGFW-04.02 | System realizujący funkcję Firewall musi być wyposażony w lokalne dyski o pojemności sumarycznej minimum 2 TB. |
| NGFW-04.03 | System musi być wyposażony w redundantne zasilacze 220V/50Hz.. |
| **NGFW-05** | **Parametry wydajnościowe:** |
| NGFW-05.01 | W zakresie Firewall’a obsługa nie mniej niż 12 mln. jednoczesnych połączeń oraz co najmniej 600 000 nowych połączeń na sekundę. |
| NGFW-05.02 | Przepustowość Stateful Firewall: nie mniej niż 80 Gbps. |
| NGFW-05.03 | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 30 Gbps. |
| NGFW-05.04 | Wydajność szyfrowania IPSec VPN nie mniej niż 28 Gbps. |
| NGFW-05.05 | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 13 Gbps. |
| NGFW-05.06 | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps. |
| **NGFW-06** | **Funkcje Systemu Bezpieczeństwa:** |
| NGFW-06.01 | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Analiza ruchu szyfrowanego protokołem SSL.
 |
| **NGFW-07** | **Polityki, Firewall** |
| NGFW-07.01 | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  |
| NGFW-07.02 | System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:1. Translację jeden do jeden oraz jeden do wielu.
2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
 |
| NGFW-07.03 | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| **NGFW-08** | **Połączenia VPN** |
| NGFW-08.01 | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:1. Wsparcie dla IKE v1 oraz v2.
2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
 |
| NGFW-08.02 | System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
 |
| **NGFW-09** | **Routing i obsługa łączy WAN** |
| NGFW-09.01 | W zakresie routingu rozwiązanie powinno zapewniać obsługę:1. Routingu statycznego.
2. Policy Based Routingu.
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
 |
| **NGFW-10** | **Zarządzanie pasmem** |
| NGFW-10.01 | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
| NGFW-10.02 | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. |
| NGFW-10.03 | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **NGFW-11** | **Ochrona przed malware** |
| NGFW-11.01 | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
| NGFW-11.02 | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. |
| NGFW-11.03 | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| NGFW-11.04 | System musi współpracować z dedykowaną platformą typu Sandbox pochodzącą od tego samego producenta, która zostanie dostarczona w ramach postępowania. |
| NGFW-11.05 | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| NGFW-11.06 | System musi umożliwiać korzystanie z funkcjonalności typu virus outbreak. |
| **NGFW-12** | **Ochrona przed atakami** |
| NGFW-12.01 | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
| NGFW-12.02 | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. |
| NGFW-12.03 | Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| NGFW-12.04 | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
| NGFW-12.05 | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |
| NGFW-12.06 | Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. |
| NGFW-12.07 | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| **NGFW-13** | **Kontrola aplikacji** |
| NGFW-13.01 | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
| NGFW-13.02 | Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| NGFW-13.03 | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  |
| NGFW-13.04 | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |
| NGFW-13.05 | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.  |
| **NGFW-14** | **Kontrola WWW** |
| NGFW-14.01 | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  |
| NGFW-14.02 | W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |
| NGFW-14.03 | Filtr WWW musi dostarczać kategorii stron zabronionych prawem. |
| NGFW-14.04 | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |
| NGFW-14.05 | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. |
| NGFW-14.06 | System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. |
| NGFW-14.07 | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| NGFW-14.08 | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.  |
| **NGFW-15** | **Uwierzytelnianie użytkowników w ramach sesji** |
| NGFW-15.01 | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Urządzenia muszą integrować się z dostarczanym Serwerem Autoryzacyjnym. |
| **NGFW-16** | **Zarządzanie** |
| NGFW-16.01 | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. |
| NGFW-16.02 | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
| NGFW-16.03 | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |
| NGFW-16.04 | System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |
| NGFW-16.05 | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
| NGFW-16.06 | Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| NGFW-16.07 | Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| NGFW-16.08 | W ramach konsoli (GUI) rozwiązania firewall musi istnieć możliwość graficznej wizualizacji architektury fizycznej oraz logicznej rozwiązań pochodzących od tego samego producenta. |
| NGFW-16.09 | Musi istnieć możliwość integracji rozwiązań w oparciu o protokół SAML celem ujednolicenia logowania do poszczególnych konsol (np. dla innych firewalli, systemów logowania i zarządzania) z poziomu platformy firewall. |
| **NGFW-17** | **Logowanie** |
| NGFW-17.01 | W ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej pochodzący od tego samego producenta. |
| NGFW-17.02 | W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |
| NGFW-17.03 | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. |
| NGFW-17.04 | Musi istnieć możliwość logowania do serwera SYSLOG. |
| NGFW-17.05 | Musi istnieć możliwość automatyzacji działań w oparciu o informacje otrzymywane z systemu logowania. Podejmowane akcje mają dotyczyć nie mniej niż:1. uruchomienia skryptu
2. wysłania maila
3. zablokowania adresu IP
4. poddania kwarantannie stacji roboczej z dedykowanym oprogramowaniem klienckim pochodzącym od tego samego producenta
5. uruchomienia akcji typu webhook
 |
| **NGFW-18** | **Certyfikaty** |
| NGFW-18.01 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. |
| **NGFW-19** | **Serwisy i licencje** |
| NGFW-19.01 | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), integracja z Urządzeniami Sandbox, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.  |

## SERWER AUTORYZACYJNY – 1 klaster HA

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **AAA-01** | **klaster HA musi składać się z 2 takich samych urządzeń** |
| **AAA-02** | **Wymagania Ogólne** |
| AAA-02.01 | Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje. Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników i ich uwierzytelnianiem. |
| **AAA-03** | **System operacyjny** |
| AAA-03.01 | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa system operacyjny.  |
| **AAA-04** | **Parametry fizyczne systemu** |
| AAA-04.01 | System musi być dostarczony pod postacią zamkniętej platformy sprzętowej i być wyposażony w co najmniej: 4 interfejsy sieciowe GE RJ45, dwa interfejsy SFP obsadzone wkładkami 1GE SX oraz dysponować powierzchnią dyskową - minimum 4 TB. |
| **AAA-05** | **Wymagania ogólne** |
| AAA-05.01 | zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrznej konsoli zarządzającej. |
| AAA-05.02 | możliwość pracy w konfiguracji HA (High Availability)z trybem Active-Passive lub Active -Active w celu zwiększenia niezawodności. |
| AAA-05.03 | odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):1. obciążenia procesor(a/ów)
2. wykorzystania pamięci
3. informacji o osiąganiu granicznej liczby użytkowników
4. informacji o osiąganiu granicznej liczby grup użytkowników
5. informacji o osiąganiu granicznej liczby uwierzytelnionych użytkowników
6. przekroczeniu ilości uwierzytelnień
7. przekroczeniu ilości błędnych uwierzytelnień
 |
| AAA-05.04 | graficzną reprezentację statusu uwierzytelnień |
| AAA-05.05 | logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:1. lokalnie
2. zdalnie w oparciu o protokół syslog
 |
| AAA-05.06 | aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI) |
| AAA-05.07 | tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI):1. również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określaniem godzin i minut
2. rzeczona kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołów FTP/SFTP
 |
| AAA-05.08 | System musi wspierać lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących akcji na użytkowniku: 1. tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie
2. przechowywanie nastepujących informacji o użytkowniku:nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo
3. możliwość przechowywania przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z uzytkowników
4. możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV
 |
| AAA-05.09 | System musi wspierać konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych)
2. czasu życia hasła
3. możliwości ponownego użycia tych samych haseł
 |
| AAA-05.10 | System musi wspierać konfigurowalną politykę blokowania kont:1. w oparciu o ilość nieudanych logowań
2. czas blokowania
3. okres nieaktywności po którym konto jest blokowane
 |
| AAA-05.11 | System musi wspierać możliwość odzyskiwania haseł:1. z wykorzystaniem adresu email
2. z wykorzystaniem pytania pomocniczego
 |
| AAA-05.12 | System musi wspierać uruchomienie portalu do samodzielnej rejestracji użytkowników1. opcjonalnie tworzenie ich kont może wymagać akceptacji administratora
2. wymagana jest również opcja tworzenie kont bez ingerencji administratora
 |
| AAA-05.13 | System musi wspierać obsługę protokołu RADIUS zgodną z RFC1. wbudowany serwer RADIUS
2. konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS
3. integrację z zewnętrznymi serwerami RADIUS
 |
| AAA-05.14 | System musi wspierać obsługę protokołu LDAP1. wbudowany serwer LDAP
2. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP)
 |
| AAA-05.15 | System musi wspierać obsługę SAML - Identity Provider (IdP) proxy |
| AAA-05.16 | System musi wspierać realizacje funkcjonalności SSO (Single Sign On) w oparciu o:1. integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny
2. dedykowaną aplikację na stację robocze z systemem Windows
3. RADIUS
4. informacje uzyskiwane poprzez protokół syslog
5. dedykowany portal
 |
| **AAA-06** | **Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe** |
| AAA-06.01 | obsługę dla tokenów sprzętowych (hardware):1. ich działanie musi być realizowane w oparciu o protokół OATH wraz ze wsparciem dla TOTP oraz HOTP
2. wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania
 |
| AAA-06.02 | wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile |
| AAA-06.03 | dla tokenów na system iOS i Android wymaga się:1. aktywacji z centralnego systemu uwierzytelniania (seed provisioning)
2. możliwości konfiguracji ilości generowanych cyfr (6 lub 8)
3. generowania kodu (cyfr) co 30 lub 60 sekund
4. możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne)
5. ochrony dostępu poprzez konfigurowalny kod PIN
6. aktywacji w oparciu o kod QR
 |
| AAA-06.04 | możliwość dostarczenia kodu (wskazania tokena) poprzez:1. email (wygaśnięcie kodu w czasie 10-3600 sekund)
2. SMS (wygaśnięcie kodu wczasie 10-3600 sekund)
3. konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP
 |
| AAA-06.05 | w przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem" |
| AAA-06.06 | możliwość integracji z logowaniem do systemu Windows |
| AAA-06.07 | wsparcie dla API |
| **AAA-07** | **Wymagania funkcjonalne - 802.1x** |
| AAA-07.01 | System musi umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, wymagane są następujące protokoły:1. PEAP
2. EAP-TTLS
3. EAP-TLS
4. EAP-GTC
 |
| AAA-07.02 | wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication) |
| AAA-07.03 | zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP |
| AAA-07.04 | możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów |
| **AAA-08** | **Wymagania funkcjonalne - zarządzanie certyfikatami** |
| AAA-08.01 | własne, samodzielne CA (Certificate Authority) |
| AAA-08.02 | CA pośredniczące (intermediary CA) |
| AAA-08.03 | ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego |
| AAA-08.04 | możliwość pobrania wygenerowanych certyfikatów |
| AAA-08.05 | możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP |
| AAA-08.06 | możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP |
| AAA-08.07 | możliwość generowania certyfikatów typu wildcard |
| AAA-08.08 | realizacja CRL (Certificate Revocation List) |
| AAA-08.09 | wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560) |
| **AAA-09** | **Parametry wydajnościowe i licencyjne** |
| AAA-09.01 | uwierzytelnianie dla 40000 użytkowników |
| AAA-09.02 | obsługa 2000 tokenów (uwierzytelnianie dwuskładnikowe) |
| AAA-09.03 | 13000 klientów protokołu RADIUS (urządzeń NAS) |
| AAA-09.04 | 4000 grup |
| AAA-09.05 | 50 certyfikatów głównych (CA) |
| AAA-09.06 | 180000 certyfikatów użytkowników |
| AAA-09.07 | nielimitowaną liczbowo licencję na aplikację typu agent umożliwiającą, po zainstalowaniu jej na stacji roboczej z systemem Windows 7/10, monitorowanie informacji o aktualnie zalogowanym użytkowniku (w ramach integracji z AD) |
| **AAA-10** | **Zarządzanie** |
| AAA-10.01 | System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS |

## SYSTEM ZARZĄDZANIA ELEMENTAMI BEZPIECZEŃSTWA – 1 klaster HA

**Producent …………………………………**

**Model …………………………………**

Obecnie w sieci prokuratury znajdują się dwa systemy do zarządzania urządzeniami bezpieczeństwa firmy Fortinet - FortiManager pracujące w układzie klastra, które posiadają wystarczające licencję do dodania 3 Urządzeń NGFW opisanych w rozdziale 4.4. W przypadku dostarczenia urządzeń kompatybilnych z tym systemem nie należy dostarczać osobnego systemu do zarządzania.

W przypadku braku kompatybilności dostarczanych Urządzeń NGFW z Systemem Zarządzania Elementami Bezpieczeństwa posiadanym przez Zamawiajacego, należy dostarczyć system równoważny spełniający poniższe wymagania:

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **MGNTSEC-01** | **W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z Urządzeniami NGFW, które zostaną dostarczone w ramach postępowania** |
| **MGNTSEC-02** | **Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i wszystkimi niezbędnymi licencjami.** |
| **MGNTSEC-03** | **Dostarczony system musi składać się z dwóch identycznych urządzeń, które będą tworzyły klaster niezawodnościowy active/pasive.** |
| **MGNTSEC-04** | **Interfejsy, Dyski:** |
| MGNTSEC-04.01 | System musi dysponować co najmniej:* 4 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps (porty obsadzone wkłądkami 1GE SX)
 |
| MGNTSEC-04.02 | Powierzchnia dyskowa min. 16 TB. |
| MGNTSEC-04.03 | Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1,5,10 |
| MGNTSEC-04.04 | System musi być wyposażony w redundantne zasilanie AC 220V/50Hz |
| **MGNTSEC-05** | **Parametry wydajnościowe** |
| MGNTSEC-05.01 | System musi umożliwiać zarządzenie co najmniej 100 systemami bezpieczeństwa. |
| MGNTSEC-05.02 | Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 100 systemów. |
| MGNTSEC-05.03 | System musi być w stanie przyjmować minimum 2 GB logów na dzień. |
| **MGNTSEC-06** | **Funkcje systemu centralnego zarządzania** |
| MGNTSEC-06.01 | System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji). |
| MGNTSEC-06.02 | System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi. |
| MGNTSEC-06.03 | System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian). |
| MGNTSEC-06.04 | System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej. |
| MGNTSEC-06.05 | System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości. |
| MGNTSEC-06.06 | System musi umożliwiać zarządzenie wersjami firmware’u oraz zapewniać centralną aktualizację oprogramowania. |
| MGNTSEC-06.07 | System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń. |
| MGNTSEC-06.08 | System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia). |
| MGNTSEC-06.09 | System musi umożliwić wstawienie w dowolne miejsce polityki określonego bloku polityk bezpieczeństwa. |
| MGNTSEC-06.10 | System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami. |
| MGNTSEC-06.11 | System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach. |
| MGNTSEC-06.12 | System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM). |
| MGNTSEC-06.13 | System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh. |
| MGNTSEC-06.14 | Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |
| MGNTSEC-06.15 | Rozwiązanie musi wspierać proces provisioning'u urządzeń. |
| MGNTSEC-06.16 | Rozwiązanie musi wspierać integrację z systemem logowania, analizy i raportowania pochdzącym od tego samego producenta. W ramach integracji musi być możliwe zarządzanie wspomnianym systemem z tej samej konsoli zarządzającej. |
| **MGNTSEC-07** | **Zarządzanie** |
| MGNTSEC-07.01 | System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.  |
| MGNTSEC-07.02 | Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI. |
| MGNTSEC-07.03 | System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów. |
| MGNTSEC-07.04 | System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API. |
| MGNTSEC-07.05 | Musi istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |

## SYSTEM LOGOWANIA – 1 klaster HA

**Producent …………………………………**

**Model …………………………………**

Obecnie w sieci prokuratury znajduje się urządzenie do zbierania logów firmy Fortinet - FortiAnalyzer 1000F z licencją IoC. W ramach postępowania należy dostarczyć drugie identyczne urządzenie w celu zbudowania klastra wysokiej dostępności przy założeniu pełnej współpracy dostarczanych Urządzeń z posiadanym przez Zamawiajacego rozwiązaniem (integracja z dostarczanymi Urządzeniami NGFW, Sandbox, Serwerem Autoryzacyjnym, Systemem Ochrony Poczty Elektronicznej, Oprogramowaniem EDR, Systemem Zarządzania Zdalnym Dostępem VPN).

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego poniższe wymagania:

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LOG-01** | **W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń NGFW.** |
| **LOG-02** | **Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.** |
| **LOG-03** | **System musi zbierać logi z dostarczonych w ramach postępowania Urządzeń: NGFW, Sandbox, Serwer Autoryzacyjny, System Ochrony Poczty Elektronicznej, Oprogramowanie EDR, System Zarządzania Zdalnym Dostępem VPN.** |
| **LOG-04** | **Dostarczony system musi składać się z dwóch identycznych urządzeń, które będą tworzyły klaster niezawodnościowy active/pasive.** |
| **LOG-05** | **Interfejsy, Dyski:** |
| LOG-05.01 | System musi dysponować co najmniej:1. portami Gigabit Ethernet RJ-45.
2. 2 gniazdami SFP28 (porty obsadzone wkładkami 10GE SR)
 |
| LOG-05.02 | Rozwiązanie musi dysponować powierzchnią dyskową min. 56 TB. |
| LOG-05.03 | Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0, 1, 5, 6,10, 50, 60. |
| LOG-05.04 | System musi być wyposażony w redundantne zasilanie AC |
| **LOG-06** | **Parametry wydajnościowe** |
| LOG-06.01 | System musi być w stanie przyjmować minimum 3 TB logów na dzień. |
| LOG-06.02 | System musi być w stanie przeanalizować minimum 40000 logów na sekundę. |
| LOG-06.03 | Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 4000 systemów. |
| **LOG-07** | **Funkcje systemu centralnego logowania** |
| LOG-07.01 | Podgląd logowanych zdarzeń w czasie rzeczywistym. |
| LOG-07.02 | Możliwość przeglądania logów historycznych z funkcją filtrowania.  |
| LOG-07.03 | System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:1. Listę najczęściej wykrywanych ataków.
2. Listę najbardziej aktywnych użytkowników.
3. Listę najczęściej wykorzystywanych aplikacji.
4. Listę najczęściej odwiedzanych stron www.
5. Listę krajów , do których nawiązywane są połączenia.
6. Listę najczęściej wykorzystywanych polityk Firewall.
7. g. Informacje o realizowanych połączeniach IPSec.
 |
| LOG-07.04 | Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. |
| LOG-07.05 | Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. |
| LOG-07.06 | System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |
| **LOG-08** | **Raportowanie** |
| LOG-08.01 | Generowanie raportów co najmniej w formatach: PDF, CSV. |
| LOG-08.02 | Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. |
| LOG-08.03 | Funkcję definiowania własnych raportów.  |
| LOG-08.04 | Możliwość spolszczenia raportów. |
| LOG-08.05 | Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |
| **LOG-09** | **Korelacja logów** |
| LOG-09.01 | Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |
| LOG-09.02 | Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |
| LOG-09.03 | Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:1. Malware.
2. Aplikacje sieciowe.
3. Email.
4. IPS.
5. Traffic.
6. Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.
 |
| LOG-09.04 | System musi zapewniać funkcjonalność IoC (Indicators of Compromise) dzięki której w oparciu o analizę ruchu ma być możliwe określenie poziomu zagrożenia danego hosta/komputera w sieci. Zasilanie w IoC ma na celu dostarczenie informacji o adresach URL, domenach oraz adresach IP które mogą stanowić źródło zagrożeń. Funkcjonalność ma działać w oparciu o informację dostarczone przez tego samego producenta co system logowania oraz ma dawać możliwość analizy logów historycznych. |
| LOG-09.05 | System ma zapewniać elementy SOC poprzez możliwość konfiguracji connectorów pozwalających na integrację z innymi systemami bezpieczeństwa oraz poprzez możliwość konfiguracji scenariuszy autoamatyzacji (playbook). |
| **LOG-10** | **Zarządzanie** |
| LOG-10.01 | System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.  |
| LOG-10.02 | Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. |
| LOG-10.03 | System musi umożliwiać definiowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |
| **LOG-11** | **Licencje** |
| LOG-11.01 | Niezbędne jest dostarczenie licencji pozwalających na wykorzystanie funkcjonalności IoC (Indicators of Compromise) oraz realizację funcjonalności SOC (Security Operations Center). |

## SYSTEM ZARZĄDZANIA ZDALNYM DOSTĘPEM VPN

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **VPN-01** | **W ramach postepowania wymaganym jest dostarczenie rozwiązania do zarządzania konfiguracją dostępu VPN dla 15 000 stacji roboczych na których będą zainstalowani agenci VPN wraz z mechanizmami centralnego zarządzania.** |
| **VPN-02** | **Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.** |
| **VPN-03** | **Dostarczone rozwiązanie musi współpracować z Urządzeniami NGFW dostarczanymi w ramach postępowania.** |
| **VPN-04** | **Parametry systemu zarządzania dostępem VPN dla stacji roboczych** |
| VPN-04.01 | Kategoryzacja URL1. URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
2. Możliwość integracji z wtyczką do przeglądarki internetowej, celem analizy kategorii WWW dla ruchu SSL/HTTPS
 |
| VPN-04.02 | Analiza podatności1. Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
2. Mechanizmy pozwalające na wymuszenie aktualizacji systemu lub popularnych aplikacji
 |
| VPN-04.03 | Dostęp VPN:1. Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
2. Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
3. Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o aplikacje, przykładowo musi istnieć możliwość wykluczenia aplikacji wymagających dużej ilości pasma np.: Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting,Zoom, WebEx, YouTube
4. Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o domeny (FQDN)
5. Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
6. Mechanizmy uwierzytelniania dwuskładnikowego.
7. System musi umożliwiać zastosowanie protokołu SAML dla SSL VPN
 |
| VPN-04.04 | Funkcjonalność kontroli i blokowania urządzeń USB |
| VPN-04.05 | System musi umożliwiać określanie czy dana stacja znajduje się w wewnętrznej sieci chronionej, czy poza nią, na podstawie reguł budowanych w oparciu cechy :* 1. Parametrów DHCP
	2. Serwerów DNS
	3. Połączenia ze stacją zarządzającą
	4. Adresacją sieci
	5. Bramą domyślną (Default Gateway) (adres IP lub adres MAC)
	6. Publiczny adres IP
	7. Tunel VPN
	8. Dostępny IP za pomocą PING
	9. Typ połączenia (Ethernet lub WiFI)
 |
| VPN-04.06 | Reguły określające czy stacja należy do sieci zaufanej muszą być budowane w oparciu o różne kombinacje powyższych parametrów |
| VPN-04.07 | Reguły muszą pozwalać na przydzielenie różnych profili bezpieczeństwa zależnie od określenia przunależności do sieci zaufanej  |
| VPN-04.08 | System musi umożliwiać wysyłanie logów o ze stacji roboczych do centralnego systemu logowania i raportowania |
| VPN-04.09 | System musi umożliwiać centralne zarządzania stacjami roboczymi |
| VPN-04.10 | Poszczególne mechanizmy muszą być dostępne dla następujących wersji systemów operacyjnych Windows oraz Mac OS: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows Server 2019/2016, Mac OS X v10.14.. |
| **VPN-05** | **Parametry systemu centralnego zarządzania** |
| VPN-05.01 | Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub komercyjnej aplikacji. Wykonawca zapewni odpowiednie sprzęt oraz licencje (licencje rozwiązania, licencje systemu operacyjnego, licencje wirtualizatora itp.) w tym zakresie.  |
| VPN-05.02 | System musi umożliwiać automatyczną aktualizację oprogramowania na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej z Urządzeniami NGFW będącymi przedmiotem postępowania. |
| VPN-05.03 | System musi umożliwiać integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD. |
| VPN-05.04 | Definiowanie różnych profilów (wersji konfiguracji) dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie. |
| VPN-05.05 | Zautomatyzowany proces zarządzania aplikacja kliencką. |
| VPN-05.06 | Przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS, w których administrator może określić komponenty dla instalatora dla stacji roboczych takich jak : filtrowanie URL, analiza podatności, agent tożsamości współpracujący z centralnym serwerem uwierzytelniania (SSO) |
| VPN-05.07 | Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym. |
| VPN-05.08 | Panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych. |
| VPN-05.09 | System musi umożliwiać wyświetlanie w konsoli zarządzania informacji o stacjach roboczych, które mogą służyć do diagnozy problemów oraz stanu stacji min:* + - 1. Typ połączenia (Ethernet/Wifi)
			2. Adres IP
			3. Adres IP domyślnej bramy
			4. Adres MAC
			5. Adres MAC bramy sieciowej
			6. Nazwa sieci WiFi (SSID)
			7. Model sprzętu
			8. Producent sprzętu
			9. Informacje o procesorze
			10. Informacje o pamięci RAM
			11. Numer seryjny
			12. Informacje o dysku twardym (rozmiar)
 |
| VPN-05.10 | Możliwość wymuszenia aktualizowania systemu i aplikacji z racji wykrytych podatności na stacjach roboczych. |
| VPN-05.11 | Automatyczne wykrywanie stacji klienckich w grupach roboczych. |
| VPN-05.12 | Logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora. |
| VPN-05.13 | Generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach. |
| VPN-05.14 | Definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcją przypisywania uprawnień do elementów panelu konfiguracyjnego. |
| VPN-05.15 | Zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN. |
| VPN-05.16 | Automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji. |
| VPN-05.17 | Możliwość przeniesienia użytkownika do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi. |
| VPN-05.18 | Możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie, |
| VPN-05.19 | Możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces. |
| VPN-05.20 | Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system. |
| VPN-05.21 | Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne. |
| **VPN-06** | **Licencje oraz serwisy** |
| VPN-06.01 | System musi umożliwiać zainstalowanie i centralne zarządzanie 20 000 aplikacjami klienckimi zlokalizowanymi na stacjach roboczych i komputerach przenośnych użytkowników. |
| VPN-06.02 | Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować funkcjonalności:* 1. Filtrowanie adresów URL
	2. Możliwość zarządzania stacjami roboczymi i profilami SSL i IPSec VPN
	3. Możliwość wykonywania analizy podatności systemów operacyjnych i zainstalowanych aplikacji
	4. Centralne zarządzanie
	5. Centralne logowanie i raportowanie
	6. Kontrolę urządzeń USB
	7. Wsparcie dla uwierzytelniania wieloskładnikowego
	8. Komponentu/agenta pozwalającego na wysyłanie informacji o aktualnie zalogowanym użytkowniku w ramach infrastruktury AD, pozwalającej na budowę transparentnego mechanizmu Single Sign On.
 |
| VPN-06.03 | System musi być dostarczony w licencją na konsolę zarządzającą oraz 15000 stacji roboczych. |

## OPROGRAMOWANIE EDR

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **EDR-01** | **System ochrony i reagowania na zaawansowane zagrożenia dla urządzeń końcowych musi zapewniać kompleksową ochronę przed malware, zaawansowanymi atakami wykorzystującymi techniki opisane w modelu MITRE™ ATT&CK, ataki typu „fileless” – bez użycia plików, ataki z wykorzystaniem oprogramowania dostępnego w ramach systemu operacyjnego lub w znanych aplikacjach tzw. „LOLBAS”. System musi potrafić zarówno wykrywać zagrożenia na poszczególnych etapach infekcji jak i mieć możliwość granularnego reagowania na wykryte incydenty zależnie od poziomu u klasyfikacji danego zagrożenia.**  |
| **EDR-02** | **Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i wszystkimi niezbędnymi licencjami.** |
| **EDR-03** | **Wsparcie dla systemów operacyjnych** |
| EDR-03.01 | System musi wspierać ochronę następujących systemów operacyjnych (dostarczać agenty działające na poniższych systemach operacyjnych):1. Systemy Windows 10/8/8.1/7/Server 2016/Server 2019.
2. Systemy Apple MacOS
3. Systemy Linux – minimum Redhat, SUSE, Ubuntu)
 |
| **EDR-04** | **Zarządzanie instalacją i aktualizacją agentów** |
| EDR-04.01 | Możliwość instalacji agenta poprzez SCCM, JAMF i RHEL Satellite |
| EDR-04.02 | Możliwość aktualizacji/zmiany wersji agenta z poziomu konsoli zarządzania bez udziału użytkownika hosta końcowego  |
| EDR-04.03 | System musi dostarczać możliwość kreowania instalatorów zawierających parametry umożliwiające podłączenie się danego agenta do określonej grupy hostów oraz danej instancji systemu zarządzającego |
| EDR-04.04 | Podłączanie się do systemu zarządzającego musi wymagać podania hasła w postaci parametru – bez podania poprawnego hasła nie może być możliwości podłączenia się do systemu zarządzania |
| **EDR-05** | **Wpływ agentów na zasoby urządzenia końcowego** |
| EDR-05.01 | Poziom zużycia pamięci RAM dla procesów agenta musi wynosić średnio poniżej 200MB |
| EDR-05.02 | Poziom średni zużycia procesora (CPU) dla procesów agenta musi wynosić średnio do 1% |
| EDR-05.03 | Zainstalowane oprogramowanie nie może zajmować więcej niż 200MB przestrzeni na dysku urządzenia końcowego  |
| **EDR-06** | **Wykrywanie zagrożeń** |
| EDR-06.01 | System musi umożliwiać agentowi wykrywanie i reagowanie na zagrożenia w przypadku odłączenia od sieci (offline) i od innych elementów system |
| EDR-06.02 | System musi umożliwiać wykrywanie podejrzanych aktywności dla działających, uruchamianych i zatrzymywanych procesów oraz w ramach interakcji pomiędzy procesami. |
| EDR-06.03 | System musi umożliwiać analizę i odzwierciedlanie informacji o parametrach z jakimi został wykonany dany proces (np. parametry z linii poleceń) |
| EDR-06.04 | System musi umożliwiać wykrywanie złośliwych zmian w rejestrach co najmniej w kontekście śledzonego wykonania danego procesu |
| EDR-06.05 | System musi umożliwiać wykrywanie żądań DNS wysyłanych z chronionej stacji |
| EDR-06.06 | System musi umożliwiać wykrywanie podejrzanej aktywności związanej z używaniem dynamicznie ładowanych bibliotek DLL |
| EDR-06.07 | System musi potrafić identyfikować podejrzane zachowanie użytkownika jak i samej stacji końcowej |
| EDR-06.08 | System musi posiadać zintegrowane informacje na temat zagrożeń bezpieczeństwa (tzw. Threat Intelligence) pozwalające na dokładniejszą analizę zagrożenia |
| EDR-06.09 | System musi stosować matrycę MITRE™ ATT&CK dla wykrywanych naruszeń polityki bezpieczeństwa |
| EDR-06.10 | System musi mieć możliwość wykorzystanie baz znaczników IoC (Indication of Compromise) dla min. adresów IP, domen, nazw plików, hashy plików. |
| EDR-06.11 | System musi wykrywać znane zagrożenia |
| **EDR-07** | **Prewencja** |
| EDR-07.01 | System musi umożliwiać wykrywać i kategoryzować urządzenia IoT w bezpośrednim sąsiedztwie sieciowym danego agenta |
| EDR-07.02 | System musi umożliwiać blokowanie wykonania się złośliwych plików wykonywalnych i bibliotek DLL |
| EDR-07.03 | System musi umożliwiać zablokowanie połączeń sieciowych zewnętrznych jak i wewnętrznych wykonywanych przez złośliwe oprogramowanie |
| EDR-07.04 | System musi umożliwiać blokowanie manipulacji plikami przez złośliwe oprogramowanie: tworzenie, edycję, usuwanie) |
| EDR-07.05 | System musi umożliwiać blokowanie wykonywaniasię złośliwych plików wykonywalnych i bibliotek DLL |
| EDR-07.06 | System musi umożliwiać zastosowywanie list blokujących jak i zezwalających dla danych:1. Hashy (funkcji skrótu) plików w formatach MD5, SHA1, SHA256
2. Nazw plików
3. Ścieżek plików
4. Aplikacji z uwzględnieniem nazwy, wersji i producenta
 |
| **EDR-08** | **Zarządzanie fałszywymi alarmami (False Positives)** |
| EDR-08.01 | System musi umożliwiać ręczne zarządzanie fałszywymi alarmami poprzez możliwość oznaczania źle sklasyfikowanej aktywności, celem poprawnego wykrywania w przyszłości |
| EDR-08.02 | System musi posiadać mechanizm automatycznej reklasyfikacji fałszywych alarmów (False Positives) i przeciwdziałać błędnemu ich wykrywaniu w przyszłości |
| **EDR-09** | **Analiza historyczna zagrożeń** |
| EDR-09.01 | System musi umożliwiać wyszukiwanie oznak ataków w zebranych informacjach bazując min, na plikach, nazwach komputerów, adresach IP. Wyniki muszą być dostępne w czasie poniżej 5 minut. |
| EDR-09.02 | Dane historyczne metadanych zebranych z urządzeń muszą być dostępne do analizy okresu z minimum 6 ostatnich miesięcy |
| EDR-09.03 | Dane do analizy muszą pochodzić bezpośrednio z urządzeń końcowych |
| EDR-09.04 | System musi umożliwiać pobieranie zrzutów pamięci ze urządzeń końcowych |
| EDR-09.05 | System musi posiadać interfejs API pozwalający na śledzenie wykrytych incydentów oraz prowadzonych analiz zagrożeń z uwzględnieniem takich parametrów jak:* 1. Adres IP
	2. Nazwa hosta
	3. Użytkownik
	4. Data
	5. Ilość wystąpień danego zdarzenia
	6. Klasyfikacja aktywności
 |
| **EDR-10** | **Reagowanie na incydenty bezpieczeństwa** |
| EDR-10.01 | Incydenty bezpieczeństwa muszą być klasyfikowane w min. następujące grupy:* 1. Złośliwe
	2. Podejrzane
	3. Niestandardowe – wymagające głębszej analizy
	4. Niechciane tzw. PUP – Potential Unwanted Programs
	5. Prawdopodobnie bezpieczne zachowanie
 |
| EDR-10.02 | W ramach każdej klasy zagrożeń musi istnieć możliwość zastosowania lub nie poniższej reakcji lub działania ograniczającego wpływ incydentu na bezpieczeństwo:1. Możliwość zabicia/zatrzymania procesu
2. Możliwość usunięcia pliku
3. Możliwość przywrócenia konfiguracji/stanu przed wykonaniem się danego zagrożenia
4. Automatyczne wprowadzenie hosta w stan izolacji sieciowej – zgodnie z konfigurowalna polityką dostępu do sieci
 |
| EDR-10.03 | Możliwość dynamicznej zmiany grupy agenta na inną, gdzie zostały przypisane polityki bezpieczeństwa o większych obostrzeniach |
| EDR-10.04 | Automatyczne blokowanie adresu IP z którym łączy się podejrzany proces na zewnętrznym urządzeniu firewall. |
| EDR-10.05 | W ramach reakcji na incydenty musi istnieć możliwość powiadamiania innych systemów za pomocą:* 1. Wysłania wiadomości pocztowej e-mail ze szczegółami zdarzenia
	2. Wysłania informacji za pomocą protokołu SYSLOG
	3. Możliwości wysłania informacji do zewnętrznego systemu zawierającego w załączeniu dane w postaci XML lub JSON umożliwiające automatyczne założenie ticketu.
 |
| EDR-10.06 | Wszystkie powyższe akcje muszą być konfigurowalne per każda klasa zagrożenia. |
| EDR-10.07 | Musi być możliwość zastosowania wszystkich akcji jednocześnie w ramach danej klasy zagrożenia (np. izolacja, wysłanie powiadomienia SYSLOG, usunięcie pliki i zablokowanie niebezpiecznego adresu IP na urządzeniu Firewall) |
| EDR-10.08 | System musi umożliwiać blokowanie adresów docelowych wykrytych w ramach danego incydentu na różnych urządzeniach firewall, z możliwością wyboru lokalizacji. |
| EDR-10.09 | Polityka reagowania na zagrożenia i incydenty bezpieczeństwa musi umożliwiać jej rozróżnienie dla poszczególnych grup agentów |
| **EDR-11** | **Określanie powierzchni ataku** |
| EDR-11.01 | Wykrywanie i katalogowanie w czasie rzeczywistym wersji aplikacji komunikujących się za pomocą sieci |
| EDR-11.02 | Wykrywanie urządzeń IoT w sieci gdzie znajdują się chronione hosty |
| EDR-11.03 | Wykrywanie innych hostów w sieci, gdzie nie ma zainstalowanego agenta  |
| **EDR-12** | **Zarządzanie podatnościami** |
| EDR-12.01 | System musi umożliwiać wykrywanie podatności w aplikacjach, które komunikują się za pomocą sieci z urządzeniami zewnętrznymi. |
| EDR-12.02 | Musi istnieć możliwość ograniczenia ryzyka dla konkretnej podatnej wersji aplikacji poprzez automatyczne ograniczenie możliwości komunikacji, na podstawie reguł bazujących na aktualizowanych informacjach CVE. |
| **EDR-13** | **Wykrywanie zaawansowanych scenariuszy ataków:** |
| EDR-13.01 | System musi działać w oparciu o mechanizmy analizy zachowań procesów i wywołań funkcji systemowych, wsparte sztuczną inteligencją, w szczególności działającymi mechanizmami opartymi o modele matematyczne algorytmów uczenia maszynowego (Machine Learning) |
| EDR-13.02 | Uczenie maszynowe musi być wykorzystywane zarówno w analizie zachowań procesów jak i w analizie samych plików |
| EDR-13.03 | System musi wykrywać i umożliwiać reakcję w locie na znane zagrożenia bazując na ich zachowaniu oraz reputacji, w szczególności:* 1. Możliwość blokowania i reagowania w ramach sekwencji wykonania danego zagrożenia bazując na heurystyce zachowań (np. podczas próby szyfrowania plików przez zagrożenie typu ransomware)
	2. Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total lub równoważna dostarczana producenta)
	3. Możliwość wykrywania zagrożeń typu RAT (Remote Acces Trojan) na podstawie zachowań
	4. Wykrywanie zagrożeń musi umożliwiać konfiguracyjnie zarówno blokowanie uruchomienia danego pliku, jak i możliwość blokowania złośliwych akcji po uruchomieniu się danego zagrożenia
	5. System musi umożliwiać blokowanie złośliwych urządzeń USB należących do innych niż dozwolone przez politykę klas
	6. System musi umożliwiać logowanie dostępu urządzeń USB mających interakcję z systemem operacyjnym
	7. System musi umożliwiać wykrywanie i blokowanie podejrzanej aktywności w interpreterach języków skryptowych takich jak min:
		1. Powershell
		2. CScript
		3. Python
		4. Makra pakiety Microsoft Office
 |
| **EDR-14** | **Architektura rozwiązania** |
| EDR-14.01 | Centralne zarządzanie za pomocą przeglądarki internetowej poprze WebUI |
| EDR-14.02 | Dostęp do interfejsu API |
| EDR-14.03 | System zarządzania musi umożliwiać integrację z usługa katalogową Active Directory oraz rozwiązaniami Two Factor Authentication i rozwiązaniami typu SSO (Single sign On) |
| EDR-14.04 | System zarządzania musi umożliwiać granuralną kontrole opartą o predefiniowane role oraz wparcie dla modelu RBAC |
| EDR-14.05 | Agent systemu musi być zabezpieczony przed próbami deinstalacji z poziomu użytkownika oraz innych złośliwych procesów |
| EDR-14.06 | Skalowanie rozwiązania musi pozwalać na :* 1. Centralne zarządzanie
	2. Lokalne realizowanie polityki bezpieczeństwa (np. w przypadku braku dostępu do systemu zarządzania przez jedną z lokalizacji) poprzez dedykowane komponenty znajdujące się w poszczególnych strefach
	3. Centralny rejestr zdarzeń wykorzystywanych
	4. Możliwość wyniesienia elementów do chmury lub instalację w środowisku zamkniętym
	5. Komponenty systemu (poza agentami) muszą być dostarczone w formie virtual appliance (system + software wspierane przez jednego producenta).
 |
| **EDR-15** | **Zgodność z normami:** |
| EDR-15.01 | Dostarczony system musi posiadać zgodność z PCI DSS |
| EDR-15.02 | Dostarczony system musi posiadać zgodność z HIPAA |
| EDR-15.03 | Dostarczony system musi posiadać zgodność z GDPR |
| **EDR-16** | **Integracja rozwiązania z innymi komponentami** |
| EDR-16.01 | System musi udostępniać API, za pomocą którego można wykonywać operacje zarządzania, konfiguracji polityki oraz wprowadzania końcówek w stan izolacji. |
| EDR-16.02 | Wymagane jest dostarczenie w ramach postępowania dokumentacji do API |
| EDR-16.03 | System musi umożliwiać interakcję z urządzeniami typu Firewall, co najmniej umożliwiając blokowanie adresów IP, z którymi komunikuje się złośliwe oprogramowanie |
| EDR-16.04 | System musi umożliwiać integrację z rozwiązaniem typu sandbox działającego lokalnie (on premise) będącym przedmiotem zamówienia |
| EDR-16.05 | System musi umożliwiać integrację z systemami typu SIEM w tym posiadanym przez Zamawiającego rozwiązaniem Splunk |
| EDR-16.06 | System musi umożliwiać integrację z systemami ticketowymi |
| **EDR-17** | **Licencje oraz serwisy** |
| EDR-17.01 | W ramach postępowania zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące co najmniej następujące funkcjonalności:1. Możliwość instalacji wszystkich komponentów rozwiązania w infrastrukturze Zamawiającego (on-prem) oraz w środowiskach zamkniętych (air gap)
2. Dostęp do baz zagrożeń bezpieczeństwa – Threat Intelligence
3. Możliwość analizy incydentów tzw. Threat Hunting.
4. Aktualizacje baz zagrożeń CVSS
 |
| EDR-17.02 | W ramach dostarczanego rozwiązania muszą być dostarczone subskrybcje lub licencje pozwalające na ochronę 20000 użytkowników w okresie obowiązywania gwarancji. Rozwiązanie dostarczane w modelu on-premise. |

## PRZEŁĄCZNIK LAN SZKIELETOWY W STREFIE WEWNĘTRZNEJ- 2 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LAN-01** | **Funkcjonalności warstwy L2:** |
| LAN-01.01 | Trunking IEEE 802.1Q VLAN;  |
| LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree  |
| LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach  |
| LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN-02** | **Funkcjonalności warstwy L3** |
| LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-02.02 | Routing w oparciu o trasy statyczne |
| LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6.  |
| LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN-02.05 | VRRP v3 |
| LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **LAN-03** | **Sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit** |
| **LAN-04** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| LAN-04.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN-04.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN-04.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN-04.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| 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) |
| 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). |
| **LAN-05** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-05.01 | layer 2 IEEE 802.1p (CoS); |
| LAN-05.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-05.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p;  |
| LAN-05.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-05.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-05.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-05.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-05.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN-06** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-06.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-06.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| 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); |
| LAN-06.04 | ACL oparte o VLAN-y (VACL); |
| LAN-06.05 | ACL oparte o porty (PACL); |
| LAN-06.06 | DHCP Snooping |
| LAN-06.07 | ARP Inspection |
| LAN-06.08 | IP Source Guard |
| LAN-06.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| **LAN-07** | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| LAN-07.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-07.02 | sFlow lub netFlow |
| LAN-07.03 | IEEE 802.1ab LLDP |
| LAN-07.04 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-07.05 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-07.06 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN-07.07 | Network Time Protocol (NTP); |
| LAN-07.08 | ping, traceroute |
| **LAN-08** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-08.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-09** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **LAN-10** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **LAN-11** | **Przełącznik posiada:** |
| LAN-11.01 | minimum 36 portów 40/100GE definiowanych za pomocą wkładek QSFP |
| LAN-11.02 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **LAN-12** | **Parametry wydajnościowe:** |
| LAN-12.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN-12.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| LAN-12.03 | obsługiwana łączna przepływność (pasmo) min. 7,2 Tbps |
| LAN-12.04 | Bufor minimum 40MB |
| LAN-12.05 | obsługiwana łączna przepustowość pakietowa przełącznika min. 2,4 Bpps |
| LAN-12.06 | opóźnienie przełączania pakietów nie większe niż 1 µs  |

## PRZEŁĄCZNIK LAN SZKIELETOWY/DOSTĘPOWY W STREFIE ZEWNĘTRZNEJ- 2 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LAN-01** | **Funkcjonalności warstwy L2:** |
| LAN-01.01 | Trunking IEEE 802.1Q VLAN;  |
| LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree  |
| LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach  |
| LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN-02** | **Funkcjonalności warstwy L3** |
| LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-02.02 | Routing w oparciu o trasy statyczne |
| LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6.  |
| LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN-02.05 | VRRP v3 |
| LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **LAN-03** | **Sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MACSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit** |
| **LAN-04** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| LAN-04.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN-04.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN-04.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN-04.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| 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) |
| 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). |
| **LAN-05** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-05.01 | layer 2 IEEE 802.1p (CoS); |
| LAN-05.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-05.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p;  |
| LAN-05.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-05.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-05.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-05.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-05.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN-06** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-06.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-06.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| 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); |
| LAN-06.04 | ACL oparte o VLAN-y (VACL); |
| LAN-06.05 | ACL oparte o porty (PACL); |
| LAN-06.06 | DHCP Snooping |
| LAN-06.07 | ARP Inspection |
| LAN-06.08 | IP Source Guard |
| LAN-06.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| LAN-07 | Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika: |
| LAN-07.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-07.02 | sFlow lub netFlow |
| LAN-07.03 | IEEE 802.1ab LLDP |
| LAN-07.04 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-07.05 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-07.06 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN-07.07 | Network Time Protocol (NTP); |
| LAN-07.08 | ping, traceroute |
| **LAN-08** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-08.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-09** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **LAN-10** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **LAN-13** | **Przełącznik musi posiadać:** |
| LAN-13.01 | minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej |
| 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 |
| LAN-13.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **LAN-14** | **Parametry wydajnościowe:** |
| LAN-14.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN-14.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| LAN-14.03 | obsługiwana łączna przepływność (pasmo) min. 4,8Tbps |
| LAN-14.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 2,5 Bpps |
| LAN-14.05 | opóźnienie przełączania pakietów nie większe niż 1 µs  |
| LAN-14.06 | Bufor minimum 40MB |

## PRZEŁĄCZNIK LAN DOSTĘPOWE W STREFIE WEWNĘTRZNEJ - 4 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LAN-01** | **Funkcjonalności warstwy L2:** |
| LAN-01.01 | Trunking IEEE 802.1Q VLAN;  |
| LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree  |
| LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach  |
| LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN-02** | **Funkcjonalności warstwy L3** |
| LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-02.02 | Routing w oparciu o trasy statyczne |
| LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6.  |
| LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN-02.05 | VRRP v3 |
| LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| LAN-03 | Mechanizmy związane z funkcjonalnością VXLAN: |
| LAN-03.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN-03.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN-03.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN-03.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| LAN-03.05 | 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) |
| LAN-03.06 | obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). |
| **LAN-04** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-04.01 | layer 2 IEEE 802.1p (CoS); |
| LAN-04.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-04.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p;  |
| LAN-04.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-04.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-04.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-04.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-04.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN-05** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-05.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-05.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| LAN-05.03 | 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); |
| LAN-05.04 | ACL oparte o VLAN-y (VACL); |
| LAN-05.05 | ACL oparte o porty (PACL); |
| LAN-05.06 | DHCP Snooping |
| LAN-05.07 | ARP Inspection |
| LAN-05.08 | IP Source Guard |
| LAN-05.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| **LAN-06** | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| LAN-06.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-06.03 | sFlow lub netFlow |
| LAN-06.04 | IEEE 802.1ab LLDP |
| LAN-06.05 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-06.06 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-06.07 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN-06.08 | Network Time Protocol (NTP); |
| LAN-06.09 | ping, traceroute |
| **LAN-07** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-07.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-08** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **LAN-09** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **LAN-10** | **Przełącznik musi posiadać:** |
| LAN-10.01 | minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej |
| LAN-10.02 | minimum 6 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 |
| LAN-10.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **LAN-11** | **Parametry wydajnościowe:** |
| LAN-11.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN-11.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| LAN-11.03 | obsługiwana łączna przepływność (pasmo) min. 3,6Tbps |
| LAN-11.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 1,2 Bpps |
| LAN-11.05 | opóźnienie przełączania pakietów nie większe niż 1 µs  |
| LAN-11.06 | Bufor minimum 40MB |

## PRZEŁĄCZNIK LAN DO STYKU Z SIECIĄ INTERNET/WAN/TRANSIT - 12 sztuk

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **LAN-01** | **Funkcjonalności warstwy L2:** |
| LAN-01.01 | Trunking IEEE 802.1Q VLAN;  |
| LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree  |
| LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach  |
| LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN-02** | **Funkcjonalności warstwy L3** |
| LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-02.02 | Routing w oparciu o trasy statyczne |
| LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6.  |
| LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN-02.05 | VRRP v3 |
| LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **LAN-03** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| LAN-03.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN-03.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN-03.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN-03.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| LAN-03.05 | 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) |
| LAN-03.06 | obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). |
| **LAN-04** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-04.01 | layer 2 IEEE 802.1p (CoS); |
| LAN-04.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-04.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p;  |
| LAN-04.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-04.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-04.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-04.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-04.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN-05** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-05.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-05.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| LAN-05.03 | 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); |
| LAN-05.04 | ACL oparte o VLAN-y (VACL); |
| LAN-05.05 | ACL oparte o porty (PACL); |
| LAN-05.06 | DHCP Snooping |
| LAN-05.07 | ARP Inspection |
| LAN-05.08 | IP Source Guard |
| LAN-05.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| **LAN-06** | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| LAN-06.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-06.02 | Openflow 1.3 |
| LAN-06.03 | sFlow lub netFlow |
| LAN-06.04 | IEEE 802.1ab LLDP |
| LAN-06.05 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-06.06 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-06.07 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN-06.08 | Network Time Protocol (NTP); |
| LAN-06.09 | ping, traceroute |
| **LAN-07** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-07.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-08** | **zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej** |
| **LAN-09** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **LAN-10** | **Przełącznik musi posiadać:** |
| LAN-10.01 | minimum 24 porty 1/10/25GE definiowanych za pomocą wkładek SFP bezpośrednio w obudowie przełącznika lub na karcie liniowej z możliwością rozbudowy licencyjnej do 48 portów. |
| LAN-10.02 | minimum 6 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 |
| LAN-10.03 | dedykowany interfejs GE 100/1000 na potrzeby zarządzania |
| **LAN-11** | **Parametry wydajnościowe:** |
| LAN-11.01 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN-11.02 | urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| LAN-11.03 | obsługiwana łączna przepływność (pasmo) min. 3,6Tbps |
| LAN-11.04 | obsługiwana łączna przepustowość pakietowa przełącznika min. 1,2 Bpps |
| LAN-11.05 | opóźnienie przełączania pakietów nie większe niż 1 µs  |
| LAN-11.06 | Bufor minimum 40MB |

## SYSTEM ZARZĄDZANIA PRZEŁĄCZNIKAMI LAN/SAN– STREFA WEWNĘTRZNA/ZEWNĘTRZNA

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **MGNT-01** | **Zestaw oprogramowania do zarządzania siecią LAN.** |
| **MGNT-02** | **Zarządzanie elementami sieci LAN (funkcjonalności dla każdego z elementów i całej sieci):** |
| MGNT-02.01 | automatyczny proces rozpoznawania środowiska i topologii sieci LAN |
| MGNT-03.02 | uproszczone narzędzia konfiguracyjne (wizards) |
| MGNT-02.03 | wizualizacja topologii sieci LAN  |
| MGNT-02.04 | 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
 |
| MGNT-02.05 | 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
 |
| MGNT-02.06 | wyszukiwanie przełączników na podstawie:* nazwy przełącznika
* adresu IP
* adresu MAC
* numeru seryjnego
 |
| MGNT-02.07 | wizualizacja topologii środowiska wirtualnego VMWare dołączonego do przełączników LAN, w tym hostów, przełączników wirtualnych i maszyn wirtualnych VM |
| MGNT-02.08 | 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
 |
| MGNT-02.09 | konfiguracja funkcjonalności przełączników:* PortChannel oraz wirtualny PortChannel
* dodawanie, usuwanie i modyfikowanie VLAN-ów 802.1Q
 |
| MGNT-02.10 | definiowanie i uruchamianie samodzielnie definiowanych zadań konfiguracyjnych |
| MGNT-02.11 | 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
 |
| MGNT-02.12 | 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
 |
| **MGNT-03** | **Zarządzanie wszystkimi dostarczanymi przełącznikami sieci LAN w strefie wewnętrznej (18 przełączników).****Zamawiający udostępni na potrzeby instancji środowisko bazujące na VMWare vSphere, nie więcej niż 8 vCPU, 12 GB vRAM, 200 GB vHDD – w przypadku większych wymagań wymagane jest zapewnienie właściwej platformy.** |

## SYSTEM ZARZĄDZANIA PRZEŁĄCZNIKAMI LAN/SAN– STREFA ZEWNĘTRZNA

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **MGNT-04** | **Zestaw oprogramowania do zarządzania siecią LAN.** |
| **MGNT-05** | **Zarządzanie elementami sieci LAN (funkcjonalności dla każdego z elementów i całej sieci):** |
| MGNT-05.01 | automatyczny proces rozpoznawania środowiska i topologii sieci LAN |
| MGNT-05.02 | uproszczone narzędzia konfiguracyjne (wizards) |
| MGNT-05.03 | wizualizacja topologii sieci LAN  |
| MGNT-05.04 | 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
 |
| MGNT-05.05 | 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
 |
| MGNT-05.06 | wyszukiwanie przełączników na podstawie:* nazwy przełącznika
* adresu IP
* adresu MAC
* numeru seryjnego
 |
| MGNT-05.07 | wizualizacja topologii środowiska wirtualnego VMWare dołączonego do przełączników LAN, w tym hostów, przełączników wirtualnych i maszyn wirtualnych VM |
| MGNT-05.08 | 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
 |
| MGNT-05.09 | konfiguracja funkcjonalności przełączników:* PortChannel oraz wirtualny PortChannel
* dodawanie, usuwanie i modyfikowanie VLAN-ów 802.1Q
 |
| MGNT-05.10 | definiowanie i uruchamianie samodzielnie definiowanych zadań konfiguracyjnych |
| MGNT-05.11 | 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
 |
| MGNT-05.12 | 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
 |
| **MGNT-06** | **Zarządzanie wszystkimi przełącznikami sieci LAN w strefie zewnętrznej (2 przełączniki).****Zamawiający udostępni na potrzeby instancji środowisko bazujące na VMWare vSphere, nie więcej niż 8 vCPU, 12 GB vRAM, 200 GB vHDD – w przypadku większych wymagań wymagane jest zapewnienie właściwej platformy.** |

## ROUTERY DO STYKU Z SIECIĄ INTERNET - 4 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **RTR-01** | **Wymagania Ogólne** |
| RTR-01.01 | Urządzenie o architekturze modularnej, wyposażone w 6 interfejsów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP lub równoważnych, a także w 2 interfejsy 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+ lub równoważnych. Interfejsy 10GB muszą być aktywne i obsadzone wkładkami. Jeżeli wymaga to licencji to musi być ona dostarczona. |
| RTR-01.02 | Urządzenie umożliwia rozszerzenie o co najmniej następujące typy interfejsów za pomocą modułów rozszerzeń:1. 1 port 10 GigabitEthernet
2. 8 portów Gigabit Ethernet
3. 4 interfejsy ATM STM1 lub 2 interfejsy STM4
 |
| RTR-01.03 | Urządzenie musi być dostarczone wraz z następującymi modułami SFP/SFP+:1. 2x moduł 10GB SR
2. 2x moduł 1GB SX
3. 6x moduł 1GB RJ45

Wymagane jest, aby wkładki optyczne/miedziane oferowane wraz z urządzeniem pochodziły od tego samego producenta, co przełącznik celem uniknięcia problemów z serwisowaniem urządzeń |
| RTR-01.04 | Urządzenie musi mieć możliwość instalacji przestrzeni dyskowej typu SSD o pojemności min. 100 GB. |
| RTR-01.05 | Urządzenie posiada redundante zasilacze AC 230V. |
| RTR-01.06 |  Urządzenie umożliwia montaż w szafie 19”. |
| **RTR-02** | **Wymagania wydajnościowe** |
| RTR-02.01 | Urządzenie posiada zasoby sprzętowe pozwalające przełączać 18 Mpps |
| RTR-02.02 | Urządzenie pozwala na przełączanie z prędkością 10 Gbps i umożliwia rozbudowę wydajności do co najmniej 20 Gbps bez modyfikacji sprzętowych. |
| RTR-02.03 | Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność co najmniej 10 Gbps dla ruchu IMIX. |
| RTR-02.04 | Urządzenie posiada co najmniej 16 GB pamięci RAM. |
| RTR-02.05 | Urządzenie obsługuje co najmniej 3 000 000 prefiksów w tablicach ruting IPv4. |
| RTR-02.06 | Urządzenie obsługuje co najmniej 3 000 000 prefiksów w tablicach ruting IPv6. |
| RTR-02.07 | Urządzenie obsługuje co najmniej 100 000 tras multicast. |
| **RTR-03** | **Wymagania funkcjonalne** |
| RTR-03.01 | Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP. |
| RTR-03.02 | Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP. |
| RTR-03.03 | Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja. |
| RTR-03.04 | Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci. |
| RTR-03.05 | Urządzenie obsługuje 8 000 instancji wirtualnych tablic routingu. |
| RTR-03.06 | Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.  |
| RTR-03.07 | Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF. |
| RTR-03.08 | Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN. |
| RTR-03.09 | Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol). |
| RTR-03.10 | Urządzenie obsługuje protokół GDOI (RFC 3547). |
| RTR-03.11 | Urządzenie obsługuje 4000 tuneli GRE. |
| RTR-03.12 | Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.  |
| RTR-03.13 | Urządzenie umożliwia ochronę kryptograficzną tuneli GRE |
| **RTR-04** | **Funkcjonalności związane z niezawodnością pracy** |
| RTR-04.01 | redundancja procesów rutingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego, jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej. |
| RTR-04.02 | BFD dla OSPF, BGP, ISIS |
| RTR-04.03 | IP FRR |
| RTR-04.04 | BGP Prefix-Independent Convergence (PIC)  |
| RTR-04.05 | Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP |
| RTR-04.06 | funkcjonalność VRRP |
| RTR-04.07 | redundantne zasilacze 230V |
| RTR-04.08 | możliwość wymiany modułów w trakcie pracy (ang. hot swap) |
| **RTR-05** | **Urządzenie obsługuje MPLS, w szczególności:** |
| RTR-05.01 | LDP |
| RTR-05.02 | EoMPLS, VPLS |
| RTR-05.03 | MPLS L3 VPN |
| RTR-05.04 | MPLS TE |
| RTR-05.05 | MPLS FRR w trybach protekcji łącza oraz węzła |
| **RTR-06** | **Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):** |
| RTR-06.01 | klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6 |
| RTR-06.02 | hierarchiczny QoS (H-QoS) - co najmniej 3 poziomy |
| RTR-06.03 | klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP. |
| RTR-06.04 | dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek |
| RTR-06.05 | algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek  |
| RTR-06.06 | możliwość obsługi jednej kolejki z priorytetem w stosunku do innych |
| RTR-06.07 | mechanizm ograniczania ilości ruchu w kolejce priorytetowej |
| RTR-06.08 | możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP |
| RTR-06.09 | możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) |
| RTR-06.10 | mechanizm WRED |
| RTR-06.11 | możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS |
| RTR-06.12 | klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6 |
| RTR-06.13 | hierarchiczny QoS (H-QoS) - co najmniej 3 poziomy |
| **RTR-07** | **Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:** |
| RTR-07.01 | sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu |
| RTR-07.02 | Unicast RPF (Reverse Path Forwarding) |
| RTR-07.03 | listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL |
| RTR-07.04 | 50 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), a także 4 000 list kontroli dostępu (ACL) |
| RTR-07.05 | dostęp administracyjny oparty o role z przypisanymi uprawnieniami  |
| RTR-07.06 | zasoby sprzętowe umożliwiające uruchomienie funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa:1. umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji)
2. obsługuje ruch IPv4 oraz IPv6
3. umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
4. umożliwia obsługę 2 000 000 równoczesnych sesji
5. umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę
6. Jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej.
 |
| RTR-07.07 | zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 5 Gbps (AES256) z obsługą 8 000 tuneli IPSec |
| RTR-07.08 | sieci VPN typu site-2-site oparte o IPSec |
| RTR-07.09 | dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmsji danych pomiędzy oddziałami |
| RTR-07.10 | bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast |
| RTR-07.11 | algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:Elliptic Curve Diffie-Hellman (ECDH)1. Galois Counter Mode Advanced Encryption Standard (GCM-AES) - 128/256 bitów
2. Galois Message Authentication Code (GMAC-AES) - 128/256 bitów
3. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2
4. konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2
5. IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych
6. IKEv2 zarówno dla ruchu IPv4 jak i IPv6
 |
| RTR-07.12 | funkcjonalność VPN per VRF |
| RTR-07.13 | Jeżeli do otrzymania funkcjonalności VPN IPSec jest wymagana licencja to nie jest wymagane dostarczenie jej. |
| RTR-07.14 | ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU |
| RTR-07.15 | logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU |
| RTR-07.16 | możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków |
| RTR-07.17 | funkcjonalność VPN per VRF |
| RTR-07.18 | Jeżeli do otrzymania funkcjonalności VPN IPSec jest wymagana licencja to nie jest wymagane dostarczenie jej. |
| RTR-07.19 | ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU |
| RTR-07.20 | logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU |
| RTR-07.21 | możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków |
| **RTR-08** | **Urządzenie umożliwia uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów** |
| RTR-08.01 | klasyfikacja opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów |
| RTR-08.02 | klasyfikacja udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji).  |
| RTR-08.03 | nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji  |
| **RTR-09** | **Funkcjonalności zarządzania** |
| RTR-09.01 | umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3 |
| RTR-09.02 | obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731) |
| RTR-09.03 | obsługuje MPLS OAM |
| RTR-09.04 | umożliwia pisanie skryptów konfiguracyjnych |
| RTR-09.05 | obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6 |
| RTR-09.06 | posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP |
| RTR-09.07 | posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+ |
| RTR-09.08 | posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX |
| RTR-09.09 | posiada port USB |
| RTR-09.10 | posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej, konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona |
| RTR-09.11 | urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów |

## MODUŁ SFP 1GE STANDARDU 1000Base-T – 144 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN  |
| SFP-02 | Zgodność ze standardem SFP 1000Base-T |

## MODUŁ SFP 1GE STANDARDU SX – 72 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN  |
| SFP-02 | Zgodność ze standardem SFP 1000Base-SX (IEEE 802.3z) |

## MODUŁ SFP+ 10GE STANDARDU SR – 288 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN  |
| SFP-02 | Zgodność ze standardem SFP+ 10GBase-SR (IEEE 802.3ae) |

## MODUŁ QSFP+ 40GE STANDARDU SR4 – 32 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN  |
| SFP-02 | Zgodność ze standardem QSFP 40GBase-SR4 (IEEE 802.3ba) |

## MODUŁ QSFP+ 100GE STANDARDU SR4 – 32 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN  |
| SFP-02 | Zgodność ze standardem QSFP 100GBase-SR4 (IEEE 802.3ba) |

## MODUŁ QSFP+ 100G SR-BiDi– 8 sztuk

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN |
| SFP-02 | Przepustowość 100Gbps |
| SFP-03 | Zakończenia QSFP+ |
| SFP-04 | Długość 3m |

## Przewód QSFP+ AOC 100GE o długości 1M – 24 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| SFP-01 | Kompatybilność z oferowanymi przełącznikami LAN |
| SFP-02 | Przepustowość 100Gbps |
| SFP-03 | Zakończenia QSFP+ |
| SFP-04 | Długość 1m |

## Dostawa sprzętu i oprogramowania

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOSSPRZ-01 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| DOSSPRZ-02 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| DOSSPRZ-03 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| DOSSPRZ-04 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| DOSSPRZ-05 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy. |
| DOSSPRZ-06 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy. |
| DOSSPRZ-07 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego. |
| DOSSPRZ-08 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| DOSSPRZ-09 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| 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. |
| DOSSPRZ-12 | Dostarczana ITS 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 |
| DOSSPRZ-13 | Wykonawca musi dostarczyć niewyspecyfikowane elementy ITS, które są niezbędne do prawidłowego funkcjonowania wyspecyfikowanych elementów ITS.  |
| 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. |
| 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. |
| 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). |
| DOSSPRZ-17 | Wykonawca dostarczy wszystkie licencje wymagane do działania dostarczanych Urządzeń.  |
| DOSSPRZ-18 | Wykonawca dostarczy wszystkie klucze licencyjne wymagane do instalacji i działania dostarczanego Oprogramowania. |
| DOSSPRZ-19 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania. |
| DOSSPRZ-20 | 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** |
| --- | --- |
| PROITS-01 | Wykonawca opracuje Projekt Techniczny ITS wdrożenia rozwiązań będących przedmiotem postępowania umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym.  |
| PROITS-02 | Wykonawca opracuje projekt rozmieszczenia Urządzeń w szafach „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń. Zmawiający udostępni miejsce w szafie rack w lokalizacji POPD. Szafa rack będąca przedmiotem zamówienia przewidziana jest do instalacji sprzętu w ZOPD.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. |
| PROITS-03 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| 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 Urządzeń,
	6. Projekt integracji dostarczanych Urządzeń z istniejącymi sieciami zarządzającymi Zamawiającego. Konfiguracja mechanizmów: NTP, DNS, zarządzanie, aktualizacje sygnatur, AAA, oraz pozostałe elementy wymagana do prawidłowego działania Urządzeń.
	7. Projekt konfiguracji dostarczanych Urządzeń w tym:
		1. Projekt bezpieczeństwa warstwy logicznej.
		2. Projekt warstwy fizycznej
		3. Schematy komunikacyjne pomiędzy poszczególnymi elementami infrastruktury
		4. Projekt utworzenia z dostarczanych Urządzeń klastra Active/Active w układzie dwóch OPD w celu realizacji funkcjonalności HA/DR (High Availability and DisasterRecovery) z uwzględnieniem urządzeń dostarczanych przez operatora telekomunikacyjnego w postaci routerów CE połączonych mechanizmem VRRP. Projekt musi uwzględniać różne scenariusze awarii rozwiązania, co najmniej awaria łącza w POPD, awaria łącza w ZOPD, awaria routera CE w POPD, awaria routera CE w ZOPD, awaria klastra urządzeń dostarczanych w ramach przedmiotowego projektu w POPD, awaria klastra urządzeń dostarczanych w ramach przedmiotowego projektu w ZOPD, awaria połączenia pomiędzy POPD i ZOPD. Konfiguracja styku z operatorem sieci Internet i wypracowanie metody równoważenia obciążenia na obydwa ośrodki.
		5. Projekt ochrony poczty elektronicznej z wykorzystaniem dostarczanych rozwiazań. Uruchomienie funkcji analizy plików anymalware/antywirus – integracja z dostarczonym systemem Sandbox.
		6. Projekt realizacji dostępu zdalnego do zasobów teleinformatycznych dla pracowników Prokuratury z wykorzystaniem dostarczanych rozwiązań z uwzględnieniem logowania do VPN z wykorzystaniem certyfikatu. Zestawienie tunelu VPN na stacji klienta powinno odbywać się przed logowaniem do systemu (dokładne warunki zostaną ustalone na etapie projektowania). Integracja Urządzeń NGFW z dostarczonym Serwerem Autoryzacyjnym. Budowa profili stacji roboczych oraz poziomów dostępu do zasobów.
		7. Projekt realizacji dostępu zdalnego do zasobów teleinformatycznych w jednostkach organizacyjnych dla administratorów lokalnych. Analiza oraz identyfikacja zasobów i systemów lokalnych. Integracja z posiadanym przez Zamawiającego rozwiązaniem PIM/PAM.
		8. Projekt ochrony stacji roboczych pracowników prokuratury (stacjonarnych oraz przenośnych) z wykorzystaniem dostarczanych rozwiazań. Budowa profili stacji roboczych oraz poziomów dostępu do zasobów.
		9. Projekt zarządzania infrastrukturą dostarczaną w ramach postępowania z wykorzystaniem dostarczanego oprogramowania do zarządzania i monitorowania.
		10. Projekt filtrowania URL oraz rozszywania ruchu SSL użytkowników. Integracja z Centralną Usługą Katalogową obejmującą wszystkie jednostki Zamawiającego oraz budowa profili dostępowych w oparciu grupy użytkowników.
		11. Projekt systemu logowania oraz raportowania zdarzeń z dostarczanych Urządzeń. Zaprojektowanie uzgodnionych raportów (do 30 raportów).
		12. Projekt testów akceptacyjnych.
		13. Procedury administracyjne do wszystkich dostarczonych urządzeń.
 |
| PROITS-05 | Projekt Techniczny będzie dotyczył środowisk produkcyjnych POPD i ZOPD. |

## Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MONTS-01 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty ITS w POPD i ZOPD zgodnie z opracowanym szczegółowym Projektem Technicznym. |
| MONTS-02 | Wykonawca dostarczy licencje Oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację wdrażanego rozwiązania. |
| MONTS-03 | Wykonawca dokona montażu Urządzeń we wskazanych szafach rack w pomieszczeniach POPD i ZOPD wskazanych przez Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym. |
| 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 zarówno dostarczanych w ramach przedmiotowego postępowania. W ramach prac Wykonawcy leży podłączenie wszystkich oferowanych rozwiązań do sieci LAN oraz WAN Zamawiającego. |
| MONTS-05 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję. |
| MONTS-06 | 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.  |
| MONTS-07 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania. |
| MONTS-08 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. |
| MONTS-10 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware) wszystkich urządzeń ITS do najnowszych stabilnych wersji. |
| MONTS-11 | 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** |
| --- | --- |
| PRACE-01 | Wykonawca przeprowadzi proces aktualizacji Oprogramowania oraz oprogramowania sprzętowego dostarczonych Urządzeń do najnowszych dostępnych stabilnych, rekomendowanych przez producenta wersji oprogramowania.  |
| PRACE-02 | Wykonawca zainstaluje i skonfiguruje wszystkie dostarczane Urządzenia i Oprogramowanie zgodnie z opracowanymi Projektami Technicznymi ITS  |

## Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| TESTY-01 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| TESTY-02 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| TESTY-03 | Testami zostanie objęta cała dostarczona ITS dla środowiska POPD i ZOPD. |
| TESTY-04 | Wykonawca przeprowadzi testy sprawdzające niezawodność ITS na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego. |
| TESTY-05 | Testy ITS będą wykonane przez Zamawiającego w asyście Wykonawcy, zgodnie z zaakceptowanym przez Zamawiającego Planem Testów i Scenariuszami Testów. |
| TESTY-06 | Wykonawca przed przeprowadzeniem testów przeprowadzi instruktaż dla testerów Zamawiającego. |
| 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,
4. wykonaniu testów sprawdzających przełączenie pomiędzy OPD,
5. zasymulowanie awarii łączy operatora, połączeń CWDM, klastrów wirtualizacyjnych,
6. zasymulowanie awarii noda/ów w klastrze.
 |

## Wymagania na opracowanie dokumentacji powykonawczej (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOKPOW-01 | Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów ITS dla POPD i ZOPD.  |
| DOKPOW-02 | Dokumentacja powykonawcza ITS będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| DOKPOW-03 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016) a także w wersji PortableDocument 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. |
| DOKPOW-04 | Wykonawca opracuje „Dokumentację administratora”. |
| 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.
 |
| DOKPOW-06 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą |
| DOKPOW-07 | Projekt Techniczny montażu i instalacji ITS powinien zostać zaktualizowany do postaci dokumentacji powykonawczej w chwili przekazywania infrastruktury Zamawiającemu do akceptacji. |

## Wymagania na opracowanie procedur utrzymania warstwy fizycznej ITS (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PROCUT-01 | Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonych komponentów ITS.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. |
| 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. |
| PROCUT-03 | Wykonawca opracuje i uzgodni katalog usług powstałych w ramach Projektu do implementacji w posiadanym przez Zamawiajacego rozwiązaniu ITSM Atmosfera. |
| PROCUT-04 | Wykonawca opracuje procedury dla administratorów lokalnych związane z odpowiednią konfiguracją sprzętu (komputerów stacjonarnych i przenośnych) umożliwiających korzystanie z produktów Projektu. |

## Wymagania na przygotowanie materiałów szkoleniowych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MATSZK-01 | Wykonawca opracuje materiały szkoleniowe dla wdrożonych komponentów warstwy fizycznej 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.  |

## Wymagania na warsztaty i szkolenia

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SZKOL-01 | Wykonawca zapewni szkolenia i warsztaty z dostarczanych produktów ITS. Przewidywana ilość uczestników warsztatów to maksymalnie **20 osób wskazanych przez Zamawiającego**. |
| SZKOL-02 | Wykonawca opracuje plan warsztatów oraz plan szkoleń z zakresu wdrażanej ITS. Warsztaty z zakresu wdrażanego rozwiązania będą trwać 5 dni roboczych i będą miały charakter tzw. „bootcamp”. W ramach warsztatów Wykonawca zaprezentuje przekrojowo cały zbudowany system dostępu do sieci Internet, system dostępu zdalnego, wdrożone zabezpieczenia na stacjach roboczych, zabezpieczenia systemu poczty, integracja z domeną AD, rozszywanie ruchu SSL itp. oraz zaprezentuje narzędzia do zarządzania i automatyzacji środowiska. W ramach warsztatów nastąpi konfiguracja środowiska laboratoryjnego symulującego rozwiązania wdrożone w infrastrukturze Zamawiajacego przez pracowników Zamawiającego. Zapewnienie odpowiedniego środowiska warsztatowego leży po stronie Wykonawcy. |
| SZKOL-03 | W zakresie warsztatów zadaniem Wykonawcy jest zapewnienie:* 1. bazy noclegowej – dla organizatorów i uczestników
		1. Obiekt nie może być w trakcie prac remontowych w czasie trwania warsztatów.
		2. Wykonawca zapewnia wszystkie miejsca noclegowe w sposób zapewniający samodzielny pobyt w pokoju (Zamawiający dopuszcza zakwaterowanie samodzielne jednego uczestnika w pokoju dwuosobowym)
		3. Każdy z pokoi noclegowych z łazienką, TV, łącze internetowe (Wi-Fi) posiadających otwierane okna lub działającą klimatyzację.
		4. Obiekt co najmniej \*\*\* (trzy gwiazdki), w rozumieniu przepisów § 2 ust. 2 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz. U. z 2006 r., Nr 22, poz. 169 ze zm.). Na każde żądanie Zamawiającego Wykonawca obowiązany jest okazać kopię decyzji właściwego Marszałka Województwa o nadaniu kategorii hoteli na podstawie art. 38 ust.1 i art. 42 ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2014 r., poz. 196 ze zm.),
		5. Na terenie obiektu lub w bezpośrednim jego sąsiedztwie powinien znajdować się bezpłatny parking.
		6. Obiekt powyżej trzech pięter powinien zostać wyposażony w windę
		7. Warsztaty, nocleg oraz wyżywienie powinny odbywać się na terenie tego samego obiektu.
		8. **Obiekt zlokalizowany w promieniu 50 km od centrum Warszawy.**
	2. odrębnych sal szkoleniowych dla każdej, równolegle szkolonej grupy. Każda z sal wykładowych przeznaczona jest maksymalnie dla 20 osób ze stanowiskiem dla wykładowców oraz miejscem na sprzęt multimedialny. Wszystkie sale szkoleniowe muszą być klimatyzowane i posiadać dostęp do światła dziennego oraz zapewniać komfortowe warunki do prowadzenia w nich szkoleń/warsztatów (tj. odpowiednie oświetlenie, odpowiednia temperatura).
	3. każda sala szkoleniowa musi być wyposażona w rzutnik multimedialny, ekran do wyświetlania prezentacji, tablicę do pisania lub flipchart z arkuszami papieru i pisakami, skaner, stację zarządzającą i stanowiska szkoleniowe dla każdej ze szkolonych osób, wyposażone w stację roboczą i zestaw 2-monitorowy. Wykonawca zapewni w miejscu przeprowadzania szkoleń/warsztatów urządzenia sieciowe celem połączenia ze środowiskiem warsztatowym zorganizowanym po stronie Wykonawcy. Czas wykorzystania sal pierwszego dnia od godz. 12.00 do 20.00, pozostałe dni od godz. 8.00 do 19.00.
	4. noclegów dla uczestników szkolenia/warsztatów w pokojach jednoosobowych z łazienkami lub dwuosobowych z łazienkami do samodzielnego wykorzystania **(Wykonawca ma obowiązek zapewnić nocleg każdej osobie w odrębnym pokoju).** Czas trwania doby hotelowej od godz. 11.00 pierwszego dnia szkolenia do godz. 16.00 ostatniego dnia szkolenia. Miejsca noclegowe muszą znajdować się na terenie tego samego obiektu, co sale wykładowe.
	5. Wyżywienia dla uczestników szkolenia składającego się z:
1. śniadania podawanego w formie bufetu, obejmujące:

- pieczywo jasne i ciemne, - wędliny (3 rodzaje), - ser żółty - ser biały - jaja- dżem- miód- ciepłe mleko- płatki śniadaniowe (co najmniej 2 rodzaje)- jogurt- jedno danie ciepłe- świeże warzywa (co najmniej 3 rodzaje)- napoje (kawa, herbata, woda mineralna, sok 100%)- masło, cytryna, mleko, cukier1. obiadu w formie bufetu obejmującego:

- zupę,- sałatki (minimum 2 rodzaje)- dania ciepłe (rybne, mięsne, warzywne)- dodatki skrobiowe- desery- napoje (kawa, herbata, woda mineralna, sok 100%)1. kolacji w formie bufetu obejmującej:

- sałatki (minimum 2 rodzaje)- pieczywo jasne i ciemne, - wędliny (3 rodzaje), - ser (3 rodzaje) - dania ciepłe (rybne, mięsne, warzywne) - napoje (kawa, herbata, woda mineralna, sok 100%)- masło, cytryna, mleko, cukier1. przerw kawowych (całodziennych, uzupełniany serwis konferencyjny), składający się:

- świeżo parzoną gorącą kawę naturalną oraz herbatę w torebkach- cytrynę, cukier, mleko, - sok owocowy 100%, - butelkowana woda mineralna gazowana i niegazowana, - co najmniej 3 rodzaje kruchych ciasteczek.1. Posiłki, które będą podawane podczas szkoleń/warsztatów muszą być przygotowywane na terenie obiektu w którym odbywa się szkolenie. Wyklucza się ich dowożenie.
	1. W zakresie wyżywienia Wykonawca zobowiązany jest do:
2. Terminowego przygotowania posiłków zgodnie z ustalonym harmonogramem.
3. Zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowywaniu posiłków.
4. Przygotowywania posiłków zgodnie z zasadami racjonalnego żywienia, urozmaiconych (każdego dnia szkolenia inne menu), przygotowywanych ze świeżych produktów z ważnymi terminami przydatności do spożycia.
5. Wyżywienie dla trenerów oraz innych osób zaangażowanych w obsługę szkolenia/warsztatów Wykonawca zapewnia na swój koszt.
 |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| SZKOL-09 | Szkolenia muszą być przeprowadzone w ośrodku szkoleniowym na terenie Warszawy. |
| SZKOL-10 | Każdy uczestnik szkolenia/warsztatu otrzyma certyfikat jego ukończenia. |
| SZKOL-11 | Szkolenia zostaną zrealizowane w postaci voucher-ów na autoryzowane szkolenia z zakresu wdrażanego rozwiązania chmury. Vouchery będą ważne co najmniej 24 miesiące od dnia podpisania Protokołu Odbioru Końcowego. |
| SZKOL-12 | **Wykonawca dostarczy vouchery dla 4 administratorów Zamawiającego na szkolenie z zakresu Oprogramowania EDR.** |
| SZKOL-13 | W przypadku zaprzestania przez dany ośrodek szkoleniowy prowadzenia szkoleń z danego tematu musi istnieć możliwość zamiany vouchera na szkolenie równoważne. |
| SZKOL-14 | 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. |
| SZKOL-15 | Wykonawca zapewni prowadzenie szkoleń/warsztatów przez wykwalifikowaną kadrę posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia oraz profesjonalny przebieg i organizację. |
| 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. |
| SZKOL-17 | Szkolenia powinny odbywać się w formie wykładów i warsztatów praktycznych w proporcji obejmującej co najmniej 75 % warsztatów. |
| 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 |
| 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. |

## Wymagania na serwis gwarancyjny

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| GWAR-SER-01 | 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. |
| GWAR-SER-02 | W ramach gwarancji Wykonawca zapewni następujące usługi: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 w siedzibie Zamawiajacego, jeżeli takie uaktualnienia są rekomendowane przez Producenta Sprzętu i/lubOprogramowania
6. dostęp do internetowych narzędzi serwisowych.
 |
| GWAR-SER-03 |  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. |
| GWAR-SER-4 | 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 |
| GWAR-SER-5 | 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 |
| GWAR-SER-6 | 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 |
| GWAR-SER-7 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającego do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| GWAR-SER-8 | **Wykonawca zapewni asystę techniczną, zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera w danym obszarze związanym z przedmiotem zamówienia w okresie 36 miesięcy, licząc od dnia podpisania Protokołu Odbioru Umowy, w wymiarze do 500 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).** |
| GWAR-SER-9 | Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym usługami w ramach udzielonej gwarancji.  |
| GWAR-SER-10 | Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności modyfikacji wdrożonych rozwiązań oraz wsparciu w zakresie utrzymania. |
| GWAR-SER-11 | Świadczenie usługi asysty technicznej inżyniera 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. |

Znak sprawy:

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**CZĘŚĆ II**

***Rozbudowa posiadanego przez Zamawiającego systemu bezpieczeństwa opartego na rozwiązaniach firmy Cisco i systemów wspomagających.***

# Słownik pojęć i skrótów.

**POPD** – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

**ZOPD** – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

**OPD** – Ośrodek Przetwarzania Danych

**CPD** – Centrum Przetwarzania Danych

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania

**ITS** – infrastruktura techniczno-systemowa

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny dostarczany w ramach przedmiotowego postępowania

# Opis stanu aktualnego

## Lokalizacje centrów przetwarzania danych

Zamawiający udostępnia na potrzeby wdrożenia dwa centra przetwarzania danych:

POPD PK – centrum podstawowe zlokalizowane w Warszawie przy ulicy Postępu 3

ZOPD PK – centrum zapasowe zlokalizowane w Warszawie przy ulicy Czerniakowskiej 100

## Łącza pomiędzy centrami przetwarzania danych

Zamawiający obecnie posiada łącze pomiędzy centrami przetwarzania danych o przepustowości 2x10Gbps wykonane w technologii CWDM.

Dostęp do sieci WAN-PROK i Internet jest obecnie zrealizowany w POPD. ZOPD łączy się z tymi sieciami poprzez POPD za pośrednictwem wspomnianego wyżej łącza.

## Dostęp do sieci WAN-PROK

Zamawiający udostępnia zbiorcze łącze dostępowe do dedykowanej sieci WAN-PROK prokuratury o przepustowości 512Mbps.

## Zegar

W celu synchronizacji czasu wszystkich dostarczanych Urządzeń, Zamawiający udostępnia serwer czasu ELPROMA NTS-3000.

# Przedmiot i zakres zamówienia

## Kontekst postepowania

Zamawiający planuje stworzenie na potrzeby własne oraz podległych jednostek wysokodostępnego styku POPD i ZOPD do sieci WAN. Rozwiązanie to będzie służyć udostępnianiu centralnych usług i systemów informatycznych dla wszystkich jednostek organizacyjnych Prokuratury. Obecnie Zamawiający posiada system bezpieczeństwa składający się z poniższych elementów:

1. System zarządzania Cisco FMC 4600
2. Firewalle Cisco ASA 5545-X
3. Firewalle Cisco ASA 5516-X
4. Firewalle Cisco ASA 5506-X
5. System do zarządzania Cisco Security Manager
6. System zbierania i korelacji logów Solarwinds LEM

System bezpieczeństwa oparty jest o centralny punkt zarządzania i konfiguracji urządzeń, dzięki temu cały system posiada spójne polityki bezpieczeństwa oraz centralny system analizy logów. Dodatkowo system ten posiada mechanizm tworzenia i zarządzania tunelami VPN IPSec w całej infrastrukturze Sieci WAN.

## Przedmiot postępowania

Przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego systemu bezpieczeństwa opartego na rozwiązaniach firmy Cisco poprzez:

1. Wymianę Urządzeń posiadanych przez Zamawiającego w lokalizacji POPD na bardziej wydajne;
2. Dostawę Urządzeń do lokalizacji ZOPD;
3. Wykonanie Projektu technicznego ITS dla Środowiska Produkcyjnego w POPD i ZOPD.
4. Opracowanie Scenariuszy Testów Sprzętu obejmujących scenariusze testów sprzętu dla Środowiska Produkcyjnego POPD/ZOPD
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. Przeprowadzenie warsztatów.
10. Gwarancja na dostarczony sprzęt oraz oprogramowanie.
11. Wsparcie techniczne.

## Architektura warstwy fizycznej ITS

Zamawiający koncentruje usługi informatyczne udostępniane jednostkom organizacyjnym oraz obywatelom w ramach dwóch ośrodków:

* Podstawowego Ośrodka Przetwarzania Danych (POPD).
* Zapasowego Ośrodka Przetwarzania Danych (ZOPD).

W stanie docelowym architektura obu ośrodków będzie identyczna, zbudowana w oparciu o rozwiązanie chmury prywatnej. Obydwa ośrodki będą połączone łączem zapewniającym wymianę danych niezbędnych dla spełnienia wymagań niezawodnościowych oraz przełączenia eksploatacji w przypadku awarii elementów OPD. Planowane jest umożliwienie dostępu do sieci WAN-PROK i Internet niezależnie z POPD i ZOPD. W ramach przedmiotowego projektu nastąpi dostawa oraz konfiguracja urządzeń stanowiących klastry umożliwiające niezawodny i bezprzerwowy dostęp do/z sieci WAN-PROK wykreowanej przez operatora telekomunikacyjnego.

Zrealizowane w ramach przedmiotowego projektu klastry Urządzeń w POPD i ZOPD będą stanowić uzupełniającą się i wzajemnie zabezpieczającą się parę (Active/Active, HA/DR [High Availability and DisasterRecovery]), gwarantując utrzymanie działania wszystkich usług przy braku dostępności jednego z dwóch ośrodków niezależnie od usług udostępnianych z poziomu danego OPD.

# Specyfikacja produktów

## Urządzenie firewall NGFW- 3 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **NGFW-0** | **Dwa z dostarczanych urządzeń będą tworzyły klaster w POPD natomiast jedno urządzenie będzie zainstalowane w ZOPD.** |
| **NGFW-01** | **Wymagania ogólne** |
| NGFW-01.01 | Urządzenie pełniące funkcję ściany ogniowej (firewall) typu NGFW, zapewniające inspekcję aplikacyjną oraz sondę NGIPS |
| NGFW-01.01 | Urządzenie musi być w pełni kompatybilne i zarządzane przez obecny w sieci Zamawiającego system Cisco FMC 4600 |
| NGFW-01.01 | Urządzenie musi być w pełni kompatybilne i zarządzane przez obecny w sieci Zamawiającego system Cisco Security Manager |
| NGFW-01.01 | Urządzenie musi współpracować z obecnym w sieci Zamawiającego system Solarwinds LEM |
| **NGFW-02** | **Funkcja ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji (NGFW):**  |
| NGFW-02.01 | 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) |
| NGFW-02.02 | polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń |
| NGFW-02.03 | możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:* 1. Microsoft Active Directory,
	2. usługi katalogowe LDAP, ,
	3. serwery Terminal Services.
 |
| NGFW-02.04 | Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie |
| NGFW-02.05 | obsługa funkcjonalności Network Address Translation (NAT oraz PAT) - zarówno dla ruchu wchodzącego, jak i wychodzącego |
| NGFW-02.06 | obsługa translacji adresów (NAT) dla ruchu multicast |
| NGFW-02.07 | 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 |
| NGFW-02.08 | możliwość uwierzytelnienia użytkowników z wykorzystaniem LDAP, NTLM oraz Kerberos |
| NGFW-02.09 | współpraca z serwerami autoryzacji w zakresie przypisania polityk dostępowych z granulacją per użytkownik |
| NGFW-02.10 | współpraca z serwerami CA |
| NGFW-02.11 | brak ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej |
| NGFW-02.12 | Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracyroutera (tzn. w warstwie 3 modelu OSI), przełącznika (tzn. w warstwie 2 modelu OSI), w trybie pasywnego nasłuchu (sniffer) |
| NGFW-02.13 | 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,
 |
| NGFW-02.14 | 1. Możliwość wykorzystania w polityce bezpieczeństwa następujących danych:możliwość klasyfikacji ruchu i wykrywania 3.000 aplikacji sieciowych
2. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portachd). Urządzenie musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na nim bez użycia zewnętrznych narzędzi lub współpracować 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
 |
| NGFW-02.15 | obsługa routingu statycznego i dynamicznego (min. dla protokołów RIP, OSPF i BGP) |
| NGFW-02.16 | możliwość zbierania informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL) |
| **NGFW-03** | **Funkcja wykrywania i zapobiegania włamaniom**  |
| NGFW-03.01 | Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania |
| NGFW-03.02 | Możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) |
| NGFW-03.03 | Możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu) |
| NGFW-03.04 | 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.) |
| NGFW-03.05 | Możliwość wykrywania znanych ataków, modyfikacji znanych ataków, a także ataków dla których nie są dostępne sygnatury |
| NGFW-03.06 | Zapewnienie co najmniej następujących sposobów wykrywania zagrożeń:1. sygnatury ataków opartych na exploitach,
2. reguły oparte na zagrożeniach,
 |
| NGFW-03.07 | 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 |
| NGFW-03.08 | Możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń |
| NGFW-03.09 | Zróżnicowane możliwości reakcji na zdarzenia, takich jak monitorowanie, blokowanie ruchu zawierającego zagrożenia oraz zapisywanie pakietów |
| NGFW-03.10 | Możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji |
| NGFW-03.11 | Mechanizm bezpiecznej aktualizacji sygnatur - zestawy sygnatur/reguł zabezpieczone przed modyfikacją przez osoby postronne |
| NGFW-03.12 | Możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła lub przeznaczenia |
| NGFW-03.13 | Mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych co najmniej poprzez możliwość zaimportowania z zewnętrznego repozytorium/pliku listy hostów skompromitowanych i automatyczne ich blokowanie w regułach firewalla |
| NGFW-03.14 | Jeżeli funkcjonalność wykrywania i zapobiegania włamaniom wymaga dodatkowej licencji lub subskrypcji, wymagane jest jej dostarczenie |
| **NGFW-04** | **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).** |
| **NGFW-05** | **zasilacze zmiennoprądowe w konfiguracji redundantnej** |
| **NGFW-06** | **obudowa przeznaczona do montażu w szafie rackowej 19”** |
| **NGFW-07** | **co najmniej 8 interfejsy 10GE SFP+ obsadzone wkładkami 10GBase-SR, możliwość rozbudowy co najmniej 8 interfejsów 40GE SFP+ przy czym Zamawiający uzna wymaganie za spełnione jeżeli urządzenie będzie posiadać wbudowane 8 interfejsów 40GE QSFP+** |
| **NGFW-08** | **dedykowany interfejs GE 100/1000 na potrzeby zarządzania** |
| **NGFW-09** | **Wymagania wydajnościowe** |
| NGFW-09.01 | przepustowość na poziomie co najmniej 9 Gbps dla usługi NGFW z kontrolą aplikacji |
| NGFW-09.02 | przepustowość na poziomie co najmniej 9 Gbps dla pakietów o średniej wielkości 1024B przy kombinacji usług NGFW i NGIPS |
| NGFW-09.03 | obsługa co najmniej 3.000.000 jednoczesnych połączeń |
| NGFW-09.04 | obsługa zestawiania co najmniej 50.000 nowych połączeń na sekundę |
| NGFW-09.05 | obsługa co najmniej 10 000 reguł bezpieczeństwa |
| NGFW-09.06 | obsługa co najmniej 10000 tuneli IPSEC VPN |
| NGFW-09.07 | przepustowość IPSEC VPN co najmniej 3 Gbps |

## Dostawa sprzętu i oprogramowania

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOSSPRZ-01 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| DOSSPRZ-02 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| DOSSPRZ-03 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| DOSSPRZ-04 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| DOSSPRZ-05 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy. |
| DOSSPRZ-06 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy. |
| DOSSPRZ-07 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego. |
| DOSSPRZ-08 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| DOSSPRZ-09 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| 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. |
| DOSSPRZ-12 | Dostarczana ITS 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 |
| DOSSPRZ-13 | Wykonawca musi dostarczyć niewyspecyfikowane elementy ITS, które są niezbędne do prawidłowego funkcjonowania wyspecyfikowanych elementów ITS.  |
| 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. |
| 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. |
| 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). |
| DOSSPRZ-17 | Wykonawca dostarczy wszystkie licencje wymagane do działania dostarczanych Urządzeń.  |
| DOSSPRZ-18 | Wykonawca dostarczy wszystkie klucze licencyjne wymagane do instalacji i działania dostarczanego Oprogramowania. |
| DOSSPRZ-19 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania. |
| DOSSPRZ-20 | 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** |
| --- | --- |
| PROITS-01 | Wykonawca opracuje Projekt Techniczny ITS wdrożenia rozwiązań będących przedmiotem postępowania umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym.  |
| PROITS-02 | Wykonawca opracuje projekt rozmieszczenia Urządzeń w szafach „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń. Zmawiający udostępni miejsce w szafie rack w lokalizacji POPD i ZOPD - 8RU w każdym.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. |
| PROITS-03 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| 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 Urządzeń,
6. Projekt integracji dostarczanych Urządzeń z istniejącymi sieciami zarządzającymi Zamawiającego. Konfiguracja mechanizmów: NTP, DNS, zarządzanie, aktualizacje sygnatur, AAA, oraz pozostałe elementy wymagana do prawidłowego działania Urządzeń.
7. Projekt konfiguracji dostarczanych Urządzeń w tym:
	1. Projekt bezpieczeństwa warstwy logicznej.
	2. Projekt warstwy fizycznej
	3. Schematy komunikacyjne pomiędzy poszczególnymi elementami infrastruktury
	4. Projekt utworzenia z dostarczanych Urządzeń klastra Active/Active w układzie dwóch OPD w celu realizacji funkcjonalności HA/DR (High Availability and DisasterRecovery) z uwzględnieniem urządzeń dostarczanych przez operatora telekomunikacyjnego w postaci routerów CE połączonych mechanizmem VRRP. Projekt musi uwzględniać różne scenariusze awarii rozwiązania, co najmniej awaria łącza w POPD, awaria łącza w ZOPD, awaria routera CE w POPD, awaria routera CE w ZOPD, awaria klastra urządzeń dostarczanych w ramach przedmiotowego projektu w POPD, awaria klastra urządzeń dostarczanych w ramach przedmiotowego projektu w ZOPD, awaria połączenia pomiędzy POPD i ZOPD.
	5. Projekt migracji konfiguracji z obecnie posiadanego w lokalizacji POPD klastra urządzeń Cisco ASA 5545-X do wdrażanego rozwiązania.
	6. Projekt uruchomienia lokalizacji ZOPD.
	7. Projekt konfiguracji infrastruktury sieci LAN w lokalizacjach POPD i ZOPD oraz dostęp z/do zasobów z sieci WAN-PROK we wdrażanej architekturze rozwiązania.
	8. Integracja z Centralną Usługą Katalogową obejmującą wszystkie jednostki Zamawiającego oraz budowa profili dostępowych w oparciu o grupy użytkowników.
8. Projekt przełączenia produkcyjnego z obecnie posiadanego w lokalizacji POPD klastra urządzeń Cisco ASA 5545-X do wdrażanego rozwiązania.
 |
| PROITS-05 | Projekt Techniczny będzie dotyczył środowisk produkcyjnych POPD i ZOPD. |

## Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MONTS-01 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty ITS w POPD i ZOPD zgodnie z opracowanym szczegółowym Projektem Technicznym. |
| MONTS-02 | Wykonawca dostarczy licencje Oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację wdrażanego rozwiązania. |
| MONTS-03 | Wykonawca dokona montażu Urządzeń we wskazanych szafach rack w pomieszczeniach POPD i ZOPD wskazanych przez Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym. |
| 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 zarówno dostarczanych w ramach przedmiotowego postępowania. W ramach prac Wykonawcy leży podłączenie wszystkich oferowanych rozwiązań do sieci LAN Zamawiającego |
| MONTS-05 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję. |
| MONTS-06 | 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.  |
| MONTS-07 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania. |
| MONTS-08 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. |
| MONTS-10 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware) wszystkich urządzeń ITS do najnowszych stabilnych wersji. |
| MONTS-11 | 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** |
| --- | --- |
| PRACE-01 | Wykonawca przeprowadzi proces aktualizacji Oprogramowania oraz oprogramowania sprzętowego dostarczonych Urządzeń do najnowszych dostępnych stabilnych, rekomendowanych przez producenta wersji oprogramowania.  |
| PRACE-02 | Wykonawca zainstaluje i skonfiguruje wszystkie dostarczane Urządzenia i Oprogramowanie zgodnie z opracowanymi Projektami Technicznymi ITS  |

## Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| TESTY-01 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| TESTY-02 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| TESTY-03 | Testami zostanie objęta cała dostarczona ITS dla środowiska POPD i ZOPD. |
| TESTY-04 | Wykonawca przeprowadzi testy sprawdzające niezawodność ITS na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego. |
| TESTY-05 | Testy ITS będą wykonane przez Zamawiającego w asyście Wykonawcy, zgodnie z zaakceptowanym przez Zamawiającego Planem Testów i Scenariuszami Testów. |
| TESTY-06 | Wykonawca przed przeprowadzeniem testów przeprowadzi instruktaż dla testerów Zamawiającego. |
| 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,
4. wykonaniu testów sprawdzających przełączenie pomiędzy OPD,
5. zasymulowanie awarii łączy operatora, połączeń CWDM,klastrów wirtualizacyjnych,
6. zasymulowanie awarii noda/ów w klastrze.
 |

## Wymagania na opracowanie dokumentacji powykonawczej (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOKPOW-01 | Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów ITS dla POPD i ZOPD. W ramach dokumentacji powykonawczej Wykonawca opracuje Politykę Bezpieczeństwa wdrożonego rozwiązania wraz z analiza ryzka oraz analizą BIA. |
| DOKPOW-02 | Dokumentacja powykonawcza ITS będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| DOKPOW-03 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016) a także w wersji PortableDocument 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. |
| DOKPOW-04 | Wykonawca opracuje „Dokumentację administratora”. |
| 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.
 |
| DOKPOW-06 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą |
| DOKPOW-07 | Projekt Techniczny montażu i instalacji ITS powinien zostać zaktualizowany do postaci dokumentacji powykonawczej w chwili przekazywania infrastruktury Zamawiającemu do akceptacji. |

## Wymagania na opracowanie procedur utrzymania warstwy fizycznej ITS (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PROCUT-01 | Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonych komponentów ITS.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. |
| 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. |

## Wymagania na warsztaty i szkolenia

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SZKOL-01 | Wykonawca zapewni warsztaty z dostarczanych produktów ITS. Przewidywana ilość uczestników warsztatów to maksymalnie 4 osoby wskazane przez Zamawiającego. |
| SZKOL-02 | Wykonawca opracuje plan warsztatów z zakresu wdrażanej ITS. 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. |
| SZKOL-03 | Warsztaty odbędą się w siedzibie Zamawiającego lub w formie zdalnej. Warsztaty będą prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań.  |
| 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. |
| SZKOL-05 | Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje harmonogram warsztatów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia. |
| SZKOL-06 | Program 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 warsztatów. Zamawiający zastrzega sobie prawo do korekty programu warsztatów w uzgodnionym zakresie. |
| 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. |
| SZKOL-15 | Wykonawca dostarczy wszystkie materiały pomocnicze niezbędne do przeprowadzenia warsztatów, jak np. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć. |
| SZKOL-17 | 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 |

## Wymagania na serwis gwarancyjny

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| GWAR-SER-01 | 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. |
| GWAR-SER-02 | W ramach gwarancji Wykonawca zapewni następujące usługi: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 w siedzibie Zamawiajacego, jeżeli takie uaktualnienia są rekomendowane przez Producenta Sprzętu i/lubOprogramowania
6. dostęp do internetowych narzędzi serwisowych.
 |
| GWAR-SER-03 |  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. |
| GWAR-SER-4 | 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 |
| GWAR-SER-5 | 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 |
| GWAR-SER-6 | 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 |
| GWAR-SER-7 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającego do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| GWAR-SER-8 | **Wykonawca zapewni asystę techniczną, zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera w danym obszarze związanym z przedmiotem zamówienia w okresie 36 miesięcy, licząc od dnia podpisania Protokołu Odbioru Umowy, w wymiarze do 100 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).** |
| GWAR-SER-9 | Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym usługami w ramach udzielonej gwarancji.  |
| GWAR-SER-10 | Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności modyfikacji wdrożonych rozwiązań oraz wsparciu w zakresie utrzymania. |
| GWAR-SER-11 | Świadczenie usługi asysty technicznej inżyniera 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. |