**Załącznik nr 4 do SIWZ**

**spr. nr 5/BŁiI/18/RG/PMP**

**Szczegółowy opis przedmiotu zamówienia**

**Budowa Systemu Elektronicznej Poczty Policji (SEPP).**

**Przedmiot zamówienia.**

Przedmiotem zamówienia jest:

* Budowa Systemu Elektronicznej Poczty (SEPP) - klasy Enterprise (wyspecjalizowanego systemu informatycznego o wysokiej niezawodności, skalowalności z wysokim poziomem bezpieczeństwa) dla wszystkich funkcjonariuszy
i pracowników Policji. W architekturze zcentralizowanej z wykorzystaniem mechanizmów wirtualizacji umożliwiającymi zbudowanie systemu w dwóch ośrodkach Podstawowy i Zapasowy zlokalizowanych na terenie Warszawy w obiektach KGP.
* Budowa systemu dostępowego do zasobów SEPP w celu umożliwienia podłączenia systemu SEPP do infrastruktury sieciowej Policji oraz zapewnienia odpowiedniego poziomu bezpieczeństwa dostępu do środowiska SEPP w dwóch ośrodkach CPD na styku sieci INTERNET/PSTD.
1. **Budowa Systemu Elektronicznej Poczty (SEPP)**

**1. Stan obecny funkcjonujący u Zamawiającego.**

Obecnie system pocztowy wykorzystywany w Policji oparty jest o rozwiązanie firmy IBM Lotus Domino. Infrastruktura sprzętowo-serwerowa systemu Lotus Domino rozmieszczona jest w lokalizacjach KWP/KSP/KGP. System Domino działa w środowisku zwirtualizowanym IBM PowerVM na platformie sprzętowej IBM Power5 pod kontrolą systemu operacyjnego AIX. W środowisku produkcyjnym na każdym z serwerów KWP/KSP/KGP zainstalowane jest oprogramowanie serwerowe Lotus Domino Enterprise Server dodatkowo na serwerach po jednym w każdej lokalizacji KWP/KSP/KGP zainstalowane jest oprogramowanie IBM Tivoli Storage Manager Server pełniące rolę serwera backup skrzynek pocztowych oraz systemów. Ponadto w KGP w środowisku Domino, zainstalowane są serwery: IBM Tivoli Directory Integrator, IBM Lotus Sametime, IBM Lotus Quickr , IBM Lotus Traveler, na których usługi udostępnione są dla wszystkich użytkowników Policji na terenie kraju.

**2. Opis ogólnych wymagań realizacji zamówienia.**

Wykonawca zobowiązany jest zaprojektować, dostarczyć oraz wdrożyć mechanizmy elektronicznej poczty dla (**100 tys. użytkowników**) użytkowników Policji z zastosowaniem tzw. rozwiązań ”pudełkowych” oprogramowania standardowego. **Zamawiający nie dopuszcza zastosowania rozwiązań opartych o oprogramowanie typu open-source (powyższy wymóg nie dotyczy komercyjnych serwerowych systemów operacyjnych klasy Linux/Unix, dla których świadczone jest wsparcie producenta).**

W ramach realizacji zamówienia Wykonawca przedstawi Zamawiającemu spełniającą wymagania SIWZ koncepcję realizacji zadania. Węzły pocztowe muszą obsługiwać wszystkich użytkowników Policji zlokalizowanych na terenie całego kraju przynależnych organizacyjnie do danej lokalizacji KGP/KSP/KWP/SP oraz lokalizacji jej podległych
z zachowaniem obecnej struktury.

Wykonawca dostarczy w miejsce wskazane przez Zamawiającego wszystkie niezbędne komponenty tj. sprzęt wraz z kompletnym okablowaniem LAN, SAN umożliwiającym podłączeniem do infrastruktury Zamawiającego, oprogramowanie wraz z (bezterminowymi licencjami) oraz zainstaluje i skonfiguruje niezbędną architekturę sprzętowo/programową wymaganą do wdrożenia centralizacji i wirtualizacji systemu elektronicznej poczty Policji. Wymagane jest również przeprowadzenie procesu migracji i integracji, opracowanie
i przeprowadzenie testów funkcjonalnych, wydajnościowych i niezawodnościowych oraz wykonanie kompletnej dokumentacji opisanej w Załączniku nr 11 do Umowy.

Zamawiający wymaga dostarczenia niezbędnego oprogramowania dla całego rozwiązania
w najnowszej, stabilnej wersji, dostępnej na dzień podpisania umowy, udostępnionej przez producenta oprogramowania. Zamawiający wymaga dostarczenia oprogramowania, zarówno standardowego jak i dedykowanego, na płytach CD/DVD.

**Proponowane rozwiązania softwarowo-sprzętowe nie mogą mieć w momencie składania oferty określonej daty wygaśnięcia okresu wsparcia, lub czas ten powinien być dłuższy niż 36 m-cy.** Dostarczona infrastruktura sprzętowa na potrzeby realizacji przedmiotu zamówienia musi być fabrycznie nowa z datą produkcji nie starszą niż rok od dnia podpisania umowy oraz wolna od wad. Wykonawca zobowiązany jest do przedstawienia Zamawiającemu odpowiednich dokumentów od producenta sprzętu/oprogramowania potwierdzających powyższe zapisy.

Nie dopuszcza się rozwiązania w postaci usługi w „chmurze publicznej”. Wszystkie informacje przetwarzane w SEPP muszą być przechowywane na serwerach dostarczonych
w ramach zamówienia, które będą stanowiły własność Zamawiającego i zainstalowane będą w lokalizacjach wskazanych przez Zamawiającego.

Oferowany system musi być przystosowany do przetwarzania danych osobowych, w zakresie obowiązujących przepisów z uwzględnieniem:

* Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
* Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.
* Regulacja UE RODO/GDPR 25 maja 2018 r.

**3. Komponenty funkcjonalne, techniczne, bezpieczeństwa wymagane dla sytemu SEPP**

Szczegółowy opis komponentów, które muszą zawierać się w docelowej architekturze rozwiązania dla systemu poczty.

**3.1. Główne komponenty systemu elektronicznej poczty Policji**

1. Serwer poczty – serwer ten musi odpowiadać, za udostępnianie poczty użytkownikom pracującym w sieci wewnętrznej (PSTD – Policyjna Sieć Transmisji Danych) oraz
w sieci INTRANET. Każdy użytkownik musi posiadać własną skrzynkę zlokalizowaną na tym serwerze. Serwery poczty muszą być skonfigurowane w klaster tak, aby zapewnić nieprzerwaną pracę wszystkim użytkownikom poczty elektronicznej.
2. Klient poczty elektronicznej – dedykowane oprogramowanie klienta aplikacji dostępowej interfejsu web do odbierania i wysyłania poczty zarówno w sieci wewnętrznej jak i internetowej (za pomocą posiadanych przez Zamawiającego rozwiązań VPN) zainstalowane na stanowiskach końcowych użytkowników.
3. Zarządzanie pocztą – Komponent ten musi umożliwiać zarządzanie systemem poczty elektronicznej, skrzynkami użytkowników oraz dostęp do statystyk i logów użytkowników.
4. Mechanizm integracji z LDAP BTUU – Komponent ten musi odpowiadać za integrację na poziomie m.in. kontroli praw dostępu oraz katalogu użytkowników nowego systemu poczty (w zakresie automatyczna rejestracja kont użytkowników po nadaniu odpowiednich uprawnień w zewnętrznym systemie LDAP) funkcjonującego
u Zamawiającego.
5. Integracja systemu pocztowego z posiadanym przez Zamawiającego systemem PKI
(w zakresie wykorzystywania podpisu elektronicznego i szyfrowania w tym udostępnianie kluczy publicznych dla podmiotów zew.)
6. Integracja systemu pocztowego z posiadanym przez Zamawiającego systemem zarządzania urządzeniami przenośnymi AirWatch
7. Mechanizm rozliczalności działań użytkowników na skrzynkach na potrzeby audytu (logowanie, kiedy użytkownik odczytał, skasował wiadomość, działania administratorów, dotyczy również skrzynek funkcyjnych w tym generowanie raportów itd.)
8. Mechanizm ochrony przed wyciekiem informacji DLP (Data Loss Prevention)
9. Mechanizm migracji z obecnego systemu poczty Lotus Domino do nowego systemu. Migracji podlegają adresy email użytkowników, list wysyłkowych i grup dystrybucyjnych oraz adresy skrzynek grupowych i funkcyjnych. Migracji nie podlegają zawartości skrzynek z obecnego systemu poczty).
10. Mechanizm monitorowania całego środowiska serwerowego
11. Mechanizm umożliwiający wdrożenie centralnej archiwizacji skrzynek pocztowych – Intencją zamawiającego jest zapewnienie i zwiększenie bezpieczeństwa systemu poczty poprzez zastosowanie komponentu odpowiedzialnego za mechanizmy archiwizacji skrzynek użytkowników. Komponent ten musi pozwalać na archiwizowanie (on-line) bez konieczności przerywania pracy systemu poczty.
12. Mechanizm backupu/archiwizacji całego środowiska serwerowego w tym skrzynek pocztowych użytkowników.

**3.1.1. Wymagania dla systemu pocztowego – część serwerowa**

Zamawiający wymaga, aby dostarczone rozwiązanie posiadało niżej wymienione cechy:

Komponent serwer poczty

1. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych w sieci Internet.
2. Wysyłanie poczty z aplikacji lub systemów zew. za pomocą protokołu SMTP
(urządzenia wielofunkcyjne, drukarki, serwery itp.)
3. Współpraca z serwerami fax w zakresie wysyłania/odbierania wiadomości
4. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
5. Globalną książkę adresową dla wszystkich użytkowników, obsługa list i grup dystrybucyjnych
6. Zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami i notatkami
7. Możliwość rejestracji i wykorzystywania w pełnym zakresie przez zarejestrowanych użytkowników systemu, kont skrzynek grupowych/funkcyjnych/współdzielonych bez ograniczeń, co do ilości i bez konieczności nabywania dodatkowej licencji.
8. Skrzynki grupowe/funkcyjne/współdzielone, jako odrębne skrzynki niepowiązane ze skrzynką żadnego z użytkowników, do której przypisywane są uprawnienia dostępu
9. Możliwość dostępu przez użytkowników do skrzynek grupowych/funkcyjnych/współdzielonych zarówno poprzez interfejs Web (w ramach jednej sesji przeglądarki), jak i dowolnego oprogramowania tzw. „grubego” klienta poczty za pomocą standardowych protokołów wykorzystywanych do obsługi poczty elektronicznej, takich jak IMAP, POP3, SMTP.
10. Wielopoziomowy mechanizm zarządzania uprawnieniami dla użytkowników, umożliwiający między innymi nadawanie/delegowanie odpowiednich uprawnień do wykonywania określonych zadań administracyjnych przez uprawnione grupy osób
w odniesieniu do użytkowników zgodnie ze strukturą organizacyjna.
11. Mechanizm definiowania różnych limitów pojemności skrzynek pojedynczych użytkowników oraz dla skrzynek różnych grup użytkowników
12. Możliwość zarządzania cyklem życia informacji przechowywanych w systemie poczty w tym wygaszanie/usuwanie po zdefiniowanym okresie czasu
13. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości zgodnego ze standardem X.509 w oparciu o infrastrukturę PKI posiadaną przez Zamawiającego
14. Możliwość integracji danych i aplikacji z innymi systemami, za pomocą LDAP, SMTP;
15. Obsługę powszechnie przyjętych i stosowanych standardów: SMTP, IMAP, POP3, MIME, S/MIME, SSL, TLS, LDAP, HTTP, HTTPS, SNMP, ActiveSync
16. Wsparcie obsługi urządzeń mobilnych z systemem Android, iOS, Microsoft Windows;
17. Możliwość elastycznego definiowania zasad routowania poczty pomiędzy węzłami np. dwóch ośrodków ( Podstawowy oraz Zapasowy)
18. Możliwość integracji z zewnętrznym katalogiem użytkowników
19. Interfejs do zarządzania skrzynkami użytkowników
20. Możliwość integracji z zewnętrznym systemem archiwizacji umożliwiającym online-owe archiwizowanie danych znajdujących się na serwerze.
21. Możliwość przenoszenia archiwów lokalnych skrzynki pocztowej z komputera użytkownika na serwer i z serwera na stację roboczą użytkownika.
22. Obsługa wielowarstwowego systemu uprawnień, z możliwością definiowania praw dostępu użytkowników do serwerów, aplikacji i danych, nadawanie praw dostępu przez użytkowników do swojej skrzynki, kalendarza i skrzynek współdzielonych.
23. Możliwość szyfrowania i kompresji komunikacji pomiędzy serwerami i stacjami klienckimi
24. Możliwość wdrożenia centralnej archiwizacji skrzynek użytkowników
25. Skalowalność systemu pozwalającą na docelową obsługę 120 000 użytkowników
26. Zakładana pojemność skrzynki użytkownika min. 1GB
27. Usunięte wiadomości przez użytkownika dostępne przez 30 dni od momentu usunięcia wiadomości, dotyczy to również skrzynek grupowych/funkcyjnych
28. W przypadku awarii pojedynczego serwera lub komponentu fizycznego system musi być nadal dostępny dla użytkowników. Awaria pojedynczego serwera lub bazy danych nie może powodować utraty dostępu do systemu poczty dla zalogowanych użytkowników. Każda baza skrzynek pocztowych musi posiadać minimum dwie instancje rozproszone pomiędzy dwa ośrodki przetwarzania. Przełączanie pomiędzy bazami musi być automatyczne i niezauważalne dla zalogowanych użytkowników
29. Pracę systemu SEPP w architekturze klastra w dwóch ośrodkach CPD Podstawowy
i Zapasowy zlokalizowanych w obiektach KGP na terenie Warszawy
30. System musi zapewniać ciągłość pracy dla wszystkich użytkowników w przypadku zdarzenia powodującego całkowitą niedostępność serwisu/usług w lokalizacji Podstawowej (Disaster Recovery), ciągłość pracy systemu powinno automatycznie zapewnić środowisko Zapasowe.
31. Możliwość automatycznej replikacji baz danych skrzynek pocztowych pomiędzy serwerami zlokalizowanymi lokalnie lub rozporoszonymi pomiędzy dwoma ośrodkami CPD (Podstawowy i Zapasowy).
32. Zamawiający wymaga dostarczenia oprogramowania wirtualizacyjnego oraz aplikacji do zarządzania środowiskiem wirtualnym z jednego centralnego miejsca w dwóch ośrodkach CPD.
33. System musi zapewniać mechanizmy równoważenia obciążenia (load balancing) również na poziomie warstwy dostępu klienckiego.
34. Zamawiający wymaga, aby dostarczony system pocztowy współpracował, z oprogramowaniem tzw. „grubego” klienta poczty za pomocą standardowych protokołów wykorzystywanych do obsługi poczty elektronicznej, takich jak IMAP, POP3, SMTP.
35. Nielimitowana ilość sesji dostępowych dla wszystkich użytkowników za pomocą różnych protokołów klienta aplikacji dostępowej interfejsu web, klienta urządzeń aplikacji mobilnych oraz aplikacji tzw. „grubego” klienta poczty za pomocą standardowych protokołów wykorzystywanych do obsługi poczty elektronicznej, takich jak IMAP, POP3, SMTP.

**3.1.2. Wymagania - klient poczty elektronicznej**

Klient poczty – dedykowane oprogramowanie klienta aplikacji dostępowej interfejsu web do odbierania i wysyłania poczty zarówno w sieci wewnętrznej jak i internetowej (za pomocą posiadanych przez Zamawiającego rozwiązań VPN) zainstalowane na stanowiskach końcowych użytkowników.

Dostarczenie dla wszystkich użytkowników SEPP bezterminowych licencji dostępowych oraz oprogramowania na aplikację dostępową interfejsu web klienta poczty. Oprogramowanie klienta aplikacji dostępowej interfejsu web musi być produktem pochodzącym od tego samego producenta, co dostarczony system pocztowy.

W środowisku zamawiającego, przez użytkownika końcowego używane są następujące systemy operacyjne: Windows XP, Vista, 7, 8, 10, Mac OS X. Oprogramowanie klienta aplikacji dostępowej interfejsu web musi współpracować z w/w systemami operacyjnymi.

Wymagany jest nieograniczony dostęp z dowolnego urządzenia/komputera i miejsca za pomocą protokołów (IMAP, IMAPs, POP3, POP3s, SMTP, ActiveSync) dla wszystkich użytkowników systemu SEPP, za pomocą oprogramowania klienta poczty posiadanego przez Zamawiającego poprzez w/w standardowe protokoły wykorzystywane do obsługi poczty elektronicznej, bez konieczności nabywania dodatkowych licencji dostępowych.

Wymagane jest, aby oprogramowanie klienta aplikacji dostępowej interfejsu web umożliwiało wykorzystanie wszystkich oferowanych przez oprogramowanie serwerowe systemu poczty funkcjonalności.

Po stronie stacji użytkowników system poczty musi spełniać następujące wymagania:

1. Obsługa poczty wewnętrznej i zewnętrznej
2. Możliwość pracy w trybie off-line oraz synchronizacji danych z serwerem
3. Zarządzanie kalendarzem osobistym, zadaniami oraz kontaktami
4. Możliwość definiowania kalendarzy grupowych
5. Możliwość rezerwacji i zarządzania zasobami typu sale, projektory, itp.
6. Możliwość bezpiecznego udostępniania skrzynki i kalendarza osobom trzecim według reguł ustawianych przez właściciela skrzynki
7. Możliwość definiowania reguł i sposobów filtrowania wiadomości przez właściciela skrzynki
8. Możliwość tworzenia i zarządzania folderami w skrzynce samodzielnie przez użytkownika, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania, zarządzanie spamem
9. Możliwość dostępu przez użytkowników do skrzynek grupowych/funkcyjnych/współdzielonych zarówno poprzez klienta aplikacji dostępowej interfejsu web, jak i oprogramowania tzw. „grubego” klienta poczty za pomocą standardowych protokołów wykorzystywanych do obsługi poczty elektronicznej, takich jak IMAP, POP3, SMTP.
10. Możliwość pełnotekstowego przeszukiwania zawartości skrzynek, oraz przeszukiwanie zaawansowane wg. różnych kryteriów
11. Możliwość automatycznego lokalnego/centralnego archiwizowania skrzynki (poczta, kalendarz, zadania) według reguł ustawianych przez użytkownika
12. Możliwość definiowania, przydzielania i delegowania zadań
13. Możliwość dostępu do skrzynki pocztowej użytkownika za pomocą przeglądarki internetowej MS Internet Explorer, MS Edge, Mozilla Firefox, Chrome
14. Możliwość obsługi aplikacji pracy biurowych
15. Możliwość wykorzystania funkcji podpisu cyfrowego i szyfrowania za pomocą systemu PKI wykorzystywanego u Zamawiającego
16. Możliwość importu i wykorzystywania certyfikatów zewnętrznych
17. Możliwość dostępu do systemu pocztowego w pełnej funkcjonalności spoza sieci wewnętrznej poprzez publiczną sieć Internet z dowolnego komputera poprzez interfejs przeglądarki
18. Możliwość archiwizacji lokalnej/centralnej wiadomości według kryteriów zdefiniowanych przez użytkownika, oraz dostępu do archiwum
19. Wsparcie i obsługa urządzeń mobilnych w pełnym zakresie oferowanych przez oprogramowanie serwerowe systemu poczty usług, za pomocą przeglądarki internetowej lub dedykowanej aplikacji.
20. Interfejs użytkownika w języku polskim

**Funkcjonalność wspierająca pracę grupową:**

* 1. Udostępnianie kalendarzy osobistych/grupowych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu: odczyt/tworzenie/zapis/usuwanie/ pełna kontrola dla wybranego użytkownika
	2. Możliwość planowania spotkań z możliwością zapraszania wymaganych
	i opcjonalnych uczestników oraz zasobów wraz z podglądem ich dostępności raportowaniem akceptacji bądź odrzucenia zaproszenia
	3. Funkcja delegowania zadań do innych pracowników wraz ze śledzeniem statusu ich wykonania
	4. Możliwość samodzielnego udostępniania skrzynek pocztowych tj. grupowych/funkcyjnych/współdzielonych przez użytkownika za pomocą aplikacji dostępowej.

 **3.2. Komponent zarządzania pocztą**

1. Zcentralizowane narzędzia administracji systemem poczty z możliwością delegowania uprawnień dla wyodrębnionych grup administratorów w obrębie podległej jednostki organizacyjnej.
2. Dostęp poprzez interfejs www, lub dedykowana konsola administracyjna
3. Monitorowanie i raportowanie zdarzeń w systemie dostęp do logów i statystyk
4. Śledzenie przesyłanych wiadomości
5. Automatyzacja czynności administracyjnych
6. Możliwość wysyłania logów i komunikatów systemowych za pomocą syslog-a

**3.3. Komponent integracji systemu poczty elektronicznej z systemem LDAP BTUU**

Aktualnie główne repozytorium użytkowników systemów informatycznych znajduje się
w systemie LDAP BTUU. System ten oparty jest o produkty firmy ORACLE, dodatkowo w projekcie należy uwzględnić konektor między IDM, a SEPP. Dostęp do repozytorium użytkowników może się odbywać z wykorzystaniem protokołu LDAP. System LDAP BTUU służy do autoryzacji użytkowników oraz kontroli praw dostępu do systemów wewnętrznych Policji. Proponowany system poczty elektronicznej musi zapewniać integrację na poziomie kontroli praw dostępu z istniejącym systemem funkcjonującym
u zamawiającego. W zakresie automatycznego zarządzania użytkownikami dodawanie/usuwanie kont w nowym systemie poczty na podstawie zdefiniowanych uprawnień w katalogu użytkowników zgodnie z obowiązującą strukturą organizacyjną
u Zamawiającego.

**3.4. Komponent integracji systemu poczty elektronicznej z posiadanym przez Zamawiającego systemem PKI (w zakresie wykorzystywania podpisu elektronicznego
i szyfrowania)**

Oferowany system musi współpracować z systemem PKI posiadanym przez Zamawiającego w zakresie podpisu elektronicznego i szyfrowania. System pocztowy musi umożliwiać wykorzystanie kluczy prywatnych przechowywanych na karcie mikroprocesorowej lub kontenerze systemowym. Zamawiający wymaga, aby klucze publiczne dla podmiotów zewnętrznych były udostępnione na dedykowanym serwerze w sieci Policji, który zostanie przygotowany i skonfigurowany przez Wykonawcę.

Wykonawca dostarczy system operacyjny oraz niezbędne oprogramowanie, wraz
z wymaganymi licencjami do wszystkich elementów systemu.”

**3.5. Komponent integracji systemu pocztowego z posiadanym przez Zamawiającego systemem zarządzania urządzeniami przenośnymi AirWatch.**

Oferowany system musi współpracować w zakresie możliwości dostępu do skrzynek pocztowych użytkowników oraz oferowanych funkcjonalności przez SEPP z zastosowaniem systemu AirWatch i urządzeniami mobilnymi posiadanymi przez Zamawiającego.

**3.6. Komponent rozliczalności/audytu systemu pocztowego**

Mechanizm rozliczności działań wszystkich użytkowników na skrzynkach pocztowych na potrzeby audytu, (logowanie czynności wykonanych przez użytkownika w odniesieniu do każdej wiadomości na wszystkich skrzynkach. Wysłanie/odebranie/odczytanie/usunięcie/stempel czasu/logowanie do systemu (udane/nieudane) /temat wiadomości i ID wiadomości zarówno przez klienta aplikacji dostępowej interfejsu web, jak i aplikacji tzw. „grubego” klienta poczty, w tym rejestr działań administratorów. Powyższe informacje dotyczą również skrzynek grupowych/funkcyjnych itd.). Logowane czynności jednoznacznie powinny wskazywać, jakie czynności użytkownik wykonywał na swojej skrzynce pocztowej oraz innych, do których był uprawniony.

Wymagane jest gromadzenie i przechowywanie takiego zbioru logów przez okres 3 lat.

Ponadto komponent musi zawierać

* Możliwość zbiorczego usuwania logów po zakładanym okresie
* Możliwość prostego generowania raportów w ramach podległej jednostki organizacyjnej za dany przedział czasowy dla wskazanego użytkownika
* Możliwość definiowania parametrów, wyszukiwania indywidualnego audytu informacji dla określonych domen, skrzynek pocztowych, tematów wiadomości, adresów e-mail, nazwisk, przez osoby uprawnione w odniesieniu do zgromadzonych danych ramach podległej jednostki organizacyjnej
* Mechanizm kontroli dostępu, który umożliwia nadanie uprawnień grupie użytkowników np. administratorom/audytorom lub innym osobom uprawnionym do wykonywania określonych zadań w odniesieniu do danych zgromadzonych tylko ramach podległej jednostki organizacyjnej.
* Zarządzanie i wykonywanie czynności audytowych/administracyjnych musi być realizowane przy użyciu interfejsu graficznego GUI przeglądarki WWW lub dedykowanej aplikacji.
* Dane powinny być przechowywane w relacyjnej bazie danych lub innej horyzontalnie skalowanej, dystrybuowanej bazie danych, dostępnej komercyjnie.
* Mechanizm musi oferować funkcję exportu raportów do formatu .pdf, .html, .xml, .csv.
* Działanie komponentu rozliczalności/audytu systemu pocztowego nie może powodować opóźnień w dostarczaniu/odbieraniu wiadomości dla adresatów oraz nadawców zarówno wewnętrznych jak i zewnętrznych. Jak również nie może wpływać na wydajność działania systemu SEPP w tym spowalniać pracy użytkownikom końcowym SEPP.

**3.7.** **Komponent ochrony przed wyciekiem poufnych informacji DLP (Data Loss Prevention**

Oferowane rozwiązanie systemu pocztowego musi posiadać moduł/mechanizm DLP.

Wymagane jest, aby komponent zawierał:

* Możliwość przeglądania incydentów DLP oraz ich wyszukiwanie na podstawie odbiorcy, nadawcy, tematu wiadomości
* Możliwość definiowania wzorców, słowników w tym również na podstawie wyrażeń regularnych, ciągu znaków lub słów kluczowych dot. danych podlegających ochronie np. PESEL, IDKadrowe itp.
* Możliwość przesyłania do użytkowników informacji o naruszeniu zasad polityki bezpieczeństwa (w języku polskim) za pomocą email.
* Możliwość automatycznego blokowania wiadomości objętych ochroną
* Możliwość zbierania logów o zaistniałych incydentach
* Możliwość obsługi polskich znaków diakrytycznych

**3.8. Komponent migracji danych z obecnego systemu pocztowego**

Wymagane jest zapewnienie mechanizmu do migracji. Komponent musi oferować współistnienie (wzajemną pracę) na czas migracji danych dwóch systemów (z obecnie wykorzystywanego opartego o technologię Lotus Domino/Notes oraz systemu poczty e-mail dostarczonego przez Wykonawcę) transparentną dla użytkowników końcowych. Użytkownicy poczty e-mail bazującej na środowisku dostarczonym przez Wykonawcę i Lotus Domino/Notes muszą mieć zapewnioną funkcjonalność bezstratnej wymiany poczty między sobą, muszą mieć możliwość zapraszania się na spotkania, podglądania statusu dostępności/zajętości terminów w kalendarzu dla użytkowników z obcego systemu (poczty
e-mail bazującej na środowisku dostarczonym przez Wykonawcę i/lub Lotus Domino/Notes). Podczas migracji musi być zapewniona prawidłowa konwersja adresacji Lotus Notes na SMTP. Migracja nie może wpływać na pracę użytkowników końcowych i musi być dokonywana w tle pracy użytkownika.

Proces migracji do nowego rozwiązania wymaga wsparcia dla migracji następujących składników poczty Lotus Notes do nowego systemu:

1. kalendarzy, zadań,
2. uprawnień do skrzynki pocztowej,
3. uprawnień do skrzynki funkcyjnej,
4. użytkowników delegowanych do folderów w skrzynce Lotus Notes (uprawnień ACL na folderach skrzynki Lotus Notes),
5. list dystrybucyjnych,
6. skrzynek zasobowych takich jak rezerwacja sal konferencyjnych, itp.,

- oferowane rozwiązanie do migracji nie może wymagać zaangażowania użytkowników końcowych w procesie migracji

- oferowane rozwiązanie do migracji musi oferować możliwość przeprowadzenia migracji
z jednego centralnego miejsca

- oferowane rozwiązanie do migracji musi ułatwiać wykonywanie z jednego miejsca następujących funkcji administracyjnych, dzięki którym sprawniej administrator będzie mógł zarządzać przebiegiem migracji:

* + Ukrywanie/wyłączanie kont użytkowników po migracji w obecnym systemie poczty, lub inny mechanizm zapewniający dostarczanie poczty do użytkownika migrowanego do nowego systemu.
	+ Migrowanie aliasów internetowych oraz skrzynek grupowych/funkcyjnych

wykorzystywanych przez Lotus Notes.

**3.9. Komponent monitorowania całego środowiska serwerowego**

W celu usprawnienia zarządzania systemem należy wdrożyć centralny systemu monitorowania całego oferowanego środowiska systemu poczty.

Poprzez centralne monitorowanie należy rozumieć:

1. Monitorowanie dostępności i wydajności systemów całego środowiska serwerowego i aplikacyjnego, w tym gromadzenie danych i parametrów
z funkcjonowania sieci, systemów operacyjnych, usług systemowych, komponentów oprogramowania, serwerów aplikacyjnych.
2. Monitorowanie dostępności i wydajności, w szczególności śledzenie
i gromadzenie danych i parametrów działania wdrożonego systemu poczty poprzez predefiniowanie reguły do monitorowania wszystkich krytycznych komponentów oferowanego systemu poczty elektronicznej
3. Korelację zdarzeń z wszystkich monitorowanych systemów i ich prezentację
w formie graficznej na centralnej konsoli.
4. Implementację konsoli zarządczej umożliwiającej pełną kontrolę nad gromadzonymi danymi, informującą o stanach awaryjnych oraz pozwalającą na reagowanie na stany awaryjne.
	* Mechanizm musi zawierać wbudowany model uprawnień umożliwiający nadawanie uprawnień dostępu oraz poziomu ról dla administratorów w ramach podległej jednostki organizacyjnej
	* Mechanizm musi posiadać centralne repozytorium danych
	* Mechanizm musi posiadać możliwość definiowania kryteriów generowania alarmów po przekroczeniu zadanych progów, jak również funkcja automatycznego powiadamiania administratora za pomocą (e-mail)
	* Interfejs dostępowy poprzez przeglądarkę internetową

System monitorowania ma obejmować wszystkie dostarczone komponenty oprogramowania
i infrastruktury.

**3.10. Komponent backupu całego środowiska system zarządzania backupem powinien:**

W celu zwiększenia bezpieczeństwa wymagane jest dostarczenie i wdrożenie systemu backupu w dla całego środowiska systemu pocztowego. Serwer backupu musi pracować
w trybie klastra w przypadku awarii (lokalizacji Podstawowej) serwera backupu musi być dostępny z (lokalizacji Zapasowej) w zakresie pełnej funkcjonalności.

Komponent backupu powinien:

1. Wspierać backup wszystkich systemów operacyjnych zainstalowanych
w wirtualnych maszynach oraz samych maszyn wirtualnych.
2. Umożliwiać odzyskiwanie całych obrazów maszyn wirtualnych z obrazów, oraz pojedynczych plików z systemu plików znajdujących się wewnątrz maszyny wirtualnej
3. Współpracować z centralnym systemem zarządzania środowiskiem witalizacyjnym zastosowanym przez Wykonawcę oraz serwerami niezarządzanymi typu (standalone)
4. Wspierać najnowsze rozwiązania wirtualizacyjne tj. VMware, Hyper-V, i inne.
5. Umożliwiać pracę w środowisku klastrowym niezależnie od aktywności węzła klastra pocztowego
6. Rozwiązanie musi korzystać z mechanizmów VSS (Windows Volume Shadow Copy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows
7. Posiadać wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji przestrzeni dyskowej
8. Posiadać możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych
9. Posiadać centralną konsolę zarządzania całym środowiskiem backupu. Dostęp do konsoli zarządzającej GUI musi być realizowany przez przeglądarkę www
10. Umożliwiać integrację z bazą użytkowników opartą o usługę katalogową
11. Umożliwiać szyfrowanie danych podlegających backupowi
12. Posiadać wbudowany model uprawnień umożliwiający nadawanie uprawnień dostępu dla administratorów w ramach podległej jednostki organizacyjnej
13. Obsługiwać urządzenia taśmowe i dyskowe, służące do przechowywania kopii zapasowych i archiwizacji danych.
14. Przechowywać informacje o wykonanych kopiach, harmonogramach oraz nośnikach
w relacyjnej bazie danych. Proces tworzenia kopii zapasowej oraz odtwarzania danych powinien być procesem transakcyjnym. Ze względów bezpieczeństwa system powinien mieć możliwość wykonania mirroring’u tej bazy danych. Jednocześnie musi istnieć możliwość wykonani kopii zapasowej na taśmy w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności i wydajności.
15. Umożliwiać definiowanie w sposób centralny, procesów jednej konsoli polityki tworzenia kopii zapasowych, tj. określenia, jakie dane, kiedy i gdzie powinny być składowane (definiowanie harmonogramu Backupu)
16. Umożliwiać realizowanie raz zdefiniowanej polityki backupu w sposób automatyczny, bez konieczności ingerencji operatora. System powinien umożliwić także wykonywanie określonej akcji (zatrzymanie procesów, wykonanie backupu i ponowne uruchomienie).
17. Wykonywać kopie zapasowe w sposób przyrostowy i całościowy.
18. Mieć możliwość zdefiniowania czasu ważności kopii danych, tj. czasu, w którym usunięte dane są przechowywane na nośnikach taśmowych bądź dyskowych.
19. Mieć możliwość jednoczesnego tworzenia kopii zapasowych na różnego rodzaju nośniki (taśmy, dyski).
20. Mieć możliwość prowadzenia wersyfikacji polityki realizowania kopii zapasowych – definiowanie ilości przechowywanych wersji backup’owanych zasobów
21. Mieć możliwość jednoczesnego Backup’owania wielu klientów (zasobów) na urządzenia dyskowe. System bez ingerencji operatora powinien przenieść dane
z dysków na taśmy. Metoda ta umożliwi znaczne zredukowanie czasu backupu.
22. Umożliwiać tworzenie kopii zapasowych tzw. On-linie z oferowanego serwera pocztowego oraz baz danych bez konieczności zatrzymywania pracy serwera
23. Bez udziału operatora zarządzać położeniem danych – system optymalizuje położenie danych na taśmach pod kątem optymalnego wykorzystania nośników.
24. Bez udziału operatora optymalizować liczbę zapisanych taśm (przenoszenie danych pomiędzy taśmami w celu zwolnienia nośników i ponownego użycia)
25. Bez udziału operatora grupować na taśmie, grupie taśm dane z grupy serwerów, jednego serwera lub systemu plików.
26. Mieć możliwość tworzenia przez serwer backupów najświeższego obrazu pełnego backupu dla serwerów na bazie już zabezpieczonych danych. Proces ten powinien odbywać się bez konieczności komunikacji pomiędzy serwerem backupów i serwerem backupującym.
27. Zarządzać backupami na poziomie pojedynczych plików.
28. Posiadać możliwość odtwarzania kopii zapasowej z dowolnego punktu w czasie.
29. Posiadać Funkcję „Checkpoint restores” dla odtwarzania danych w przypadku przerwania transmisji od miejsca gdzie nastąpiła przerwa.
30. System musi realizować funkcje archiwizacji danych – kopia danych niepodlegających modyfikacji.
31. Umożliwiać odtwarzanie danych w dowolne wskazane miejsce dyskowe.
32. Umożliwiać tworzenie jak i odtwarzanie kopii zapasowych z wykorzystaniem struktury sieciowej SAN (Storage Area Network) oraz LAN
33. Powinien posiadać możliwość przywracania kopii skrzynek pocztowych bez konieczności zatrzymywania serwera pocztowego.

**4. Minimalne wymagania sprzętowe na potrzeby systemu.**

Wykonawca w ramach realizacji projektu oszacuje wymagania odnośnie całej niezbędnej infrastruktury sprzętowo-systemowej wraz z niezbędnym okablowaniem dla platformy wirtualizacji i centralizacji m.in. ilość sztuk, zasobów sprzętowych, mocy obliczeniowej, maszyn wirtualnych, ilości pamięci RAM, ilości procesorów, rozmiaru zasobów dyskowych, rozmiaru macierzy, oraz urządzeń sieci LAN, SAN itp. Wykonawca uwzględni również oprogramowanie serwerowe w tym systemy operacyjne, systemy wirtualizacji, system backupu, tak by zaoferowana platforma systemowo-sprzętowa spełniała wymogi centralizacji i wirtualizacji całego rozwiązania. Była skalowalna, stabilna i niezawodna. Dostarczone urządzenia sieci LAN, SAN muszą współpracować z infrastrukturą posiadaną w obiektach Datacenter u Zamawiającego, oraz muszą umożliwiać podłączenie i współpracę
z urządzeniami wskazanymi w Rozdziale II. Wykonawca dostarczy zainstaluje i skonfiguruje kompletną niezbędną infrastrukturę serwerowo-sprzętową wraz z oprogramowaniem
i licencjami z uwzględnieniem, poniżej podanych parametrów. Wszystkie połączenia komunikacyjne dla danego, pojedynczego ośrodka, tj. (FC, LAN itp.) muszą być redundantne tzn. (minimum 2 kanały transmisji na połączenie realizujące te same funkcje komunikacyjne). Zamawiający wymaga również redundancji dla dostarczonego sprzętu w zakresie zasilaczy
w dostarczonych urządzeniach dla danego, pojedynczego ośrodka.

**4.1. Minimalne parametry dla serwerów (na potrzeby wirtualizacji):**

Zamawiający wymaga dostarczenia takich samych serwerów pocztowych na potrzeby realizacji przedmiotu zamówienia. Przy czym na jeden ośrodek CPD musi przypadać nie więcej niż 4 fizyczne serwery. Ilość ośrodków CPD - 2, dostarczone serwery do obydwu ośrodków CPD muszą mieć tą samą wydajność. Łączna wydajność serwerów pocztowych
w jednym ośrodku nie może być mniejsza niż wynik 10000 punktów w teście SPECint2006 Rate Value dostępnym na stronie www.spec.org.

Wykonawca dostarczy konsole zarządzające umożliwiające zarządzanie wszystkimi serwerami w danym ośrodku z jednego miejsca w danym ośrodku.

|  |  |
| --- | --- |
| **Elementy konfiguracji /pojedynczego serwera** | **Wymagania minimalne** |
| Typ obudowy | Przystosowana do montażu w szafie rack 19" |
| Pamięć RAM | 512 GB z możliwością rozbudowy o 100% |
| Dysk twarde wewnętrzne | Zainstalowane 2 szt. o pojemności 300 GB SAS min 10K rpm  |
| Karty FC | 2 szt dwuportowe min.8 Gb/s |
| Karty sieciowe  | 2 szt. dwuportowe 10Gb/s |
| Karta sieciowa wbudowana | 1 szt. dwuportowa 1GE |
| Karta graficzna | zintegrowana |
| Napęd DVD | wewnętrzny |
| Zasilacze |  Min. 2 szt. typu Hot-Plug, redundantne |
| Chłodzenie | Zestaw wentylatorów redundantnych typu Hot-Plug |
| Zarządzanie | Serwer musi mieć możliwość zdalnego zarządzania poprzez interfejs, www lub za pomocą konsoli: pozwalającej na zdalne wyłączenie, włączenie, restart podgląd logów sprzętowych serwera. |
| Wsparcie dla systemów wirtualizacyjnych | wymagane |
| Wsparcie dla systemów operacyjnych | Windows, Linux lub Unix |

**4.2. Minimalne parametry dla pojedynczej macierzy dyskowej w ośrodku:**

 (Wykonawca dostarczy 2 szt.)

|  |  |
| --- | --- |
| **Elementy konfiguracji** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być dostarczona w oddzielnej szafie/szafach rack. Przystosowana do montażu w szafie/szafach rack 19” lub dostarczona w specjalnie przygotowanej dla niej własnej obudowie.  |
|  Architektura | Oferowany system dyskowy musi składać się z pojedyńczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedyńczą macierz uznaje się rozwiązanie, w którym wszystkie kontrolery wbudowane wewnętrznie w ramach jednej macierzy, rozwiązanie takie musi gwarantować zarządzanie z jednego interfejsu GUI, CLI. Wszystkie krytyczne komponenty macierzy tj. kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą mieć możliwość wymiany w trakcie pracy macierzy. |
| Obsługa dysków | Macierz musi obsługiwać dyski SAS, Nearline SAS, SSD lub Flash Drive.  |
| Redundancja | Macierz musi cechować brak pojedyńczego punktu awarii. Awaria dowolnej, całej półki dyskowej nie może powodować utraty dostępu do pozostałych zainstalowanych półek dyskowych.Wszystkie połączenia pomiędzy elementami składowymi macierzy (wszystkie ścieżki) muszą być redundantne. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap. System musi się skłądać, z co najmniej dwóch kontrolerów pracujących w trybie active-active.Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania –odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy.  |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać, co najmniej poziomy RAID 5,6,10. Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową.  |
| Tryb pracy kontrolerów macierzowych | Macierz musi być wyposażona w min. dwa symetryczne kontrolery pracujące w trybie active-active. Kontrolery muszą pracować w trybie wysokiej dostęponości tzn. w przypadku awarii jednego kontrolera inny kontroler automatycznie przejmuje jedo funkcje, czyli udostępnia klientom (tzw. hostom) wszystkie zdefiniowane w macierzy zasoby.  |
| Pamięć cache | 64GB rozszerzalne do 128GB  |
| Interfejsy | Macierz musi posiadać, co najmniej 8 zew. portów FC, o proędkości min. 8 Gb/s. Porty nie mogą być duplikowane za pomocą przełączników SAN, duplikatorów portów oraz innych form wirtualizacji zasobów pamięci masowych i sieci SAN. |
| Typy obsługiwanej replikacji macierzowej minimum | Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów. Macierz musi mieć możliwość replikacji synchronicznej, asynchronicznej, flashcopy. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym jak i w trybie typu Thin Provisioning. Należy dostarczyć wymagane licencje. |
| Przestrzeń dyskowa | Min całkowita netto 600 TiB, możliwość rozbudowy do min. 800 TiB. Jeżeli powyższa funkcjonalność wymaga dodatkowych licencji, wymagane jest dostarczenie odpowiednich licencji do rozbudowy. Wykonawca przy szacowaniu wymaganej przestrzeni dyskowej na potrzeby SEPP dodatkowo uwzględni wymaganą przestrzeń dyskową na potrzeby wymagań opisanych w pkt. 3.6. Komponent rozliczalności/audytu systemu pocztowego. |
| Wydajność macierzy | Min. wydajność IOPS = 4700 (optymalna do zaoferowanego rozwiązania, tak by zagwarantować wydajność i stabilność całego systemu dla podanej liczby użytkowników |
| Dynamiczne zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać dynamiczne zwiększanie pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych dla korzystających z tego wolumenu hostów.Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje należy je dostarczyć dla całej pojemności.  |
| Optymalizacja wykorzystania zasobów wewnętrznych) | Optymalne wykorzystanie dysków SSD, poprzez analizowanie obciążenia wolumenów logicznych na poziomie ich elementów (extent) a następnie automatycznie przenoszenie najbardziej aktywnych na szybkie dyski SSD. |
| Podłączenie zew. systemów operacyjnych  | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności, (co najmniej dwoma ścieżkami). Macierz dyskowa musi wspierać obsługę minimum 32 hostów podłączonych poprzez sieć SAN. Musi wspierać podłączenie systemów operacyjnych Windows, Linux, AIX, UNIX oraz zastosowane rozwiązanie, wirtualizatora. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. kopii migawkowej danych (snapshot, point in time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Należy dostarczyć wymagane licencje. |
| Zarządzanie | Dostęp administracyjny do macierzy poprzez sieć Ethernet, za pomocą graficznego interfejsu użytkownika za pomocą przeglądarki internetowej, lub aplikacji dostarczonej przez producenta.Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego.Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych. |
| Waga | Poniżej 500 kg na macierz. W przypadku przekroczenia tej wagi możliwe jest zastosowanie rozwiązań rozkładających obciążenia na większej powierzchni.  |

**4.3. Minimalne parametry dla pojedynczej biblioteki taśmowej w ośrodku:**

 (Wykonawca dostarczy 2 szt.)

|  |  |
| --- | --- |
| **Elementy konfiguracji** | **Wymagania minimalne** |
| Typ obudowy | Biblioteka musi być przystosowana do montażu w szafie rack 19", lub być wyposażona we własną szafę rack. Wszystkie komponenty niezbędne do instalacji muszą zostać dostarczone (szyny, śruby, itd.) |
| Robot | Mechanizm robota odpowiedzialny za automatyczne podawanie taśm do napędów i odkładnie ich do slotów po zakończonym zapisie/odczycie |
| Napędy taśmowe | Biblioteka musi być wyposażona w minimum 6 napędów LTO-8 FC. o wydajności, co najmniej 300 MB/s ( bez kompresji) każdy. |
| Interfejs zewnętrzne | Każdy napęd musi być wyposażony w 2 interfejsy FC 8Gb/s. |
| Sloty na taśmy | Biblioteka musi być wyposażona w minimum 100 slotów na taśmy oraz co najmniej 4 tzw. "mail slots" umożliwiające wymianę pojedynczej taśmy bez konieczności wyjmowania z modułu całego magazynka z taśmami. |
| Nośniki Danych | Wszystkie sloty w bibliotece\* (minimum 100) obsadzone taśmami LTO-8 (o pojemności pojedynczej taśmy, co najmniej 6 TB - bez uwzględniania kompresji danych) wraz z etykietami\*\* (barcode) oraz 4 szt. taśm czyszczących dla dostarczonych napedów wraz z etykietami\*\* (barcode).Dodatkowo 20 szt. taśm LTO-8 wraz z etykietami, \*\*(barcode) jako rezerwa. |
| Możliwość rozbudowy | Biblioteka musi zapewniać możliwość rozbudowy |
| Sposób zarządzania | Biblioteka musi umożliwiać lokalne zarządzanie przy użyciu panelu użytkownika oraz możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej. Biblioteka musi umożliwiać monitorowanie stanu biblioteki oraz napędów, konfiguracji oraz diagnostyki. Wsparcie dla protokołu SNMP. |
| Niezawodność | Biblioteka musi być wyposażona w redundantne moduły zasilające oraz wymianę uszkodzonego modułu w trybie on-line. Biblioteka musi umożliwiać automatyczne przełączenie ścieżek danych pomiędzy dwoma portami FC napędu taśmowego w przypadku awarii jednego z tych portów. |
| Dodatkowe funkcjonalności | Biblioteka musi być wyposażona w czytnik kodów kreskowych. Napędy LTO-8 muszą posiadać wsparcie dla taśm typu WORM oraz umożliwiać sprzętowe szyfrowanie AES 256-bit. |
| Obsługa systemów | Windows, UNIX, Linux |
| Współpraca z oprogramowaniem | IBM Tivoli Storage Manager, HP Data Protector |

**4.4. Minimalne parametry dla urządzeń przełączniki FC**

(Wykonawca dostarczy odpowiednią ilość przełączników FC dla całego systemu)

|  |  |
| --- | --- |
| **Elementy konfiguracji** | **Wymagania minimalne** |
| Obudowa i zasilanie | Przełącznik FC musi zapewniać techniczną możliwość montażu w szafir rack 19” dostarczonej w ramach zamówienia. Komponenty (szyny, śruby itp.) niezbędne do instalacji dostarczonych przełączników. Musi posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie na „gorąco” bez przerywania pracy przełącznika. |
| Konfiguracja portów | Wszystkie wymagane funkcje muszą być dostępne dla wszystkich dla wszystkich portów FC przełącznika. Rodzaj obsługiwanych portów: E,F, Mirror Port, Diagnostic Port. |
| Technologia | Przełącznik FC musi być wykonany w technologi FC 16Gb/s i posiadać możliwość pracy portów FC z prędkościami 16,10,8,4 Gb/s z funkcja autonegocjacji prędkości. Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.  |
| Trunking | Możliwość agregacji połączeń pomiędzy przełącznikami (trunking) na poziomie poszczególnych ramek. Musi posiadać możliwość balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. Musi posiadać mechanizm szyfrowania i kompresji przesyłanych danych pomiędzy przełącznikami FC w sieci fabric.  |
| Zoning | Przełącznik FC musi udostępniać usługę Name Server Zoning – tworzenie stref (zon) w oparciu o bazę danych nazw serwerów. Musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN. |
| Bezpieczeństwo | Przełącznik FC musi posiadać wsparcie dla mechanizmów zwiększających poziom bezpieczeństwa:- możliwość uwierzytelniania (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP- możliwość uwierzytelniania (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP- kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów.- szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2-szyfrowanie komunikacji narzędzi administracyjnych za pomocą HTTPS- obsługa SNMP v3 Przełącznik FC musi posiadać wsparcie dla mechanizmów zwiększających poziom bezpieczeństwa przez możliwość definiowania zakresu uprawnień administratora.  |
| Funkcjonalność  | Wsparcie dla N\_Port ID Virtualization (NPIV). Przełącznik musi umożliwiać wprowadzenie ograniczenia prędkości dla dowolnego portu lub portów. Musi być możliwość określenia limitów niższych niż wynegocjowana prędkość portu. Musi umożliwiać kategoryzację ruchu między inicjatorem i targetem oraz przydzielaniem takiej pary urządzeń do kategorii o wysokim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi być konfigurowana za pomocą standardowych narzędzi do konfiguracji zoningu.  |
| Diagnostyka | Przełącznik musi być wyposażony w narzędzia do logowania zdarzeń poprzez mechanizm „syslog”. |
| Zarządzanie | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z trybem graficznym.Musi zapewniać możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy.Musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet a pomocą protokołu DHCP oraz statycznie. |

**4.5. Minimalne parametry dla szafy rack 19” o wysokości 42U z modułami PDU**

(Wykonawca dostarczy odpowiednią ilość szaf dla całego systemu)

|  |  |
| --- | --- |
| **Elementy konfiguracji** | **Wymagania minimalne** |
| Obudowa | RACK 19 cali o wysokości 42 U i szerokości nie więcej niż 60x100 cm, wyposażona w drzwi przednie i tylne zamykane, boczne ściany zdejmowane. Szafa musi być wyposażona w kółka umożliwiające przemieszczanie szafy w przypadku zmiany lokalizacji.  |
| Zasilanie | System zasilania każdej z szaf serwerowych powinien zostać wyposażony, w co najmniej dwa niezależne PDU, z których Wykonawca powinien zapewnić odpowiednią ilość gniazd zasilających w każdej z szaf umożliwiających podłączenie dostarczonego sprzętu z nadmiarowością rzędu 5%. Przy założeniu, iż dostarczone urządzenia przez Wykonawcę wymagają więcej mocy z każdego PDU niż pozwalają na to zabezpieczenia posiadane na pojedynczy obwód –C32 przez Zamawiającego Wykonawca powinien dostarczyć wielokrotność PDU. Kable zasilające, PDU powinny zostać zakończone wtykami jednofazowymi 32A. |
| Waga | Całkowita waga pojedynczej szafy wraz z kompletnym wyposażeniem nie może przekraczać 500 kg.  |

**4.6. Minimalne parametry dla stacji zarządzających – 2 szt.:**

|  |  |
| --- | --- |
| **Elementy konfiguracji pojedynczej stacji** | **Wymagania minimalne** |
| Procesor | Procesor i7 2 core (2, 8GHz) lub równoważny |
| Pamięć  | 32 GB RAM |
| Ekran  | 14” powłoka antyrefleksyjna o rozdzielczości 1920x1080 |
| Dysk | 1TB |
| Porty USB | 3 szt. min 1 USB 3.0 |
| Karta sieciowa | 1GBit |
| Port HDMI | Tak |
| Karta WiFi | 802.11 a/b/g/n |
| Bluetooth | Tak |
| Stacja dokująca | Tak |
| Torba | Tak |
| Mysz bezprzewodowa | Tak |
| Oprogramowanie | MS Windows 10 Professional 64-bitMS Office 2016 Standard |

**4.7. Minimalne parametry dla monitorów LED – 4 szt.:**

|  |  |
| --- | --- |
| **Elementy konfiguracji** | **Wymagania minimalne** |
| Rozdzielczość nominalna  | 1920 x 1080 (Full HD) piksele |
| Porty wejścia/wyjścia | 1 x D-Sub, 1 x DisplayPort, 1 x HDMI, 1 x DVI, |
| Przekątna  | 32 cali |
| Typ matrycy | matowa |
| Rodzaj matrycy | IPS |
| Rodzaj podświetlenia | LED |

**5. Szkolenia administracyjne.**

Wykonawca w ramach realizacji Umowy przeprowadzi szkolenia dla wyznaczonych administratorów Zamawiającego z wszystkich elementów systemu dostarczonego rozwiązania z uwzględnieniem poniższych zapisów.

 Zakres szkoleń powinien obejmować:

* 1. Szkolenia dla 3 administratorów KGP Zamawiającego z dostarczonych elementów infrastruktury z zakresu budowy architektury, instalacji, konfiguracji i administracji
	(serwery, macierze, biblioteki taśmowe, urządzeń/mechanizmów równoważenia obciążenia)
	2. Zaawansowane certyfikowane szkolenia dla 3 administratorów KGP z zakresu instalacji, konfiguracji, administracji zarządzania aplikacjami serwerowymi
	i klienckimi systemu SEPP oraz rozwiązywania problemów z dostarczonymi
	w ramach realizacji Umowy tj. (systemu poczty, systemu wirtualizacji, systemu backupu, systemu audytowego, systemu monitoringu, systemu operacyjnego, administracja siecią i urządzeniami SAN, bazy danych.)
	3. Szkolenie dla 36 administratorów jednostek KGP/KWP/KSP w zakresie administracji i zarządzania użytkownikami dostarczoną aplikacją serwerową
	w ramach jednostki organizacyjnej oraz aplikacją kliencką. Szkolenie powinno być przeprowadzone w dwóch turach.
	4. Warsztaty/szkolenie dla 40 kluczowych użytkowników KGP/KSP/KWP/SP
	w zakresie obsługi aplikacji dostępowej interfejsu web klienta dostarczonego systemu poczty.
	5. Szkolenia muszą odbywać się w certyfikowanym ośrodku szkoleniowym
	na terenie Warszawy, zajęcia prowadzone przez wykwalifikowany personel
	i zakończyć się wydaniem imiennych certyfikatów dla uczestników szkolenia.
	6. Szkolenia muszą obejmować wykłady teoretyczne i laboratoria praktyczne. Muszą być przeprowadzone w języku polskim, a materiały szkoleniowe powinny być dostarczone w języku polskim lub angielskim. Materiały dydaktyczne i instrukcje odzwierciedlać będą całokształt zagadnień poruszanych na szkoleniu, przygotowane zostaną dla każdego uczestnika w formie papierowej. Zamawiający dopuszcza wersję elektroniczną materiałów.
	7. W przypadku szkolenia/warsztatu przewidzianego na dłużej niż 1 dzień Wykonawca zapewni zakwaterowanie dla wyznaczonych na szkolenia osób z jednostek organizacyjnych KWP/SP zlokalizowanych poza Warszawą.
	8. Terminy szkoleń zostaną ustalone z Zamawiającym.
1. **Budowa systemu dostępowego do zasobów Systemu Elektronicznej Poczty Policji (SEPP)**

**1.** **Opis Środowiska Zamawiającego:**

Aktualne środowisko sieciowe oparte jest na urządzeniach Cisco, Brocade. System zarządzania zamawiającego realizowany jest za pomocą oprogramowania CISCO Prime Infrastructure, Cisco LMS, CSM, DCMN, Cisco Firepower Management Center, Juniper STRM.

W infrastrukturze sieciowej wykorzystywane są między innymi protokoły sieciowe
i rozwiązania: EIGRP, STP, FabricPath. Ponadto infrastruktura sieciowa jest umieszczona
w dwóch ośrodkach CPD połączonych za pomocą czterech łączy każde po 10 Gb.
W środowisku zamawiającego, przez użytkownika końcowego używane są następujące systemy operacyjne: Windows XP, Vista, 7, 8, 10, Mac OS X, Linux/Unix.

**2**. **Wymagania ogólne**

1. Wszystkie parametry podane w wymaganiach są wymaganiami min., jakie winny spełniać Urządzenia.
2. Urządzenia oraz Oprogramowanie winny zostać zamontowane oraz skonfigurowane
w obiektach KGP wskazanych przez Zamawiającego zgodnie z wymaganiem szczegółowo opisanym w punkcie 4. Środowisko sieciowe Zamawiającego zostało opisane w pkt. 1.
3. Jeżeli nie są wyszczególnione specyficzne warunki świadczenia usług gwarancyjnych obowiązujące wymagania minimalne tj. 36 miesięcy świadczenia usługi gwarancyjnej.
4. Jeżeli nie nadmieniono to należy uznać, że wszystkie Urządzenia powinny być dostarczone wraz z Oprogramowaniem.
5. Dodatkowo, jeśli nie wskazano to należy uznać, że wszystkie Urządzenia powinny być dostarczone wraz z niezbędnym do instalacji Urządzeń okablowaniem.
6. O ile inaczej nie zaznaczono, wszelkie zapisy zawierające parametry techniczne należy odczytywać, jako parametry minimalne.
7. Wykonawca w celu dostępu do serwerowni Zamawiającego winien okazać poświadczenie dostępu do informacji niejawnych, co najmniej o klauzuli poufne dla wszystkich pracowników wchodzących na teren serwerowni lub zaświadczenie o niekaralności.
8. Oferowane produkty nie mogą znajdować się na liście urządzeń, dla których ogłoszono informację o terminie zakończenia produkcji lub datę zaprzestania świadczenia wsparcia.
9. Zaproponowane przez Wykonawcę urządzenie musi posiadać autoryzowany serwis techniczny producenta na terytorium Unii Europejskiej
10. Wraz z dostarczonym sprzętem Wykonawca zobowiązany jest dostarczyć odpowiadające mu instrukcje i sterowniki producenta sprzętu.
11. Dostarczane Urządzenia muszą być kompatybilne z uruchomionymi u Zamawiającego systemami zarządzania. W przypadku braku takiej kompatybilności Wykonawca musi zapewnić system zarządzania dedykowany dla takiego urządzenia.
12. Zamawiający wymaga przedstawienia pełnej konfiguracji dostarczanych produktów wraz z podaniem nazwy producenta i modelu urządzenia. W przypadku zaoferowania produktów równoważnych, Wykonawca wraz z ofertą powinien złożyć opis parametrów technicznych proponowanego sprzętu z podaniem nazwy producenta
i modelu produktu, pozwalający zweryfikować przedstawioną ofertę ze wszystkimi minimalnymi parametrami technicznymi wymaganymi przez Zamawiającego.
Z dołączonej dokumentacji musi wynikać w sposób jednoznaczny, że oferowany sprzęt spełnia minimalne parametry techniczne wymagane przez Zamawiającego. Opis parametrów technicznych proponowanego sprzętu może mieć formę folderów, opisów technicznych, kart sprzętu itp.
13. Dopuszcza się dla uniknięcia niejednoznaczności opisów dokumentację w języku angielskim.

**3. Opis szczegółowych wymagań dla systemu dostępowego**

Wykonawca zobowiązany jest do:

 **3.1.   Dostarczenia systemu zabezpieczeń opartych o urządzenia i oprogramowanie**

**3.1.1.  Loadbalancer (urządzenie równoważenia ruchu) – 2 kpl**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

 Wymagania minimalne dla urządzeń:

1. System musi realizować co najmniej następujące funkcje:
	1. Rozkład ruchu pomiędzy serwerami aplikacji Web i serwerami pocztowymi
	2. Selektywny http caching
	3. Selektywna kompresja danych
	4. Terminowanie sesji SSL
	5. Filtrowanie pakietów
	6. Optymalizacja i akceleracja aplikacji
	7. Moduł SSL VPN
	8. Globalnego równoważenia obciążenia za pomocą protokołu DNS
	9. Ochrona przed atakami na aplikacje i serwery WWW
2. Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia
3. Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej
4. System musi posiadać co najmniej następujące metody równoważenia obciążenia:
	1. Cykliczna
	2. Ważona
	3. Najmniejsza liczba połączeń
	4. Najszybsza odpowiedź serwera
	5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera
	6. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie
	7. Dynamicznie ważona oparta na SNMP/WMI
	8. Definiowana na podstawie grupy priorytetów dla serwerów
5. Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:
	1. Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów
	2. Obsługa protokołów: http, tcp, xml, rtsp, sip
	3. Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS
6. Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami
7. Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego
8. Producent systemu musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego opisanego
w punkcie 6. Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend.
9. Rozwiązanie musi pracować w trybie pełnego proxy.
10. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
11. Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji
12. Funkcjonalność lokalnego równoważenia obciążenia
	1. Wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego
	2. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera
	3. Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług
	4. Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID
	5. Wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP
13. Optymalizacja i akceleracja aplikacji
	1. Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci:
		1. LAN
		2. WAN
		3. CELL (komórkowy)
	2. Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta.
	3. Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control)
	4. Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP
	5. Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:
		1. Listy dozwolonych URI
		2. Listy wykluczonych URI
		3. Listy kompresowalnych Content-Type
		4. Listy wykluczonych Content-Type
14. Moduł SSL VPN musi posiadać co najmniej następujące funkcje:
	1. Obsługa trybów: portal dostępowy, tunel aplikacyjny, tunel szyfrowany SSL VPN
	2. Obsługa IPv6
	3. Definiowanie polityki dostępu poprzez graficzny edytor. W graficznym edytorze można wybierać konkretne obiekty konfiguracyjne (elementy uwierzytelnienia, konfiguracji dostępu, dostępnych zasobów, itp.) oraz najczęstsze powtarzające się konfiguracje kopiować do makr.
	4. Obsługa szyfrowania danych przy użyciu protokołu DTLS
	5. Wsparcie dla SSO poprzez SAML 2.0 w trybie IdP (Identity Provider) jak i SP (Service Provider), wsparcie dla profilu SAML ECP
	6. Wsparcie dla OAuth 2.0 w trybie: klient, serwer zasobów (resource server) oraz serwer autoryzacji (authorization server).
	7. Obsługa nie mniej niż 40 tysięcy jednocześnie uwierzytelnionych sesji z wykorzystaniem SAML lub OAuth, z możliwością rozbudowy do 100 tysięcy.
	8. Uwierzytelnienie użytkowników przy wykorzystaniu: formularzy, certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius, LDAP, Oracle Access Manager, kart smart cards, uwierzytelnienia wieloskładnikowego
	9. Wsparcie dla platform klientów VPN: Windows, Mac, Linux, Android, iPad, iPhone oraz przeglądarek: IE, Firefox, Chrome
	10. Inspekcja stacji klienta sprawdzająca poprawność pracy aplikacji (antywirus, firewall, dostępność plików, rejestrów (Windows), procesów, CPU ID (Windows), HDD ID (Windows)) dla systemów Windows, Linux, Mac
	11. Możliwość automatycznego aktualizowania wersji oprogramowania klienta dla systemów Windows
	12. Możliwość utworzenia bezpiecznego wirtualnego pulpitu na czas trwania sesji użytkownika
	13. Wsparcie dla CAPTCHA
	14. Wsparcie dla tzw. "step-up authentication"
	15. Wsparcie dla Microsoft ActiveSync oraz Outlook Anywhere z wykorzystaniem NTLM
	16. Możliwość generacji jednorazowych tokenów (OTP) i wysyłanie ich mailem lub integrując się z zewnętrzną bramką poprzez SMS
	17. Możliwość definiowania per grupa użytkowników (np. Active Directory)/lub per użytkownik limitu pasma przydzielonego dla użytkownika do ściągania informacji
	18. Możliwość wykorzystania wirtualnej klawiatury do procesu logowania użytkownika
	19. Definiowanie reguł dostępu użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI.
	20. Funkcja SSO (gromadzenia parametrów uwierzytelnienia użytkownika - credential caching)
	21. Możliwość budowania dynamicznej strony www, w zależności od użytkownika, jego przynależności do danej grupy, zawierającej udostępnione aplikacje
	22. Wsparcie dla VMWare View oraz Citrix XenApp/XenDesktop
	23. Wsparcie dla proxy PCoIP, Blast oraz Blast Extreme dla rozwiązania VMware Horizon
	24. Wsparcie dla przekierowania USB dla VMware Horizon
	25. Obsługa funkcji szyfrowania site-to-site IPSec VPN
	26. Moduł SSL VPN musi obsługiwać tryb wymuszający nawiązanie połączenia VPN, tzw. tryb always-on dla systemu Windows
	27. Wsparcie dla zewnętrznego uwierzytelnienia w dostępie SSL VPN tzw. captive portal
	28. System musi umożliwiać kompresję przesyłanych danych
	29. Moduł SSL VPN musi posiadać mechanizm raportowy, uwzględniający nie mniej niż:
		1. Błędne próby uwierzytelnienia
		2. Informacje o użytkownikach
		3. Zasoby, do których odwołują się użytkownicy
		4. Lokalizacja (Geolocation)
	30. Obsługa nie mniej niż 500 jednocześnie pracujących użytkowników SSL VPN z możliwością licencyjnej rozbudowy do 100 tysięcy licencji.
	31. Licencjonowanie musi odbywać się per ilość jednocześnie pracujących użytkowników z możliwością instalacji klienta SSL VPN na dowolnej ilości urządzeń/stacji roboczych.
15. Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach którego zapewni:
	1. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI
	2. Rozdzielanie ruchu korzystając co najmniej z metod:
		1. Cykliczna
		2. Ważona
		3. Na podstawie adresów IP klienta usługi (topologii)
		4. Obciążenia serwera
		5. Najmniejszej liczby połączeń
	3. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera dns klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji
	4. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS
	5. Ochronę serwerów DNS z wykorzystanie DNSSEC a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu
	6. Możliwość pracy, jako serwer DNS obsługujący następujące rekordy: A, NS, CNAME, SOA, PTR, HINFO, MX, TXT, AFSDB, SIG, KEY, AAAA, LOC, SRV, NAPTR, KX, CERT, DNAME, OPT, DS, SSHFP, IPSECKEY, RRSIG, NSEC, DNSKEY, DHCID, NSEC3, NSEC3PARAM, HIP, TKEY, TSIG, IXFR, AXFR, ANY, ZXFR, DLV
	7. Konwersja rekordów między IPv4 i IPv6
	8. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji
	9. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych
	10. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich
	11. Możliwość bezpośredniego odpytywania serwerów o obciążenie
	12. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji
16. WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:
	1. wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a.
	2. typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT)
	3. przejścia pomiędzy URL-ami (servletami)
	4. dopuszczalne metody http,
	5. dopuszczalne cookie,
	6. dopuszczalne parametry w polityce,
	7. parametry dynamiczne,
	8. typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany)
	9. oraz dopuszczalne parametry w danym serwlecie
	10. długość zapytań
	11. nazwy hosta
	12. wystąpień i długość parametrów (per każdy parametr)
	13. wystąpień i długości nagłówków
	14. wystąpień i długości cookies
	15. oczekiwanych typów znaków per każdy parametr
	16. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku
	17. URL-i podatnych na CSRF
17. Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego
18. WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej
19. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń)
20. Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego.
	1. W szczególności na podstawie publicznego ruchu produkcyjnego.
	2. Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać nadużycia w procesie nauki.
21. Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.
22. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr
23. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa
24. Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http
25. WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.
26. WAF musi posiadać mechanizmy ochrony przed atakami:
	1. SQL Injection,
	2. Cross-Site Scripting,
	3. Cross-Site Request Forgery,
	4. Session hijacking,
	5. Command Injection,
	6. Cookie/Session Poisoning,
	7. Parameter/Form Tampering,
	8. Forceful Browsing,
	9. Brute Force Login,
	10. Web Scraping
	11. Cookie manipulation/poisoning
	12. Dynamic Parameter tampering
	13. Buffer Overflow
	14. Stealth Commanding
	15. Unused HTTP Methods
	16. Malicious File Uploads
	17. Hidden Field Manipulation
27. Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.
28. Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta).
29. Wstrzykiwanie przez WAF dodatkowych informacji (cookie, tokeny, JavaScript), nie powinno powodować degradacji wydajności oferowanego urządzenia.
30. System musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie:
	1. Host
	2. URN
	3. Nagłówków
	4. Cookie
31. Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do:
	1. Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2
	2. System Operacyjny: Windows, Linux, UNIX
	3. Język aplikacji, frameworki: ASP, ASP .NET, PHP, Java, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Java Servlets/JSP, Lotus Domino, Macromedia ColdFusion, JRun, Outlook Web Access, SSI, WebDAV, JQuery, SSI, WebDAV, jQuery
	4. Serwer WWW: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy.
32. WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http)
33. WAF musi blokować ataki typu Slow Loris
34. WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:
	1. Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania
	2. Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless broser
	3. Sygnatur botów
	4. Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).
35. System powinien umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub brute force.
36. System powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.
37. Moduł ochrony przed DDoS powinien wykrywać ataki per:
	1. Source IP,
	2. Obszar geolokacyjny,
	3. URL,
	4. Globalnie - website
38. Powinna istnieć możliwość przypisania różnych poziomów detekcji ataków (D)DoS dla danych URL-i portala. Np. /infoportal/\* powinien posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS niż /portal/\*.
39. System powinien wykrywać i chronić przed atakami DDoS na tzw. ciężkie serwlety, czyli serwlety wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych.
	1. Wykrycie ataku na ciężkie serwlety powinno opierać się przynajmniej o ilość zapytań (TPS) oraz czas odpowiedzi
40. System powinien umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS.
	1. System powinien umożliwiać definicję maksymalnego czasu próbki ruchu,
	2. Maksymalnej pojemności próbki ruchu,
	3. Interwału czasowego pomiędzy pobieraniem próbki ruchu.
41. Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia
42. WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.
43. WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a.
44. WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem
45. WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a
46. W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP.
47. WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON.
48. WAF powinien wyświetlać stron blokowania (błędu) w technologiach AJAX i JSON
49. WAF musi posiadać wsparcie dla Google Web Toolkit
50. WAF musi posiadać możliwość ochrony komunikacji XML poprzez:
	1. walidację Schema/WSDL,
	2. wybór dozwolonych metod SOAP,
	3. szyfrację /deszyfrację fragmentów wiadomości SOAP,
	4. Wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie),
	5. Definiowanie możliwości użycia załączników wiadomości SOAP,
	6. Włączanie/wyłączanie podążania za odnośnikami do schematów SOAP,
	7. Walidację SOAPAction Header,
	8. Włączanie/wyłączanie możliwości użycia DTD
	9. Włączanie/wyłączanie możliwości użycia zewnętrznych referencji
	10. Włączanie/wyłączanie możliwości użycia początkowych białych znaków
	11. Włączanie/wyłączanie możliwości użycia numerycznych nazw
	12. Włączanie/wyłączanie możliwości użycia Processing Instructions
	13. Włączanie/wyłączanie możliwości użycia CDATA
	14. Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace
	15. Ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów
	16. Definicję dopuszczalnych znaków
	17. Definicję sygnatur.
51. Funkcja sprawdzania reputacji adresów IP dostających się do chronionych aplikacji.
52. Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania. Subskrypcja serwisu reputacyjnego nie jest przedmiotem niniejszego postępowania.
53. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia.
54. WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel.
55. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać:
	1. Directory traversal
	2. Kodowanie typu %u
	3. Kodowanie typu IIS backslash
	4. IIS Unicode codepoints
	5. Bare byte decoding
	6. Apache whitespace
	7. Bad unescape
	8. Wstrzykiwanie komentarzy (np. <!-- -->)
56. Mechanizm normalizacji powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania.
57. Urządzenie musi wspierać następujące tryby pracy:
	1. Tryb wykrywania, logowania i blokowania ataków
	2. Tryb wykrywania i logowania ataków bez blokowania
	3. Tryb uczenia się bez blokowania
	4. Tryb uczenia się z blokowaniem i logowaniem
58. WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach.
59. WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression.
	1. Włączenie funkcji maskowania numerów kart kredytowych nie powinno powodować degradacji wydajności oferowanego urządzenia.
60. WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6
61. Rozwiązanie musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego w warstwie 3 i 4 ISO/OSI
62. Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w system interfejsu graficznego.
63. Reguły definiujące ruch muszą zawierać oprócz adresu, adresów IP również możliwość wskazanie lokalizacji (w ruchu źródłowym oraz ruchu docelowym) tzw. geolokalizacja
64. Rozwiązanie musi chronić przed atakami typu flood, sweep, teardrop oraz smurf.
65. Rozwiązanie musi wspierać Remote Triggered Black Hole.
66. Rozwiązanie musi umożliwiać uruchomienie proxy SSH, które umożliwia np. blokowanie ściąganie lub wgrywanie plików po SCP lub SFTP, ustawienie czy użytkownik ma dostęp do shella czy nie.
67. Rozwiązanie musi wykrywać nieprawidłowe protokoły przechodzące przez otwarte porty (np. otwarty port 80 dla ruchu http, gdy na tym porcie odbywa się ruch ssh).
68. Jedno urządzeni musi obsłużyć sprzętowo minimum 130 milionów SYN cookies na sekundę
69. Rozwiązanie musi obsłużyć sprzętowo mitygację minimum 100 wektorów ataków DDoS
70. Rozwiązanie musi posiadać wsparcie obsługi protokołów routingowych BGP, OSPF, RIP, ISIS, BFD.
71. Szczegółowe wymagania w zakresie modułu do ochrony DoS/DDoS
72. System musi zapewniać ochronę DoS/DDoS przynajmniej dla protokołów HTTP/HTTPS, SIP, DNS
73. Wykrywanie anomalii w protokołach i pakietach SYN/ICMP/ACK/UDP/TCP/IP4/IP6/DNS/ARP
74. Dla każdego obsługiwanego wektora ataku możliwość wybrania stanu, wyłączony (nie zbierane są statystyki, brak mitygacji), tryb uczenia się (zbierana są statystyki, brak mitygacji), tylko tryb detekcji (tryb uczenia się, powiadamianie), tryb mitygacji (tryb uczenia się, powiadamiania, mitygacja).
75. W trybie mitygacji możliwość ustawienia trybu pracy czy:
76. mitygacja i detekcja następują w pełni automatycznie
77. detekcja następuje manualnie a mitygacja automatycznie
78. zarówno detekcja jak i mitygacja następują manualnie
79. Możliwość tworzenie własnych czarnych list, które będą wypełniane adresem IP i aplikowane w regułach firewallowych w zależności od kierunku ruchu: adres źródłowy, adres docelowy, zarówno adres źródłowy i docelowy
80. Możliwość ustawienia we wspieranych wektorach ataków czy w przypadku ataku automatycznie wykrywany jest adres IP
81. wykryty adres IP musi zostawać dodany do wskazanej dowolnie wybranej czarnej listy
82. możliwość zdecydowania czy wykryte adresy IP dla konkretnego wektora ataku ma zostać wysłany do routerów BGP.
83. System musi umożliwiać behawioralną analizę ruchu sieciowego. System musi umożliwiać włączenie lub wyłączenie tego trybu oraz pracę w trybie nauki.
84. Rozwiązanie musi posiadać możliwość automatycznego dostosowania progów DDoS.
85. Na podstawie wykrytych anomalii system musi automatycznie budować i aplikować sygnaturę ataku.
86. Raportowanie ataków DDoS:
* System musi umożliwiać jednocześnie zapisywać informacje o atakach DDoS na urządzeniu i wysyłać je do zewnętrznego systemu
* W czasie rzeczywistym informację o wektorze ataku (w tym również utworzonym na podstawie behawioralnej analizy), status ataku, wykryte atakujące adresy IP), ilość pakietów na sekundę (aktualnie, w ciągu 5 minut, w ciągu godziny), szczegóły ustawionych progów dla danego wektora ataku, ilość odrzuconych pakietów na sekundę
* W systemie raportowania muszą znaleźć się informację na temat źródłowego adresu atakującego, jaki i adres, port był atakowany, typ ataku, podjętej akcji, numer identyfikujący atak
* Możliwość wyświetlenie odświeżanego (co wskazany interwał czasu) dashboardu zawierającego informacje na temat czasu trwania ataku, jego ważności, co go spowodowało, mitygacji, zablokowanych adresów IP, z jakiego kraju pochodził atak, wektora ataku, kategorii ataku, średniej ilość transakcji na sekundę, mapy świata pokazującego atakujących lub atakowanych w zależności od źródła pakietu
* Możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID
1. System musi posiadać co najmniej następujące interfejsy administracyjne:
	1. GUI przy wykorzystaniu protokołu https
	2. Zarządzanie poprzez SSH
	3. Zarządzanie poprzez SOAP-SSL
	4. Zarządzanie poprzez API REST
2. Autoryzacja administratorów systemu musi bazować na rolach użytkowników
3. System musi posiadać funkcje przywiązywania sesji (*Session persistence*) przy wykorzystaniu co najmniej następujących atrybutów:Cookie (hash, rewrite, custom, insert, passive)
	1. Adres źródła
	2. SIP call ID
	3. Identyfikator sesji SSL
	4. Microsoft Terminal Services (RDP) – nazwa użytkownika
	5. Adres docelowy
	6. Tworzone przez administratora systemu przy wykorzystaniu języka skryptowego
	z punktu 5
4. System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
5. System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.
6. System musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.
7. Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy.
8. Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów.
9. System musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.
10. System musi obsługiwać sieci VLAN w standardzie 802.1q
11. System musi obsługiwać agregację linków w standardzie 802.3ad (LACP)
12. System musi obsługiwać Jumbo Frames
13. System musi posiadać funkcjonalność bramy VXLAN oraz NVGRE
14. System musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody)
15. System musi świadczyć, co najmniej następujące usługi w warstwach 4-7:
	1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http
	2. Ukrywanie zasobów
	3. Zmiana odpowiedzi serwera
	4. Przepisywanie odpowiedzi (response rewriting)
	5. Ochrona przed atakami typu DoS/DDoS
	6. Ochrona przed atakami typu SYN Flood
	7. Multipleksowanie połączeń http
16. System musi posiadać następujące funkcje zarządzania siecią:
	1. Obsługa protokołu SNMP v1/v2c/v3
	2. Zewnętrzny syslog
	3. Zbieranie danych i ich wyświetlanie
	4. Zbieranie danych zgodnie z ustawieniami administratora
	5. Osobna brama domyślna dla interfejsu zarządzającego
	6. Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot)
	7. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy)
	8. Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
17. System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
18. System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.
19. System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:
	1. Czas odpowiedzi per serwer
	2. Czas odpowiedzi per URI
	3. Ilość sesji użytkownika
	4. Przepustowość
	5. Adres źródła
	6. Kraj
	7. User Agent (wykorzystywana przez klienta aplikacja)
	8. Metoda dostępu
20. System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.
21. Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.
22. Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.
23. Rozwiązanie musi oferować stworzenie minimum 1000 partycji administracyjnych oraz 1000 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra.
24. Rozwiązania musi być dostarczone w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1
25. Urządzenie musi umożliwiać podział urządzenia na wirtualne części, przy czym każda taka część musi pracować logicznie jako niezależne urządzenie z niezależnym oprogramowaniem (każda cześć może posiadać inną wersję oprogramowania oraz osobną tablice routingu). Urządzenie musi umożliwić podział na minimum 8 wirtualnych części.
26. W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych
27. Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu
28. Klaster wysokiej dostępności musi zapewniać synchronizację:
	1. Konfiguracji
	2. Stanu połączeń
	3. Przywiązywania sesji (*Session persistence*)
29. Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod:
	1. Weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover)
	2. Weryfikacji stanu pracy urządzenia poprzez interfejs szeregowy (serial failover)
30. Wymagana jest 3 letnia gwarancja producenta. W obrębie gwarancji zawarte musi być:
	1. Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta
	2. Sposób obsługi zgłoszeń gwarancyjnych w trybie 7x24
	3. Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki
	4. W razie awarii dysk pozostaje u Zamawiającego
31. System w postaci jednego urządzenia musi spełniać wymogi przedstawione w tabeli 1.

**Tabela 1. Wymagania dla jednego urządzenia systemu**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania** |
|  | Pamięć | Nie mniej niż 256GB |
|  | Dysk twardy | Dwa dyski SSD pracujące w RAID1 o pojemności nie mniejszej niż 960GB każdy |
|  | Przepływność dla warstwy 4 | Nie mniej niż 80 Gbps |
|  | Przepływność dla warstwy 7 | Nie mniej niż 70 Gbps |
|  | Przepustowość wewnętrznej magistrali | Nie mniej niż 960 Gbps |
|  | Ilość jednocześnie obsługiwanych połączeń | Nie mniej niż 140 milionów |
|  | Ilość transakcji SSL na sekundę dla klucza o długości 2048 | Nie mniej niż 63 tysięcy, licencyjna możliwość aktualizacji do 280 tysięcy |
|  | Ilość transakcji SSL na sekundę dla szyfru ECDSA P-256  | Nie mniej niż 55 tysięcy, licencyjna możliwość aktualizacji do 200 tysięcy |
|  | Przepływność ruchu szyfrowanego | Nie mniej niż 25 Gbps, licencyjna możliwość aktualizacji do 70 Gbps |
|  | Ilość zapytań na sekundę w warstwie 7 | Nie mniej niż 1.8 miliona, licencyjna możliwość aktualizacji do 5.5miliona |
|  | Kompresja sprzętowa | Nie mniej niż 70 Gbps |
|  | Sprzętowa ochrona DDoS | Nie mniej niż 130 milionów SYN cookies na sekundę |
|  | Gęstość interfejsów | Nie mniej niż osiem interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX) lub SFP+ 10G (SR lub LR), nie mniej niż sześć interfejsów z możliwością obsadzenia wkładkami 40Gb QSFP+, oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USBNależy zapewnić 4 wkładki 10 Gigabit Ethernet SFP+ oraz 2 wkładki 40 Gigabit Ethernet QSFP+ oraz 2 kable QSFP+ na 4 duplex LC.Dopuszcza się tylko moduły dostarczane przez producenta urządzenia. |
|  | Zarządzanie | Panel i wyświetlacz LCD (dotykowy) z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu urządzenia, wyświetlania informacji o systemieFunkcjonalność „Always On Management” |
|  | Obudowa | Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 1 U |
|  | Zasilanie | Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC |
|  | Wymagana certyfikacja | EN 300 386 V1.6.1 (2012)EN 55032:2012 Class AEN 61000-3-2:2014EN 61000-3-3:2013EN 55024:2010EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013 |
|  | MTBF platformy | Nie mniej niż 62 tysięcy godzin |

**3.1.2** **Dostarczenia urządzeń Firewall – 2 kpl**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

 Wymagania minimalne dla urządzeń **Firewall**:

**Wymagania ogólne:**

1.   System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.

2.   System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 39Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 20Gbps dla kontroli zawartości (w tym kontrola antywirus, antyspyware i IPS web filtering) i obsługiwać nie mniej niż 8 000 000 jednoczesnych sesji.

3.  System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 100/1G/10G, 16 portów 1/10G SFP/SFP+, 4 porty 40G/100G QSFP+ z czego w każdym urządzeniu po 8 portów SFP+ musi zostać obsadzone wkładkami 10GE SR i 2 porty QSFP+ muszą zostać obsadzone wkładkami 40GE, pochodzącymi od tego samego producenta co firewall celem uniknięcia problemów z serwisowaniem urządzeń.

4.       System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.

5.       Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).

6.       System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.

7.    System zabezpieczeń firewall musi obsługiwać nie mniej 125 wirtualnych routerów posiadających odrębne tablice routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż RIP, BGP, OSPF

8.       System zabezpieczeń 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).

9.       Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).

10.   System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

11.   System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.

12.   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 portach. Wydajność kontroli firewalla stanowego i firewalla aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 39Gbps

13.   Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).

14.   Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.

15.   Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.

16.   System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

17.   System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

18.   System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

19.   System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

20.   System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

21.   System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.

22.   System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

23.   System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

24.   System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.

25.   System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

26.   System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

**Identyfikacja użytkowników:**

1.       System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

2.       System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.

3.       System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

4.       Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

**Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day**

1.       System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

2.       System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.

3.       System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

4.       System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

5.       System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

6.       System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

7.       System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

8.       System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

9.       System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

10.   System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

11.   System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

12.   System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

13.   System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

14.   System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

15.   System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

16.   System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

**Wymagania dot. NAT, DoS, IPSEC VPN, SSL VPN, QoS**

1.       System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

2.       System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

3.       System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

4.       System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.

5.       System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

6.       System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.

7.       System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.

8.       System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

9.       System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

**Obsługa środowiska wirtualnego vmware**

1.       System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

**Zarządzanie i raportowanie**

2.       Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.

3.       System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

4.       System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.

5.       System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

6.       System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

7.       Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

8.       System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.

9.       System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

10.   System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.

11.   System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.

12.   System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.

13.   System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.

14.   System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

15.   System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.

16.   System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.

17.   System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

18.   System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

19.   System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

20.   Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |
|  |  |  |
|  |  |  |
|  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |
|  |  |  |
|  |  |  |

**3.1.3   Przełączniki - 8 kpl**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Wymagania minimalne dla przełączników:

 1.  Przełącznik musi zapewniać:

a.  minimum 48 portów 10/25GE definiowanych za pomocą wkładek SFP/SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej

b.  minimum 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP powinien mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps

2.   Parametry wydajnościowe:

a.   Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika

b.   Obsługiwana łączna przepływnośc (pasmo) min. 3 Tbps

c.   Obsługiwana łączna przepustowosć pakietowa przełącznika min. 2,000 mpps

d.   Opóźnienie przełączania pakietów nie większe niż 2 µs

3.   Przełącznik musi spełniać następujące wymagania dla warstwy L2:

a.       Trunking IEEE 802.1Q VLAN;

b.       Wsparcie dla 4094 sieci VLAN;

c.       Funkcjonalność izolowania portów znajdujących się w tym samym VLAN

d.       Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC

e.       IEEE 802.1w Rapid Spanning Tree (RST)

f.        IEEE 802.1s Multiple Spanning Tree (MST)

g.       Wsparcie sprzętowe dla tunelowania QinQ

h.       Spanning Tree Guard lub odpowiadający;

i.        Internet Group Management Protocol (IGMP) Versions 2, 3;

j.        Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych

 przełącznikach (MCEC, vPC lub odpowiadający mechanizm)

k.       Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością

 zgrupowania minimum 32 interfejsów fizycznych w wiązce

l.        Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

4.  Przełącznik musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie warstwy L3

a. Sprzętowe przełączanie pakietów w warstwie L3

b. Routing w oparciu o trasy statyczne

c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.

d. Policy Based Routing (PBR) dla IPv4

e. VRRP v3

f. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)

g.Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta ·
 w tablicy routingu IP

h.Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast)

i. Wsparcie dla IGMPv3 oraz MSDP

j. Wsparcie dla minimum 32, 000 tras multicastowych

k.Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością

importu/eksportu tras (route leaking)

l. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)

m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list

5.  Przełącznik musi zapewniać możliwość rozszerzenia funkcjonalności o następujące mechanizmy związane z funkcjonalnością VXLAN:

a. Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint)

b. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway)

c. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast)
 z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności, PIM Anycast RP

d. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)

e. 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)

f. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)

6.   Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

a. Layer 2 IEEE 802.1p (CoS);

b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) w warstwach 2, 3, 4;

c. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;

d. Bezwzględne (strict-priority) kolejkowanie na wyjściu;

e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm

 odpowiadający

f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach

wejściowych i wyjściowych

g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach

 wyjściowych

h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb

7.   Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:

a. Wejściowe ACL (standardowe oraz rozszerzone);

b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy,

typ protokołu;

c. 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);

d. ACL oparte o VLAN-y (VACL);

e. ACL oparte o porty (PACL);

f. DHCP Snooping

g. ARP Inspection

h. IP Source Guard

i. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast,

multicast, broadcast

8.  Wymagania dotyczące zarządzania i zabezpieczenia przełącznika:

a. Port zarządzający 100/1000 Mbps;

b. Port konsoli CLI;

c. Zarządzanie In-band;

d. SSHv2;

e. Authentication, authorization, and accounting (AAA);

f. RADIUS;

g. TACACS+

h. Syslog;

i. SNMP v1, v2, v3;

j. RMON (przynajmniej grupy Events, Alarms)

k. Openflow 1.3

l. sFlow

m. IEEE 802.1ab LLDP

n. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)

o. Role-Based Access Control RBAC;

p. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)

q. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror)

r. Network Time Protocol (NTP);

s. Precision Time Protocol IEEE 1588

t. Diagnostyka procesu BOOT;

u. Ping

v. Traceroute

9.  Wymagania dotyczące narzędzi programowania i zarzadzania przełącznikiem:

a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API

b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika

c. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener musi mieć możliwość wykorzystywania portów fizycznych przełącznika.

d. Interfejs programistyczny REST API wraz z upublicznionym SDK

e. Możliwość zainstalowania klienta Chef

f. Możliwosć zainstalowania agenta Puppet

g. Wsparcie dls NETCONF i zarządzania poprzez XML

h. Wsparcie dla OpenStack Neutron plugin

10. Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony połączeń zasilających urządzenia

11. Oferowane przełączniki muszą być wyposażone w: 12 modułów 10GBase-SR oraz 12 modułów GLC-SX-MMD każdy pochodzącymi od tego samego producenta co switch celem uniknięcia problemów z serwisowaniem urządzeń.

12. Obudowa o rozmiarach maksymalnie 1RU (rack unit), musi być przeznaczona do montażu w szafie rackowej 19”

13. Wymagana jest 3 letnia gwarancja producenta. W obrębie gwarancji zawarte musi być:

* 1. Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta
	2. Sposób obsługi zgłoszeń gwarancyjnych w trybie 24x7
	3. Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki

**4****. Zakres prac do wykonania w ramach dostawy urządzeń do budowy systemu dostępowego SEPP**

Zamawiający wymaga:

1. Dostarczenie urządzeń z punktu 3 według  specyfikacji określonej przez Zamawiającego.
2. Transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. Instalację urządzeń w zakresie:
	1. fizycznej instalacji w szafach, w miejscu wskazanym przez Zamawiającego (2 lokalizacje na terenie Warszawy)
	2. Uruchomienia urządzeń z oprogramowaniem rekomendowanym przez producenta
	3. Konfiguracji urządzeń dostarczonych w ramach punktu 3
	4. Konfiguracji i instalacji licencji i polityk bezpieczeństwa dostarczanych urządzeń z pkt. 3
	5. Integracji dostarczanego rozwiązania ze środowiskiem DC Zamawiającego
	6. Instalacja nowych polityk bezpieczeństwa do nowo dostarczonego rozwiązania oraz przeniesienie obecnych polityk znajdujących się w systemie RBD Zamawiającego.
	7. Instalacja I konfiguracja systemu balansowania dla:
		1. nowego systemu SEPP
		2. przeniesienie obecnego systemu balansowania opartego o ACE30 do wydzielonego kontekstu dostarczanych balanserów
	8. Uruchomienia urządzeń w klastrach
	9. Uruchomienia funkcjonalności modułu wykrywania i zapobiegania włamań.
	10. Opracowania polityki bezpieczeństwa, analizy otrzymanych zdarzeń oraz optymalizację reguł w celu lepszej ochrony środowiska Zamawiającego.
	11. Podłączenia (okablowanie) urządzeń do infrastruktury Klienta. Okablowanie musi zostać dostarczone przez Wykonawcę.
	12. Uruchomienie i integracja systemów zarzadzania z dostarczonym systemem
	13. Przeprowadzenia certyfikowanych szkoleń dla 5 administratorów Zamawiającego w zakresie urządzeń bezpieczeństwa z pkt. 3.1.1, 3.1.2,
	14. Sporządzenie powykonawczej dokumentacji technicznej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.
	15. Podział dostarczanych urządzeń na min. 4 niezależne konteksty.

**5. Wymagania w zakresie usługi szkolenia certyfikowanego**

1. Wykonawca w ramach realizacji projektu zorganizuje certyfikowane szkolenia dla wyznaczonych pięciu administratorów Zamawiającego dotyczące urządzeń opisanych w punktach 3.1.1, 3.1.2 w certyfikowanych ośrodkach na terenie Warszawy. Dopuszczana jest realizacja szkoleń poza siedzibą Zamawiającego (tj. Warszawa); wówczas Wykonawca poniesie koszty dojazdu, zakwaterowania, akomodacji i wyżywienia;
2. Jeżeli nie ma na rynku polskim szkoleń certyfikowanych Wykonawca przeprowadzi warsztaty partnerskie dla dostarczanego rozwiązania.
3. Wykonawca zapewni zaplecze techniczno-dydaktyczne oraz zorganizuje szkolenie w dwóch turach w różnym okresie czasu.
4. Szkolenia powinny uwzględnić całościową wiedzę z zakresu budowy architektury, instalacji, konfiguracji i administracji dostarczanych urządzeń. Jeżeli zakres materiału realizowany jest na kilku szkoleniach należy przeprowadzić kompleksowe szkolenie uwzględniające materiał dla wszystkich modułów.
5. Szkolenie musi być przeprowadzone w języku polskim, a materiały instruktażowe powinny być dostarczone w języku polskim lub angielskim. Materiały dydaktyczne odzwierciedlać będą całokształt zagadnień poruszanych na szkoleniu, przygotowane zostaną dla każdego uczestnika w formie papierowej. Zamawiający dopuszcza wersję elektroniczną materiałów.
6. Szkolenie powinno być przeprowadzone dla 5 osób w dwóch turach po minimum 2 osoby na turę.
7. Wykonawca opracuje harmonogram szkoleń zawierający:
8. cel i projektowany zakres szkolenia,
9. informacje o zakresie tematycznym szkolenia,
10. metodę i formę szkolenia,
11. czas trwania szkolenia
12. Harmonogram, o którym mowa w pkt. 7 Wykonawca przedstawi do akceptacji Zamawiającego w terminie 10 Dni Roboczych przed rozpoczęciem danego rodzaju szkolenia.

9) Wykonawca wystawi dla każdego uczestnika szkolenia imienny certyfikat ·
w wersji papierowej i elektronicznej potwierdzający, że nabył on wiedzę zgodną · z celem szkolenia.