**Załącznik nr 1 do SIWZ**

**dot. sprawy nr: 31/DE/Z/2015**

**Przedmiot Zamówienia:**

1. dostawa, montaż, instalacja, konfiguracja, uruchomienie elementów środowiska informatycznego, tj. systemu ochrony poczty, systemu kontroli dostępu do zasobów sieciowych, przełącznika 10 GbE, systemu SIEM, skanera podatności sieci, rozbudowy klastra HPC, systemu poczty elektronicznej, szafy RACK wraz z integracją z istniejącym środowiskiem informatycznym Zamawiającego,
2. przeprowadzenie niezbędnych szkoleń,
3. wykonanie dokumentacji wykonawczej,
4. wykonanie dokumentacji powykonawczej,
5. przygotowanie procedur testowych i eksploatacyjnych
6. wykonanie testów akceptacyjnych
7. świadczenie usług serwisu gwarancyjnego, wsparcia technicznego, zapewnienie aktualności i ciągłości wszystkich dostarczanych licencji i subskrypcji w okresie 60 miesięcy od daty podpisania końcowego protokołu odbioru

**Ogólne wymagania dla Przedmiotu Zamówienia:**

1. Wykonawca musi uwzględnić w kosztach realizacji dostawę, montaż, instalację i podłączenie dostarczanych urządzeń do sieci strukturalnych Zamawiającego oraz koszty akcesoriów i osprzętu montażowo-instalacyjnego (stelaże, wysięgniki, prowadnice, uchwyty, śruby i nakrętki, łączówki, kable przyłączeniowe i zasilające, przewody, patchcordy, przejściówki, opaski, listwy, korytka itp.).
2. Wszystkie dostarczone urządzenia i systemy muszą być zamontowane, zainstalowane, skonfigurowane i uruchomione zgodnie z wymaganiami niniejszej specyfikacji. Wszystkie dostarczone produkty muszą być wyposażone we wszystkie niezbędne komponenty, podzespoły i licencje, obejmujące okres nie krótszy niż 60 miesięcy od daty podpisania protokołu odbioru końcowego.
3. Dla wdrożonych w ramach Przedmiotu Zamówienia systemów wymagane jest zapewnienie przez Wykonawcę szkoleń personelu IT Zamawiającego co najmniej w zakresie konfiguracji i administrowania wdrożonymi elementami systemu. Szkolenie powinno być przeprowadzone w języku polskim w siedzibie Zamawiającego. Każdy z dostarczanych systemów musi być objęty oddzielnym szkoleniem teoretycznym i praktycznym w wymiarze co najmniej 8 godzin roboczych.
4. Wykonawca zobowiązany jest do oznaczenia zainstalowanych urządzeń i połączeń za pomocą etykiet z kodami zgodnymi z metodologią stosowaną przez Zamawiającego.
5. Miejsca (pomieszczenia) wykonywania prac muszą zostać uporządkowane i przywrócone do stanu nie gorszego niż przed ich rozpoczęciem
6. Odbiory po zakończeniu każdego z etapów i odbiór końcowy przeprowadzone będą po wykonaniu testów akceptacyjnych i zakończeniu ich pozytywnym wynikiem i potwierdzane obustronnym podpisaniem bezusterkowego protokołu odbioru.

**Wymagania dotyczące dokumentacji powykonawczej:**

1. Dokumentacja powykonawcza powinna zawierać ostateczne wersje (wraz z komentarzami) plików konfiguracyjnych urządzeń i oprogramowania.
2. Kody na opisach i schematach w dokumentacji powykonawczej muszą być zgodne z faktycznymi oznaczeniami na etykietach urządzeń i połączeń
3. W dokumentacji należy zastosować schemat oznaczania kodowego zasobów używany u Zamawiającego.
4. Dokumentacja powykonawcza powinna zawierać co najemni ej:
   1. Opis rozwiązania wraz ze wskazaniem zastosowanych urządzeń i oprogramowania (producent, model, wersja) oraz ich ilości i rozmieszczenie w poszczególnych lokalizacjach
   2. Schematy rozmieszczenia, połączeń, przepływu danych i sterowania oraz komunikacji pomiędzy poszczególnymi elementami infrastruktury teleinformatycznej z uwzględnieniem połączeń w warstwie fizycznej i logicznej
   3. Oznaczenia urządzeń i połączeń zgodne ze schematem oznaczania kodowego zasobów używanym u Zamawiającego.
   4. Plany (schematy) rozmieszczenia urządzeń w poszczególnych szafach montażowo-dystrybucyjnych
   5. Wykazy uzgodnionych z Zamawiającym początkowych parametrów konfiguracyjnych urządzeń i oprogramowania (np. numeracja i nazewnictwo urządzeń, segmentów sieci, podsieci, sieci wirtualnych, , strefy i polityki bezpieczeństwa, listy kontroli dostępu itp)
   6. Zakres testów akceptacyjnych wraz z kryteriami sukcesu
   7. Wzory formularzy testów akceptacyjnych i protokołów odbiorów technicznych
5. W trakcie odbioru końcowego Wykonawca przekaże Zamawiającemu 1 egzemplarz dokumentacji powykonawczej w wersji papierowej i 1 egzemplarz w wersji elektronicznej.
6. Wykonawca przekaże na rzecz Zamawiającego majątkowe prawa autorskie do dokumentacji powykonawczej będącej częścią Przedmiot u Zamówienia

**Ogólne wymagania Zamawiającego dla stosowanych produktów, o ile wymagania szczegółowe dla produktów opisanych w dalszej części dokumentu nie stanowią inaczej:**

1. Wymagane jest, aby dostarczany sprzęt był fabrycznie nowy, kompletny i pochodził z legalnego kanału sprzedaży oraz nie posiadał żadnych wad prawnych
2. Wymagane jest aby dostarczany sprzęt był wyprodukowany nie wcześniej niż 6 miesięcy przed dniem zawarcia Umowy dotyczącej Przedmiotu Zamówienia
3. W przypadku licencji ograniczonych w czasie wymagane jest zapewnienie ich co najmniej na czas taki, jak okres serwisu.

**Warunki świadczenia usług serwisowych**

Wykonawca zobowiązany jest zapewnić usuwanie awarii oraz świadczenie wsparcia technicznego dla służb IT w zakresie rozwiązywania problemów wynikających z bieżącego funkcjonowania dostarczanych systemów. W przypadku świadczenia usług gwarancyjnych i/lub serwisowych w siedzibie Zamawiającego, Zamawiający nie ponosi żadnych dodatkowych kosztów związanych z dojazdem i zakwaterowaniem pracowników Wykonawcy.

Wykonawca zapewni następujące warunki zgłaszania incydentów poprzez prowadzenie ich rejestru:

1. Zgłoszenia serwisowe muszą być przyjmowane przez co najmniej następujące kanały: telefon, faks, e-mail, WWW
2. Każdemu zgłoszeniu musi zostać nadany unikalny numer (identyfikator), pozwalający na jego jednoznaczną identyfikację
3. Zgłoszenie musi zawierać datę, opis incydentu wraz z jego klasyfikacją, dane osoby zgłaszającej, dane osoby prowadzącej obsługę gwarancyjną lub serwisową
4. Wykonawca zapewni Zamawiającemu dostęp do systemu śledzenia stanu obsługi zgłoszenia. Dostęp ten musi być możliwy poprzez następujące kanały komunikacyjne: telefon, e-mail, WWW
5. Lista osób upoważnionych ze strony Zamawiającego do dokonywania zgłoszeń będzie określona w załączniku do protokołu odbioru końcowego.

Usługi serwisu, gwarancji i wsparcia technicznego muszą muszą być świadczone w języku polskim.

Klasyfikacja incydentów:

|  |  |  |
| --- | --- | --- |
| **Klasy incydentów** | **Opis** | **Możliwe rodzaje incydentu** |
| A – Wysoki | System nie funkcjonuje lub jego dysfunkcja ma krytyczny wpływ na działalność statutową Zamawiającego. | System nie działa i powoduje przerwę w działaniu innych krytycznych elementów sieci lub aplikacji. Awaria wszystkich elementów tworzących układ redundantny. Incydent skutkujący odpowiedzialnością prawną, spowodowaną niewydolnością wynikłą z niedostępności sieci lub aplikacji. Brak możliwości zastosowania rozwiązania tymczasowego. |
| B – Średni | Skuteczność (dostępność, wydajność, bezpieczeństwo) działania systemu jest wyraźnie obniżona, ale większość działań przebiega nieprzerwanie lub ujawnił się błąd utrudniający działanie Systemu w zakresie pełnej funkcjonalności. | Zidentyfikowane incydenty, które ustępują bez interwencji albo mogą być skutecznie ominięte w wyniku działania Zamawiającego lub dzięki zastosowaniu rozwiązania tymczasowego. Uszkodzenie jednego z kilku elementów tworzących układ redundantny. |
| C – Niski | Skuteczność (dostępność, wydajność, bezpieczeństwo) działania systemu jest nieznacznie obniżona lub użytkownicy potrzebują informacji lub pomocy, związanych z możliwościami produktu, instalacją systemu lub konfiguracją. | Incydenty nienaglące, o małym znaczeniu, zapytanie techniczne lub prośba o informacje. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasa incydentu** | **Gotowość** | **Czas reakcji [godziny]** | **Czas naprawy** |
| A – Wysoki | 8x5  Pon – Pt  7:00 – 15:00 | 2 | Następny dzień roboczy |
| B – Średni | 4 | 2 dni robocze |
| C – Niski | 8 | 5 dni roboczych |

Dopuszcza się zdalną (telefon, mail) obsługę incydentów klasy C bez konieczności przyjazdu inżyniera Wykonawcy po każdorazowym uzgodnieniu z Zamawiającym.

**ELEMENT 1**

**Ochrona poczty**

1. **Wstęp**

Przedmiotem postępowania jest zakup i wdrożenie oraz świadczenie usług serwisowych dla systemu ochrony poczty elektronicznej (zwany dalej **OE**) zbudowanego w oparciu o gateway’e pocztowe pełniące funkcje ochronne i obsługujące transmisję poczty do wnętrza sieci Zamawiającego i w odwrotnym kierunku.

System OE ma zapewnić ochronę przed spamem i wiadomościami email zawierającymi kod złośliwy oraz dodatkowe funkcjonalności, opisane poniżej, w zakresie kontroli i ochrony poczty elektronicznej Zamawiającego.

Należy przewidzieć redundantny układ systemu ochrony, (co najmniej 2 gateway’e pocztowe), który zapewnia obsługę poczty nawet w wypadku awarii jednego z elementów systemu.

Układ gateway’ów pocztowych będzie zrealizowany na bazie appliance’ów sprzętowych, na których działa oprogramowanie gateway’a pocztowego. Należy uwzględnić w ofercie dostawę odpowiednich ilości appliance’ów sprzętowych, dostosowanych do wymaganej wydajności.

Poza dostawą urządzeń, licencji i oprogramowania, w ramach postępowania należy zapewnić także:

* Dostęp do usług wsparcia technicznego producenta w okresie 5 lat od daty odbioru końcowego
* Wdrożenie systemu wg uzgodnień technicznych

Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług zostały przedstawione w dalszej części opisu.

1. **Wymagania ogólne**
2. Dostarczony system ma pochodzić od jednego producenta, włączając w to appliance’y sprzętowe.
3. Cały system OE ma obsługiwać w sumie 500 użytkowników Zamawiającego.
4. W ramach dostawy systemu ochrony należy zapewnić licencje na oprogramowanie ochronne i co najmniej dwa urządzenia typu appliance dedykowane do obsługi poczty elektronicznej (lub więcej, jeśli jest to wymagane dla spełnienia wymagań wydajnościowych) pracujące w HA.
5. W razie potrzeby rozbudowy systemu pod kątem wydajności dostarczone licencje muszą umożliwiać wdrożenie kolejnych gateway’i pocztowych opartych na appliance i/lub maszynach wirtualnych VMware, bez konieczności zmiany licencji, dokupowania ich lub zakupu dodatkowego oprogramowania.
6. **Szczegółowe wymagania dla platformy sprzętowej**

Każdy z dostarczonych appliance, na których będzie działało oprogramowanie gateway’a pocztowego, musi spełniać poniższe minimalne wymagania sprzętowe:

1. Możliwość instalacji w szafie montażowej 19”
2. Maksymalna wysokość obudowy - 1U
3. Co najmniej 2 dyski twarde pracujące w układzie RAID-1, zapewniające co najmniej 450GB przestrzeni dyskowej dla oprogramowania gateway’a pocztowego i na potrzeby lokalnej kwarantanny email
4. Minimum 3 wbudowane interfejsy UTP 1GE (10/100/1000)
5. Minimum 4GB RAM
6. Napęd CD/DVD
7. **Szczegółowe wymagania funkcjonalne**

**Wymagania dotyczące zarządzania Gateway’ami pocztowymi**

1. Interfejs zarządzający dostępny na każdym urządzeniu/maszynie wirtualnej osobno przez przeglądarkę internetową i połączenie https bez użycia maszyny wirtualnej Java
   1. GUI interfejsu zarządzania musi być wyposażone w konfigurowany pulpit (dashboard), na którym znajduje się podsumowanie najważniejszych parametrów Gateway’a i wyników ochrony poczty
   2. Musi istnieć możliwość zdefiniowania wielu kont administratorów i przypisania im uprawnień do wykonywania tylko pewnych czynności administracyjnych (co najmniej ograniczenie dostępu tylko do konfiguracji polityk bez możliwości zmian konfiguracji sieciowej, ograniczenie dostępu tylko do modułu raportowania, ograniczenie dostępu do konfiguracji szyfrowania poczty)
   3. Konta administratorów można tworzyć lokalnie w systemie oraz korzystać z zewnętrznych usług katalogowych dostępnych przez protokoły Radius i Kerberos
2. Oprogramowanie gatewayów pocztowych musi umożliwiać centralne zarządzanie wieloma gatewayami działającymi w klastrze jak i niezależnie bez konieczności zakupu dodatkowych licencji lub oprogramowania.
3. System musi posiadać wbudowane raportowanie, bez konieczności stosowania dodatkowego oprogramowania i zewnętrznych serwerów
   1. Raporty powinny być na podstawie predefiniowanych, gotowych szablonów
   2. Musi być możliwe także tworzenie własnych raportów
   3. Raporty mają być generowane na żądanie i okresowo, według zdefiniowanego harmonogramu
   4. Musi być możliwe zapisanie Raportu, co najmniej w formacie PDF, HTML, TXT
   5. Musi być możliwe automatyczne wysłanie raportu mailem pod wskazany adres
4. Interfejs zarządzający musi umożliwiać wizualizację przebiegu transakcji SMTP i przejścia wiadomości przez poszczególne filtry ochronne Gateway’a
5. Interfejs zarządzający musi umożliwiać administratorowi zarządzanie wiadomościami przechowywanymi w lokalnej kwarantannie.

**Wymagania dotyczące implementacji sieciowej**

1. Rozwiązanie powinno umożliwiać wdrożenie gateway’a pocztowego w trybie proxy aplikacyjnego (*mail relay*), routera (*transparent router*) oraz *transparent bridge*
   1. W każdym z trybów pracy powinna być zachowana taka sama funkcjonalność ochrony poczty przed spam i kodem złośliwym
2. Rozwiązanie musi posiadać wbudowane mechanizmy budowy klastra wysokiej dostępności (HA) oraz współdzielącego ruch dla rozłożenia obciążenia między urządzenia wchodzące w skład klastra.
3. Rozwiązanie ma działać w warstwie sieciowej (gateway poczty elektronicznej) i musi obsługiwać co najmniej protokoły SMTP i POP3, przy czym musi być możliwe określenie portów na jakich działają te protokoły
4. Gateway’e muszą umożliwiać wysyłanie wiadomości SNMP, syslog oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń
   1. Rozwiązanie powinno posiadać predefiniowane formaty logów, co najmniej w formacie HP/ArcSight, Splunk, McAfee SIEM/Nitro
5. Gateway’e muszą posiadać możliwość monitorowania z zewnątrz za pomocą SNMP
6. Gateway’e muszą posiadać wbudowane wydajne mechanizmy ograniczania skutków ataków typu Denial of Service (DoS) z wykorzystaniem poczty elektronicznej co najmniej takie, jak:
   1. Określenie minimalnego czasu pomiędzy komendami SMTP.
   2. Określenie minimalnej przepustowości przesyłania danych.
   3. Określenie maksymalnej liczby tzw. trywialnych komend SMTP
   4. Określenie maksymalnej ilości odbiorców wiadomości.
   5. Określenie maksymalnej długości połączenia SMTP.
   6. Określenie maksymalnej długości części domenowej adresu.
   7. Stosowanie technik zapobiegających przed atakami Directory Harvest, gdzie można zdefiniować ile procentowo odbiorców musi być niepoprawnych w stosunku do wszystkich by zablokować połączenie od nadawcy.
7. System musi posiadać mechanizmy routingu poczty elektronicznej – kierowania jej zależnie od domeny do różnych hostów (MTA, serwer pocztowy)
8. System ma zapewniać ochronę *anti-relay*.
9. System musi mieć możliwość ochrony przed spamem przez użycie graylistingu.

**Wymagania dotyczące tworzenia polityki działania Gateway’ów**

1. Każdy z gateway’ów pocztowych musi współpracować z serwerami Active Directory i LDAP pozwalając na autentykację odbiorcy poczty i stworzenie dokładnej polityki skanowania poczty uzależnionej od grup użytkowników lub poszczególnych użytkowników pochodzących z AD i LDAP
   1. Musi być zapewnione wsparcie co najmniej dla następujących rodzajów LDAP: AD, Lotus Domino, Novell NDS, Netscape/Sun iPlanet, MS Exchange, Generic LDAP Server v3
   2. Musi istnieć możliwość odpytania serwera AD/LDAP na bieżąco lub zdefiniowanie okresowej synchronizacji danych z AD/LDAP na Gateway
2. Integracja z AD/LDAP musi umożliwiać także realizację:
   1. maskowania realnych adresów email w zależności od wpisu w AD/LDAP
   2. decyzje o sposobie (ścieżce – route) dostarczenia poczty
3. Gateway pocztowy musi pozwalać na stworzenie dokładnej polityki skanowania zależnie od danej domeny pocztowej, adresu źródłowego/docelowego, użytkownika lub grupy użytkowników, numeru VLAN (w trybie *transparent bridge*)
   1. Musi być możliwe definiowanie równocześnie wielu polityk, których zastosowanie zależy od kolejności na liście polityk i w/w kryteriów
   2. Musi być możliwe tworzenie osobnych polityk dla wiadomości wychodzących i dla przychodzących
4. Sposób konfigurowania polityki działania Gateway’a pocztowego musi umożliwiać definiowanie kilku jednoczesnych reakcji na wykryte zdarzenie – na przykład:
   1. zablokowanie wiadomości i wysłanie niezależnego powiadomienia o tym zdarzeniu pod wskazany adres email
   2. przesłanie poczty do odbiorcy, a dodatkowo przesłanie jej kopii pod wskazany adres
   3. zablokowanie wiadomości i skierowanie jej do kwarantanny
5. Gateway’e pocztowe muszą usuwać z nagłówków wiadomości email informacje dotyczące wewnętrznej infrastruktury Zamawiającego, mogących posłużyć do jej rozpoznania przez osoby nieupoważnione
6. Rozwiązanie musi obsługiwać aliasy pocztowe oraz umożliwiać automatyczne, zależne od przyjętej konfiguracji, dodawanie do poczty wychodzącej zdefiniowanego zapisu tzw. *disclaimer*
7. Rozwiązanie, w ramach poszczególnych polityk, musi umożliwiać ograniczanie :
   1. Maksymalnej wielkości przesyłki pocztowej
   2. Maksymalnej wielkości załącznika do email
   3. Maksymalnej ilości załączników do email
8. Rozwiązanie musi umożliwiać definiowanie wirtualnych instancji działających na Gateway’u (wirtualne hosty)
   1. Wirtualne instancje muszą umożliwiać przydzielenie niezależnych adresacji IP, różnych od adresów Gateway’a dla ruchu wychodzącego i przychodzącego
   2. Musi być możliwe definiowanie niezależnych zestawów polityk określających funkcje ochronne dla poszczególnych wirtualnych instancji
   3. Musi być możliwe takie sterowanie przepływem poczty, żeby wiadomości przychodzące były obsługiwane przez Gateway, a poczta wychodząca przez wybraną wirtualną instancję
9. Rozwiązanie musi umożliwiać filtrowanie poczty pod kątem przesyłanych obrazów/zdjęć zawierających treści erotyczne i pornograficzne
   1. Filtr musi analizować obrazy/zdjęcia pod kątem ich zawartości w czasie rzeczywistym, na podstawie reputacji obrazu/zdjęcia
   2. Filtracja nie może wymagać wcześniejszego zarejestrowania blokowanych zdjęć / obrazów lub jakiegokolwiek innego uprzedniego określania, które zdjęcia/obrazy mają podlegać filtracji
10. Gateway musi umożliwiać filtrację poczty na podstawie jej zawartości
    1. Rozwiązanie musi przeprowadzać filtrowanie treści według zdefiniowanych reguł, w co najmniej 150 rodzajach/formatach przesyłanych plików
    2. Musi być możliwe filtrowanie wiadomości z załączonymi plikami na podstawie ich nazw
    3. Musi być możliwe filtrowanie wiadomości na podstawie ich wielkości
    4. Musi być możliwe blokowanie wiadomości zawierających załączniki zaszyfrowane lub spakowane z hasłem
11. Gateway musi posiadać wbudowany mechanizm przeciwdziałania wyciekowi danych (filtr DLP)
    1. Filtr DLP musi działać na tej samej platformie, co pozostałe funkcjonalności ochronne i nie może wymagać zastosowania dodatkowych licencji lub oprogramowania
    2. Musi istnieć możliwość zarejestrowania (zindeksowania) chronionych dokumentów bezpośrednio poprzez GUI Gateway’a pocztowego
    3. Poza zarejestrowaniem chronionych dokumentów musi być także możliwe określenie chronionych treści na podstawie słów kluczowych, fraz, wyrażeń regularnych i słowników (w tym słowników tworzonych samodzielnie przez Zamawiającego) zawierających słowa, frazy i wyrażenia regularne
    4. Moduł DLP musi posiadać predefiniowane reguły wykrywające dane dotyczące polskich danych osobowych, co najmniej numerów: PESEL, NIP, dowodów osobistych, REGON oraz paszportów

**Wymagania dotyczące obsługi szyfrowania poczty**

1. Każdy z Gateway’ów pocztowych musi umożliwiać szyfrowanie poczty elektronicznej korzystając z technologii:
   1. B2B (*Gateway – Gateway*) – szyfrowanie w tunelu TLS/SSL pomiędzy gateway’ami oraz między gateway’em a serwerem pocztowym, szyfrowanie S/MIME, szyfrowanie PGP
   2. B2U (*Gateway – User*) – szyfrowanie wiadomości pocztowej w taki sposób, aby jej odczytanie możliwe było po uwierzytelnieniu się odbiorcy na portalu web dostępnym poprzez HTTPS. Portal Web musi być obsługiwany bezpośrednio przez Gateway pocztowy
   3. System musi umożliwiać elastyczną definicję wiadomości, które mają być szyfrowane (co najmniej zależnie od odbiorcy, domeny pocztowej, treści wiadomości, określonych słów kluczowych w temacie wiadomości, specyficznych nagłówków dodanych do wiadomości pocztowej)
   4. System musi umożliwiać importowanie certyfikatów i ustalenie w polityce, który z nich zostanie użyty do uwierzytelnienia tuneli TLS/SSL z poszczególnymi odbiorcami (na podstawie ich domeny pocztowej i adresacji IP)
2. Wymagania dotyczące szyfrowania B2U
   1. Nie może być wymagane instalowanie na komputerze odbiorcy jakiegokolwiek dodatkowego oprogramowania poza wykorzystywanymi przez niego klientami poczty (dowolny klient poczty obsługujący SMTP i POP3) oraz przeglądarką web
   2. Użytkownicy muszą posiadać indywidualne konta w systemie web umożliwiającym odczytanie zaszyfrowanych wiadomości. Każdy użytkownik systemu musi posiadać unikalny klucz, którym szyfrowane są wiadomości
      1. Poza predefiniowanymi kontami użytkowników musi być też możliwe użycie samodzielnej rejestracji konta przez użytkownika
   3. System musi umożliwiać zarówno wysłanie całej wiadomości w postaci zaszyfrowanej do odbiorcy (wiadomości nie są przechowywane na gateway’u) oraz wysłanie tylko linku do wiadomości zaszyfrowanej przechowywanej na gateway’u
3. Musi istnieć możliwość zainstalowania oprogramowania Gateway’a pocztowego w taki sposób aby pełnił on dedykowaną rolę szyfrowania poczty, przekierowywanej do niego przez pozostałe Gateway’e zgodnie z warunkami ich polityki obsługi poczty
4. Żadna z metod szyfrowania poczty wymienionych powyżej nie może wymagać zakupu dodatkowych licencji, oprogramowania lub instalowania dodatkowych urządzeń

**Wymagania dotyczące wykrywania kodu złośliwego**

1. Gateway pocztowy musi być wyposażony w skaner anti-malware (AM) pochodzący od tego samego producenta, co całe oferowane rozwiązanie
2. Skaner AM musi wykorzystywać dzienne, automatyczne aktualizacje baz sygnatur antywirusowych
   1. Musi istnieć możliwość określenia częstotliwości i harmonogramu aktualizacji silnika AM i baz sygnatur
3. Skaner AM musi posiadać mechanizm wykrywający nowe zagrożenia w technologii „in the cloud” za pomocą serwisów reputacyjnych posiadanych przez producenta rozwiązania
   1. W razie wykrycia podejrzanego kodu/pliku i braku definicji w lokalnym pliku sygnatur anty-wirusowych, skaner AM musi mieć możliwość wysłania zapytania do centralnej bazy prowadzonej przez producenta rozwiązania o to czy dany plik/kod jest już znany i zakwalifikowany jako zagrożenie
   2. Zależnie od wyniku zapytania, skaner AM musi mieć możliwość podjęcia takiej samej reakcji jak w przypadku wykrycia zagrożenia na podstawie lokalnego pliku sygnatur
4. Skaner AM musi wykrywać i blokować oprogramowanie szpiegujące oraz wykrywać próby ataków typu PHISHING
5. Skaner AM musi wykrywać wykorzystanie mechanizmów kompresji (archiwizery, packery) używanych przez szkodliwe oprogramowanie i musi umożliwiać automatyczne skasowanie plików przygotowanych z ich użyciem
6. Skaner AM musi skanować media strumieniowe oraz umożliwiać wyłączanie ze skanowania określonych w polityce typów tych mediów
7. Skaner AM musi umożliwiać blokowanie skryptów, apletów Java oraz ActiveX
8. Skaner AM musi mieć możliwość stosowania konfiguracji, w której wirusy konkretnego typu (np. Mass Mailery) są zawsze usuwane przez Gateway pocztowy bez powiadamiania użytkownika, a w razie wykrycia kodu zagrożeń innego typu logowanie go standardowo.
9. Oprócz skanera anti-malware (AM) pochodzącego od tego samego producenta, co całe oferowane rozwiązanie powinien być dostępny inny silnik anti-malware innego producenta. Silnik ten powinien być dostarczany w ramach głównej licencji – bez dodatkowych kosztów.
10. System musi umożliwiać integrację z produktem typu Sandbox tego samego producenta. Wyklucza się jednak integrację z systemami typu Sandbox „w chmurze”.

**Wymagania dotyczące ochrony anty-spamowej**

1. Gateway pocztowy musi zapewniać także ochronę przed spamem – powinien być wyposażony w moduł anty-spam (AS) pochodzący od tego samego producenta, co całe oferowane rozwiązanie
2. Skaner AS musi działać w oparciu o system oceny prawdopodobieństwa wystąpienia spamu bazujący na regułach aktualizowanych przez producenta
3. Aktualizacja reguł musi odbywać się na bieżąco kilka razy na godziną, a co najmniej raz dziennie
4. Skaner AS musi współpracować z serwerami AD i LDAP pozwalając na stworzenie dokładnej polityki skanowania zależnie od adresu email, grupy użytkowników w AD/LDAP, domeny pocztowej, zakresu adresów IP
5. System AS musi obsługiwać białe i czarne listy (*blacklist* i *whitelist*) definiowane przez administratora oraz samodzielnie przez końcowych użytkowników (odbiorców poczty)
6. System AS musi obsługiwać serwery RBL prowadzone przez producenta rozwiązania. Musi być także możliwe definiowanie dodatkowych źródeł RBL przez administratora systemu
7. System AS musi wykrywać i blokować ataki typu *directory harvest*
8. System AS musi obsługiwać technologie *graylist*, SPF oraz Sender ID
9. System AS musi chronić przed spamem generowanym za pomocą mechanizmu potwierdzania problemów z doręczeniem przesyłki (NDR)
10. System powinien wykorzystywać funkcję FCrDNS realizującą sprawdzenie poprawności konfiguracji rozwiązywania nazw DNS systemu nadającego wiadomość.
11. System AS musi posiadać filtr reputacyjny badający domenę i adres IP, z których nadana została wiadomość oraz zawartość przesyłaną w email
12. Reputacja powinna być określona dynamicznie, na bieżąco przez zapytania do serwisu reputacyjnego prowadzonego przez producenta rozwiązania
13. Musi być możliwe takie skonfigurowanie polityki ochrony anty-spam, aby już sam wynik z serwisu reputacyjnego (niska reputacja nadawcy) powodował odrzucenie email lub skierowanie go do kwarantanny
    1. Musi być także możliwe uwzględnienie wyników z serwisu reputacyjnego w całościowej ocenie prawdopodobieństwa wykrycia spam i podejmowanie decyzji o losie email na podstawie końcowego wyniku analizy, po przejściu email przez inne filtry analizujące wiadomość
14. System powinien umożliwiać rozpoznawanie URL’i w treści wiadomości i filtrować wiadomość i URL’ami o złej reputacji. Kontrola reputacji URL powinna być badana w momencie dostarczania wiadomości oraz w momencie kliknięcia URL’a przez użytkownika w kliencie pocztowym w czasie rzeczywistym.
15. Musi być możliwe zdefiniowanie różnych akcji podejmowanych po wykryciu spamu zależnie od określonego przez system prawdopodobieństwa wykrycia spam (*spam score*)
    1. Zablokowanie i skasowanie wiadomości z powiadomieniem do końcowego użytkownika, a także bez takiego powiadomienia (zależnie od przyjętej polityki)
    2. Przekazanie wiadomości do kwarantanny
    3. Przesłanie wiadomości do odbiorcy z oznakowaniem jej jako spam w tytule wiadomości
    4. Dodanie do nagłówka wiadomości informacji o *spam score*
    5. Dodanie do nagłówka wiadomości informacji, które reguły ant-spamowe spowodowały wykrycie spam

**Obsługa kwarantanny**

1. Gateway musi umożliwiać zapisanie wiadomości do kwarantanny przechowywanej lokalnie, a także na zewnętrznym serwerze.
2. Decyzja o zapisaniu wiadomości do kwarantanny musi wynikać z definicji działania poszczególnych filtrów: anti-malware, anti-spam, DLP i weryfikacji treści.
3. Administrator Gateway’a ma mieć możliwość dostępu do lokalnej kwarantanny na Gateway’u bezpośrednio z interfejsu GUI
   1. Administrator ma mieć możliwość usunięcia wybranych wiadomości z kwarantanny, „zwolnienia” z kwarantanny (przesłania wiadomości do odbiorcy), przekazania pod inny adres email
   2. Administrator musi mieć możliwość analizy treści wiadomości zatrzymanej w kwarantannie i jej nagłówków dla sprawdzenia powodu zatrzymania email
   3. Musi być możliwe zdefiniowanie maksymalnego czasu przechowywania wiadomości w kwarantannie
4. Gateway musi umożliwiać automatyczne wysyłanie mailem powiadomień o wiadomościach zatrzymanych w kwarantannie do ich oryginalnych odbiorców
   1. Wraz z informacją o zatrzymaniu emaila, konstrukcja wiadomości informacyjnej powinna umożliwiać bezpośrednie podjęcie akcji przez użytkownika na kwarantannie bez konieczności logowania się do GUI Gateway’a: zwolnienie wiadomości z kwarantanny, skasowanie wiadomości, dodanie nadawcy do białej listy (whitelist), dodanie nadawcy do czarnej listy (blacklist), nie podjęcie żadnej akcji
   2. Musi istnieć możliwość pełnego dostosowania treści wiadomości z powiadomieniem, w tym spolonizowanie jej
   3. Musi być możliwe określenie częstotliwości wysyłania powiadomień
5. W ramach oferowanego rozwiązania należy zapewnić także rozwiązanie do centralnej, wspólnej obsługi kwarantanny ze wszystkich działających w sieci Gateway’ów
   1. Centralna kwarantanna powinna działać na dedykowanym serwerze (maszynie wirtualnej) z systemem operacyjnym MS Windows Server i korzystać z bazy danych MS SQL
   2. Platformę (maszyny wirtualne) dla instalacji centralnej kwarantanny i bazę SQL Express zapewni Zamawiający,
   3. Jeśli Wykonawca stwierdzi, że baza SQL Express jest niewystarczająca, powinien zapewnić bazę, która zagwarantuje opisane poniżej funkcjonalności centralnej kwarantanny.
6. Centralna kwarantanna musi umożliwiać co najmniej:
   1. Zarządzanie z różnych kont administratorów, do których zostaną przydzielone role określające zakres administracji
   2. Integrację z Active Directory i dzięki temu umożliwianie autentykacji przy nawiązywaniu połączenia
   3. Obsługę poprzez interfejs Web dostępny przez HTTPS
   4. Bezpośredni dostęp do swoich, wydzielonych kont z informacjami o zawartości kwarantanny dla poszczególnych użytkowników. Dostęp do kwarantanny ma być uwierzytelniany w sposób transparentny, z wykorzystaniem integracji z AD
   5. Użytkownik na swoim koncie w kwarantannie może zwolnić wiadomość z kwarantanny, skasować ją, pozostawić do automatycznego usunięcia po zdefiniowanym przez administratora czasie, dodawać odbiorców do białych i czarnych list (whitelist, blacklist), które następnie synchronizowane z gateway’ami i wpływają na politykę wykrywania/blokowania spam
   6. Użytkownik nie może mieć uprawnień do zwolnienia z kwarantanny wiadomości zawierających kod złośliwy
   7. Wysyłanie powiadomień z informacją o wiadomościach zatrzymanych w kwarantannie do ich oryginalnych odbiorców. Konstrukcja powiadomienia powinna umożliwiać bezpośrednie podjęcie akcji przez użytkownika na kwarantannie bez konieczności logowania się do GUI Gateway’a: zwolnienie wiadomości z kwarantanny, skasowanie wiadomości, dodanie nadawcy do białej listy (whitelist), dodanie nadawcy do czarnej listy (blacklist), nie podjęcie żadnej akcji
   8. Zdefiniowanie czasu przechowywania wiadomości w kwarantannie, nie mniej niż pół roku
   9. Sięgnięcie minimum pół roku wstecz do maili będących w kwarantannie
7. **Wymagania dla wsparcia technicznego producenta**

W ramach oferty należy zapewnić dla Zamawiającego dostęp do usług wsparcia technicznego dla oferowanego rozwiązania (oprogramowanie i platformy sprzętowe) w okresie 3 lat od zakupu. W ramach usług wsparcia producenta należy zapewnić co najmniej:

1. Dostęp do najnowszych wersji oprogramowania, bez konieczności wnoszenia dodatkowych opłat
2. Dostęp do poprawek i łatek do oprogramowania po ich opublikowaniu przez producenta
3. Dostęp do aktualizacji plików sygnatur, baz danych opisujących ataki, baz kategorii URL, itp.
4. Możliwość bezpośredniego zgłaszania do producenta problemów serwisowych przez Zamawiającego w trybie 24/7 poprzez email, telefon, stronę web
5. Dostęp do części zamiennych lub całych urządzeń na wymianę w razie awarii, realizowany w miejscu instalacji sprzętu w siedzibie Zamawiającego w Warszawie
6. Dostęp do bazy wiedzy prowadzonej przez producenta z artykułami dotyczącymi oferowanych produktów
7. **Wymagania do usług wdrożeniowych**

W ramach wdrożenia systemu OE należy opracować i wykonać co najmniej:

1. Uzgodnienia techniczne i projekt wdrożenia
2. Instalację urządzeń i oprogramowania we wskazanych przez Zamawiającego miejscach w Warszawie
3. Konfigurację polityk komponentów OE wg ustaleń i integrację systemu z innymi systemami sieciowymi Zamawiającego
4. Testy działania systemu OE dla każdej funkcjonalności
5. W ramach testów koniecznym jest stworzenie testowej strony phishingowej dla całego Instytutu
6. 1-dniowe warsztaty dla co najmniej 3 osób przedstawiające szczegóły implementacji rozwiązania, realizowane w miejscu wdrożenia
7. Dokumentację powykonawczą systemu

**ELEMENT 2**

**System kontroli dostępu do zasobów sieciowych (NAC)**

Wymagane jest zbudowanie systemu kontroli dostępu do sieci (NAC) dla 500 użytkowników na bazie dwóch dedykowanych urządzeń pracujących w układzie klastra wysokiej dostępności HA, umieszczonych w dwóch serwerowniach Zamawiającego, włączonych do odpowiednich elementów rdzeniowych sieci łączami o przepustowości 2x1 Gbps każde i współpracujących z posiadanymi przez Zamawiającego systemami:

1. Przełączniki dostępowe Juniper EX4200, EX2200 i EX4500
2. Centralne zapory sieciowe Juniper SRX3400
3. System zdalnego dostępu Juniper SSL VPN/Junos Pulse client

Celem jest stworzenie zintegrowanego systemu kontroli dostępu opartego na standardzie 802.1x i portalu przechwytującym (captive portal) zarówno dla sieci przewodowej jak i bezprzewodowej zapewniającego:

1. Uwierzytelnianie użytkowników sieci
2. Dynamiczne przydzielanie sieci wirtualnych VLAN na podstawie tożsamości użytkownika
3. Kontrolę konfiguracji wybranych stacji roboczych pod kątem zgodności z polityką bezpieczeństwa (np. obecność oprogramowania antywirusowego, aktualność poprawek systemu operacyjnego)
4. Automatyczną kwarantannę zainfekowanych lub złośliwych stacji roboczych
5. Wsparcie dla budowy polityk bezpieczeństwa na centralnych zaporach sieciowych na podstawie tożsamości użytkownika
6. Możliwość imiennego rozliczania użytkowników.
7. Wysyłanie logów systemowych i aktywności użytkowników poprzez protokół Syslog, w formacie Welf oraz W3C

Stacje użytkowników nie posiadających możliwości uwierzytelnienia 802.1x, powinny być przenoszone do gościnnej sieci wirtualnej VLAN, z której zapewniony będzie dostęp wyłącznie do zasobów określonych polityką bezpieczeństwa Zamawiającego. Dostęp do wewnętrznych zasobów Zamawiającego będzie wówczas możliwy wyłącznie po uwierzytelnieniu stacji przez dodatkowy portal (automatyczne przekierowanie przy próbie dostępu).

System kontroli dostępu do sieci musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny.

System musi zapewniać co najmniej:

* Kontrole konfiguracji stacji i weryfikacje zgodności z założoną polityką bezpieczeństwa
* Sterowanie posiadanymi przez Zamawiającego urządzeniami firewall SRX serii 3000 w zakresie dynamicznej modyfikacji polityki bezpieczeństwa (min. listy kontroli dostępu) w oparciu o dane z systemu kontroli bezpieczeństwa NAC
* Sterowanie przełącznikami będącymi w użyciu przez zamawiającego, przy wykorzystaniu mechanizmów protokołu RADIUS oraz 802.1x, w szczególności dynamiczne przypisywanie VLAN-u do portu, w zależności od polityki bezpieczeństwa.

Polityka bezpieczeństwa musi umożliwiać kontrolę dostępu na podstawie nie mniej niż następujących kryteriów lub ich dowolnej kombinacji:

* Tożsamość użytkownika
* Adres IP komputera
* Stan bezpieczeństwa stacji użytkownika
* Parametry czasowe.

Weryfikacja tożsamości użytkownika musi się odbywać za pomocą nie mniej niż następujących mechanizmów:

* Lokalna baza danych na urządzeniu z autentykacją imienną kont oraz lokalną autentykacją adresów MAC ze wsparciem dla WildCard
* Zewnętrzny serwer RADIUS
* Zewnętrzny serwer LDAP
* Domena Active Directory z wykorzystaniem protokołu Kerberos
* Certyfikat cyfrowy
* Serwer NIS.

Musi być dostępny mechanizm uwierzytelnienia dwuskładnikowego, nie mniej niż hasło statyczne wraz z certyfikatem cyfrowym.

System musi przeprowadzać weryfikację stanu bezpieczeństwa stacji użytkownika z systemami operacyjnymi nie mniej niż Windows XP SP3, Windows 7, Windows 8.1. Weryfikacja musi obejmować nie mniej niż:

* sprawdzenia obecności konkretnego procesu, pliku, wpisu w rejestrze Windows, otwartych portów
* sprawdzenia czy włączono odpowiednie usługi zabezpieczeń takie jak oprogramowanie antywirusowe, zapora, system antyszpiegowski, zarówno w momencie logowania jak w trakcie trwania sesji
* sprawdzenia, czy odpowiednie usługi zabezpieczeń są aktualne, w szczególności czy system antywirusowy ma aktualną bazę sygnatur
* sprawdzenia, czy zostały zainstalowane odpowiednie poprawki do oprogramowania
* sprawdzenia czy włączony jest system automatycznych uaktualnień systemu Windows oraz zapora systemu Windows przy wykorzystaniu mechanizmu SOH.

Dodatkowo musi być możliwa weryfikacja systemów Linux oraz Mac OSX – nie mniej niż sprawdzenia obecności konkretnego procesu, pliku, otwartych portów.

Weryfikacja stanu bezpieczeństwa stacji musi być przeprowadzana na bieżąco w trakcie trwania sesji. Zmiana stanu bezpieczeństwa musi być przekazywana automatycznie do systemu.

Musi istnieć możliwość weryfikacji polityki bezpieczeństwa za pomocą następujących mechanizmów:

* Agent zainstalowany na komputerze klienta jako aplikacja Windows, z wbudowanym suplikantem 802.1x, dostarczany przy pomocy mechanizmów wbudowanych w system Windows, dostępny w postaci pliku msi.
* Agent dostarczany przez przeglądarkę WWW w postaci apletu Java lub kontrolki ActiveX
* Agent wbudowany w system Windows XP SP3, Windows 7 oraz Windows 8.1 wykorzystujący mechanizm SOH

Dodatkowo system musi dostarczać mechanizm automatycznego konfigurowania i aktualizowania oprogramowania agenta, dla użytkowników nie posiadających uprawnień administratora.

System musi dostarczać mechanizmów, które w zależności od polityki bezpieczeństwa będzie przydzielał dostęp do zasobów na urządzeniach obsługujących protokół 802.1x, bez konieczności posiadania zewnętrznego serwera RADIUS. System musi mieć możliwość wprowadzenia dowolnego słownika RADIUS zawierającego dowolne VSA (vendor-specific attributes).

Agent dostarczany w postaci aplikacji musi zawierać centralnie sterowaną zaporę sieciową. Agent musi zawierać funkcjonalność zestawiania tunelu IPsec pomiędzy komputerem, na którym jest zainstalowany i centralnym firewall. Agent musi posiadać funkcjonalność umożliwiającą modyfikację konfigurację stacji zdalnej, nie mniej niż:

* włączenie aktualizacji automatycznych oraz zapory systemu Windows
* włączenie oprogramowania antywirusowego, jego aktualizacja oraz skanowanie.

Centralne urządzenia sytemu NAC muszą mieć możliwość instalacji redundantnych zasilaczy.

Dostarczone oprogramowanie nie może powodować konfliktu lub ograniczenia funkcjonalności obecnie działającego u Zamawiającego środowiska informatycznego.

Wraz z dostawą systemu kontroli dostępu wymagane jest wykonanie pełnego wdrożenia systemu NAC dla wszystkich użytkowników oraz wykonanie integracji w ramach 802.1x z posiadaną przez Zamawiającego infrastrukturą sieciową (do 500 użytkowników oraz ok. 40 szt. przełączników EX4200, 4500 i firewall SRX serii 3000).

**ELEMENT 3**

**Przełącznik 10 Gigabit Ethernet**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2. Przełącznik musi posiadać wbudowane nie mniej niż 32 porty dostępowe przeznaczone na moduły SFP+ oraz SFP.
3. Przełącznik musi posiadać możliwość rozbudowy do nie mniej niż 48 portów SFP+ oraz SFP. Wszystkie wbudowane porty urządzenia muszą być aktywne po wyposażeniu przełącznika w dodatkowej karty z portami Ethernet.
4. Przełącznik musi posiadać możliwość rozbudowy o min. 2 porty 40 Gigabit Ethernet QSFP+
5. Urządzenie musi obsługiwać moduły SFP Gigabit Ethernet nie mniej 1000Base-T, SX, LX. Urządzenie musi obsługiwać moduły SFP+ 10 Gigabit Ethernet nie mniej niż SR, LRM, LR, ER. Ponadto urządzenie musi obsługiwać moduły miedziane (Direct Attach Copper) do zestawienia połączeń 10 Gigabit Ethernet. Urządzenie musi być dostarczone z następującymi modułami: 32szt. SFP+ SR
6. Przełącznik musi posiadać wymienne zasilacze AC. Urządzenie musi być wyposażone w redundantne zasilacze. Urządzenie musi posiadać wymienny moduł wentylacji. Przepływ powietrza przez przełącznik musi być od przodu (strona z portami dostępowymi) do tyłu. Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset, odczyt statusu niektórych komponentów przełącznika).
7. Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 9 urządzeń. Do łączenia w stos muszą być zastosowane dedykowane porty przełącznika o przepustowości nie mniej niż 32 Gb/s lub porty SFP+ 10GE. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup’u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Przełącznik musi umożliwiać pracę w tym trybie w stosie złożonym z czterech przełączników EX4500 i dwóch EX4200-48T posiadanych już przez Zamawiającego. Dopuszcza się uzyskanie wymaganej funkcjonalności i kompatybilności przełączników w stosie poprzez wymianę istniejących urządzeń.
8. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
9. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
10. Przełącznik musi posiadać architekturę non-blocking. Zagregowana wydajność przełączania w warstwie 2 nie może być niższa niż 960 Gb/s (pełne 10 Gb/s full-duplex na wszystkich portach). Urządzenie musi obsługiwać nie mniej niż 700 milionów ramek/sekundę. Przełącznik musi obsługiwać conajmniej 32 000 adresów MAC.
11. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
12. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4096. W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół MVRP lub równoważny.
13. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 64 grupy LAG, po nie mniej niż 8 portów.
14. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
15. Przełącznik musi obsługiwać protokół LLDP.
16. Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokoły routingu dynamicznego: RIP, OSPF. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 10 000. Urządzenie musi obsługiwać protokoły routingu multicast, nie mniej niż IGMP i PIM-SM.
17. Urządzenie musi posiadać możliwość obsługi rutingu IPv6.
18. Urządzenie musi posiadać możliwość rozszerzenia funkcjonalności routingu do obsługi IS-IS, BGP, MPLS.
19. Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie konfiguracji HA z wykorzystaniem protokołu VRRP.
20. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
21. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
22. Przełącznik musi obsługiwać limitowanie adresów MAC.
23. Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu.
24. W celu integracji z sieciami storage urządzenie musi obsługiwać funkcje: FIP Snooping, Data Center Bridging Capability Exchange (DCBX) oraz Priority-based Flow Control (PFC).
25. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
26. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.

Pomoc techniczna oraz autoryzowane przez producenta szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.

**Należy zapewnić wszystkie niezbędne elementy nie wymienione w specyfikacji a niezbędne do realizacji przedmiotu zamówienia.**

**ELEMENT 4**

**System SIEM**

**INSTALACJA i SPRZĘT:**

1. Rozwiązanie powinno być dostarczone i wdrożone w jednej z poniższych postaci:

1A. Dedykowane urządzenie z własnym systemem operacyjnym i preinstalowanym oprogramowaniem

1B. Oprogramowanie instalowane w systemie operacyjnym Red Hat Enterprise Linux

2. Rozwiązanie SIEM wymienione w punkcie 1. musi zostać wdrożone w jednej z dwóch opcji:

2.A Jako pojedyncze urządzenie wykonujące wszystkie bez wyjątku funkcjonalności, o których mowa w dalszych punktach o parametrach 5000 EPS oraz 50 tysięcy flows (przepływów) na minutę (z możliwością skalowania licencyjnie do rozmiarów minimum 15000 EPS oraz 300 tysięcy flows (przepływów) na minutę). Minimalne parametry tego urządzenia to:

1. Obudowa typu RACK o wysokości nie więcej niż 2U.
2. Serwer musi posiadać dwa ośmiordzeniowe procesory taktowane zegarem co najmniej 2,4 GHz. Serwer musi posiadać co najmniej 128GB pamięci RAM min. 2133 MHz oraz możliwość instalacji do co najmniej 768 GB pamięci.
3. Oferowane procesory muszą osiągać wynik 673 w teście SPECint\_rate\_base2006 w konfiguracji dwuprocesorowej. Wynik musi być opublikowany na stronie [www.spec.org](http://www.spec.org/) na moment złożenia oferty
4. Serwer musi posiadać co najmniej 26 dysków o pojemności co najmniej 1,2TB i prędkości obrotowej 10000 rpm
5. Serwer musi posiadać dwa kontrolery dyskowe umożliwiające utworzenie RAID 0, 1, 5, 10, przynajmniej jeden z pamięcią 1GB cache podtrzymywanego bateryjnie lub flash-backed
6. Serwer musi posiadać co najmniej 3 sloty PCI-E 2.0 x16 (elektrycznie), oraz 3 sloty PCI-E 2.0 x8 (elektrycznie)
7. Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód,tył), oraz 2 wewnętrzne porty SD lub USB
8. Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000, 2 porty 10Gb Ethernet na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.
9. Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym
10. Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0
11. Serwer musi posiadać minimum dwa porty FC 8Gb/s.
12. Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 750W
13. Serwer musi posiadać kartę VGA
14. Serwer musi posiadać wysokość maksymalnie 2U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi
15. Wsparcie dla oferowanego oprogramowania systemowego.
16. Gwarancja producenta 5 lat z gwarantowanym czasem naprawy 24h

2.B Jako zintegrowany system wykonujący wszystkie bez wyjątku funkcjonalności, o których mowa niżej, wdrożony z zastosowaniem architektury rozproszonej (poszczególne elementy tego systemu wyspecyfikowano w punktach 3, 4. oraz 5, o parametrach 5000 EPS oraz 50 tysięcy flows (przepływów) na minutę skalujące się licencyjnie do rozmiarów minimum 15000 EPS oraz 300 tysięcy flows (przepływów) na minutę.

3. Przy zastosowaniu architektury rozproszonej zarządzanej z jednej konsoli, wszystkie urządzenia składowe tej architektury dają się zastosować jako dowolny z wariantów wspomnianych wyżej t.j. 1.A; 1.B

4. Korelacja zdarzeń i informacji o przepływach, wnioskowanie oraz obsługa incydentów, a także prezentacja zdarzeń w architekturze rozproszonej odbywa się na podstawie wszystkich zdarzeń i przepływów składowych niezależnie od miejsca ich kolekcji, a wyniki prezentowane są w jednej wspólnej dedykowanej konsoli.

5. W architekturze rozproszonej, rozróżnia się następujące elementy składowe:

5.A Kolektor i procesor zdarzeń (mogący przyjąć nawet 20 tysięcy EPS = Events Per Second, czyli ciągłego strumienia zdarzeń (logów) w ciągu jednej sekundy bez ograniczeń okresu trwania tej wielkości strumienia logów czyli zdarzeń). Minimalne parametry tego urządzenia to 2 x CPU (4 rdzenie każdy zdolnych obsłużyć 8 wątków per CPU) 2,4 GHz, 48GB RAM, 9 TB przestrzeni dyskowej w tym 6,5 TB dedykowane dla oprogramowania SIEM,

5.B Kolektor i procesor przepływów (mogący przyjąć nawet 1200 000 = jeden milion dwieście tysięcy przepływów w ciągu minuty bez ograniczeń okresu trwania tej wielkości strumienia przepływów). Minimalne parametry tego urządzenia to 2 x CPU (6 rdzeni zdolnych obsłużyć 12 wątków per CPU) 2,93 GHz; 64 GB RAM, 24 TB przestrzeni dyskowej w tym 16TB dedykowanej dla oprogramowania SIEM,

5.C Kolektor i procesor zarówno zdarzeń jak i przepływów mogący przyjąć jednostajny strumień minimum 1000 EPS = Events Per Second czyli zdarzeń (logów) w ciągu jednej sekundy oraz przynajmniej jednoczesny strumień 50 tysięcy przepływów czyli flows w ciągu jednej minuty. Minimalne parametry tego urządzenia to 2 x CPU (4 rdzenie każdy zdolnych obsłużyć 8 wątków per CPU) 2,4 GHz, 48GB RAM, 9 TB przestrzeni dyskowej w tym 6,5 TB dedykowane dla oprogramowania SIEM,

5.D Konsoli administratora, z której zarządza się konfiguracją i działaniem elementów wymienionych w punktach 5.A, 5.B, 5.C lub też ich odpowiedników w postaci maszyn wirtualnych. Minimalne parametry tego urządzenia to: 2 x CPU (6 rdzeni zdolnych obsłużyć 12 wątków per CPU) 2,93 GHz; 64 GB RAM 48 GB RAM, 24TB miejsca na dyskach w tym minimum 16TB dla samego oprogramowania SIEM,

5.E Konsola administratora może występować także jako maszyna wirtualna, ale istnieje możliwość jej migracji do urządzenia wymienionego w punkcie 5.D,

5.F Kolektor przepływów generowanych na podstawie podsłuchu ruchu na dedykowanym porcie przełącznika sieciowego przez samo rozwiązanie SIEM, tutaj oprócz informacji istotnych dla określenia ruchu sieciowego (nagłówki warstw od 2 do 4 modelu ISO/OSI) rozróżniane są także dane zawarte w ładunku pakietu (tzw. ang. payload) co dodatkowo pozwala zidentyfikować aplikacje działające na nietypowych portach TCP lub UDP. Taki kolektor dla urządzeń wymienionych w punktach 2.B i 2A. może występować jako wbudowany moduł działający w oparciu o jedną z dedykowanych kart sieciowych na pokładzie tych maszyn.

**ZARZĄDZANIE OPROGRAMOWANIEM:**

6. Zarządzanie oprogramowaniem ma odbywać się przy użyciu przeglądarki internetowej, nie wymagane jest instalowanie żadnego dedykowanego oprogramowania klienta.

7. Wymagane przeglądarki internetowe to:

7.A Mozilla Firefox

7.B Internet Explorer 7.0, 8.0 i 9.0 z włączoną funkcjonalnością „Compatibility View”

8. Inne minimalne wymagania oprócz jednej z przeglądarek wymienionych w punkcie 7. to:

8.A Java TM Runtime Environment (JRE)

8.B Adobe Flash 10.x

**CECHY UŻYTKOWE – TABLICE NADZORU DZIAŁANIA:**

9. Oprogramowanie musi udostępniać możliwość prezentacji statystyk i wyników działania systemu SIEM w postaci tzw. „Dashboard” czyli tablic, których wygląd w tym rozkład poszczególnych ekranów składowych daje się przystosować do potrzeb administratora czy też zalogowanego użytkownika

10. W oprogramowaniu, widoczność stworzonych i domyślnych dostępnie tablic musi się przełączać przy pomocy łatwo osiągalnej listy rozwijanych pozycji.

11. Poszczególne ekrany składowe, o których mowa w punkcie 9. muszą być m wynikiem stworzonych przez producenta wyników wyszukiwania danych, a także podobnych elementów (wyników wyszukiwania danych) stworzonych przez użytkownika lub udostępnionych mu przez innych użytkowników (administratorów)

12. Wyniki wyszukiwania danych, o których mowa w punkcie 11. Muszą mieć postać graficzną zarówno jako wielkości zagregowanych jak i zanotowanych i prezentowanych w czasie rozkładów wielkości (trendów) – w tym przypadku oś pozioma stanowi określony interwał czasowy, a oś pionowa zagregowane wielkości różnych parametrów w danym momencie prezentowanych innym kolorem.

13. Dane podlegające wyszukiwaniu i tworzone z nich wyniki muszą dotyczyć wartości pozyskanych z logów (czyli zdarzeń) jak i przepływów czyli tzw. flows.

**CECHY UŻYTKOWE – KOLEKCJONOWANIE ZDARZEŃ i PRZEPŁYWÓW**

14. SIEM musi obsługiwać przepływy, o których mowa w punkcie 13. Ze wszystkich wymienionych poniżej standardów tego typu danych:

14.A NetFlow (wersje 1 ; 5; 7 oraz 9)

14.B sFlow (wersje 2, 4, oraz 5)

14.C J-Flow

14.D Packeteer

14.E Flowlog File (plik wygenerowany przez samo rozwiązanie)

14.F Napatech Interface (pochodzący z zainstalowanego w samym rozwiązaniu Adaptera sieciowego Napatech)

14.G Danych o ruchu i jego zawartości (ang. payload pakietu) zbieranych przez urządzenia wymienione w punkcie 5.F

15. Kolekcjonowanie zdarzeń czyli logów musi odbywać się przynajmniej z zastosowaniem protokołów mechanizmów wymienionych poniżej:

15.A Syslog

15.B JDBC (Java DataBase Connectivity)

15.C JDBC – SiteProtector (Java DataBase Connectivity w połączeniu do oprogramowania zarządzania środowiskiem sond IDS/IPS IBM Site Protector)

15.D Sophos Enterprise Console – JDBC (Java DataBase Connectivity wprost do konsoli Sophos Enterprise Console)

15.E Juniper Networks NSM (połączenie wprost do konsoli Juniper Network and Security Manager)

15.F OPSEC/LEA (połączenie przy pomocy standard Check Point OPSEC [Open Platform for Security] i jego mechanizmu LEA [Log Export API] do systemu Check Point SmartCenter)

15.G SDEE (Security Device Event Exchange)

15.H SNMPv1 (Simple Network Management Protocol wersja 1) – kolekcjonowanie tzw. SNMP traps wysyłanych przy pomocy protokołu SNMP w wersji 1 przez urządzenia i systemy na adres IP kolektora zdarzeń systemu SIEM

15.I SNMPv2 (Simple Network Management Protocol wersja 2) – kolekcjonowanie tzw. SNMP traps wysyłanych przy pomocy protokołu SNMP w wersji 2 przez urządzenia i systemy na adres IP kolektora zdarzeń systemu SIEM

15.J SNMPv3 (Simple Network Management Protocol wersja 3) – kolekcjonowanie tzw. SNMP traps wysyłanych przy pomocy protokołu SNMP w wersji 3 przez urządzenia i systemy na adres IP kolektora zdarzeń systemu SIEM

15.K Sourcefire Defense Center Estreamer – zdarzenia wysyłane bezpośrednio z konsoli zarządzania środowiskiem urządzeń Sourcefire

15.L Log File – cykliczne pobieranie plików i importowanie zdarzeń w nim zapisanych do bazy systemu SIEM przy pomocy protokołów SFTP, FTP oraz SCP o zadanej porze, wzorze nazwy i wprowadzeniu zdefiniowanej nazwy użytkownika i hasła lub odpowiednich kluczy.

16. Dane pochodzące z logów zapisywane muszą być w domyślnie dostępnych polach bazy danych przynajmniej takich jak: Nazwa zdarzenia, Kategoria zdarzenia, Adres IP źródłowy, Źródłowy Port TCP/IP, Adres IP źródłowy przed translacją, Adres IP źródłowy po translacji, Adres MAC źródłowy, Źródłowy Port TCP/IP przed translacją, Źródłowy Port TCP/IP po translacji, Adres IP Przeznaczenia, Port TCP/IP Przeznaczenia, Port TCP/IP Przeznaczenia przed translacją, Port TCP/IP Przeznaczenia po translacji, Adres IP Przeznaczenia przed translacją, Adres IP Przeznaczenia po translacji, Adres MAC Przeznaczenia, Czas urządzenia gdy wysłany był log, Nazwa protokołu, Nazwa użytkownika, Nazwa hosta, Nazwa grupy, Nazwa NetBIOS.

17. Oprócz pól podstawowych musi instnieć możliwość dodania własnych pól w bazie, które można szybko przywoływać jako kryteria wyszukiwania, określane przy pomocy nowych wzorców specyfikowanych przy pomocy wyrażeń regularnych i źródeł logów

**CECHY UŻYTKOWE – ANALIZA ZDARZEŃ (LOGÓW)**

18. System SIEM musi umożliwiać na tworzenie wyszukiwanie logów w oparciu o kryteria wymienione w punkcie 16 i 17. wraz z możliwością dotarcia do szczegółów zdarzenia (tzw. payload czyli zawartość całego logu) oraz interwału czasowego.

19. System SIEM musi pozwalać tworzyć graficznie i tekstowo prezentowaną agregację danych z wyszukiwania utworzonego wg opisu w punkcie 18.

20. Musi istnieć możliwość modyfikacji agregacji danych opisanej w punkcie 19. w sposób interaktywny wybierając zarówno inny interwał czasowy, za który dane są agregowane jak i wymiar agregacji

21. Wymiar agregacji danych opisanych w punkcie 20. powinien być zarówno wielkością domyślnie dostępną opisaną w punkcie 16. jak i własną użytkownika lub administratora opisaną w punkcie 17.

22. Interwały czasowe wspomniane w punkcie 18. muszą być wybierane z dostępnych fabrycznie wielkości: ostatnie 5 minut, ostatnie 15 minut, ostatnie 30 minut, ostatnie 45 minut, ostatnie 3 godziny, ostatnie 6 godzin, ostatnie 12 godzin, ostatnie 24 godziny, ostatnie 3 dni, ostatnie 7 dni oraz własny interwał czasowy wskazany przez początek w danym dniu (data) i godzinie oraz koniec w danym dniu (data) i godzinie

23. Prezentacja wyników wyszukiwania musi być możliwa dla danych liczbowych w postaci sumy tych wartości, wartości minimalnej, maksymalnej lub też wartości średniej (można określić sposób prezentacji tych danych na etapie budowania szablonu prezentacji wyników tego wyszukiwania).

24. Wzorce wyszukiwania (związane z nimi szablony prezentacji) i związane z tym wyniki muszą być zapisane w postaci nazwy w celu późniejszego łatwego przywołania lub też udostępnienia takiego szablonu wyszukiwania innym użytkownikom.

25. Wzorce wyszukiwania (związane z nimi szablony prezentacji) muszą być oprócz nadania nazwy umieszczone w odpowiedniej grupie oraz w tablicy szybkich przywołań oraz na tablicach czyli tzw. „Dashboards”, o których mowa w punkcie 9.

26. Wzorce wyszukiwania i dopasowanie kryteriów z punktów 16. i 17., muszą być budowane w oparciu o częściowe dopasowania do wzorców (podanie części danych, które musza występować) oraz różnych konstrukcji warunków jako: „jeden z podanej listy” i/lub „wszystkie z listy”

27. Wzorce wyszukiwania muszą być też zastosowane do danych aktualnie kolekcjonowanych przez system SIEM i wyświetlanych w postaci przewijających się automatycznie ekranów

28. System SIEM musi pozwalać określić jaka jest aktualnie występująca i zanotowana dla pewnego interwału czasowego liczba kolekcjonowanych zdarzeń w ciągu sekundy i przepływów (flows).

29. Każde pojedynczne zdarzenie zapisane w bazie systemu SIEM musi być opatrzone flagą kraju jeśli adresacja IP nie pochodzi z puli RFC 1918 oraz dynamicznie obliczonym parametrem priorytetu, na który składają się odpowiednie wartości cząstkowe (z uwzględnieniem wag) odzwierciedlające miedzy innymi: powszechnie uznany stopień zagrożenia związany z danym zdarzeniem, relacja tego zdarzenia do faktycznie zarejestrowanego stanu usług sieciowych zasobu, którego dotyczy to zdarzenie, a także stopień zaufania do danego źródła logów.

30. Każde zdarzenie musi mieć możliwość otwarcia w dodatkowym oknie prezentującym wszystkie przyporządkowane i dające się przyporządkować pola w bazie danych systemu SIEM dla tego zasobu oraz payload tego zdarzenia.

**CECHY UŻYTKOWE – ANALIZA PRZEPŁYWÓW (FLOWS)**

31. System musi pozwalać osiągnąć identyczne funkcjonalności jak opisane w punktach 18. do 28., ale dla zebranych przepływów (flows) z uwzględnieniem modyfikacji opisanych w punktach 32. i 33.

32. Podstawowe pola bazy danych dla przepływów to przynajmniej: Adres IP źródłowy, Źródłowy Port TCP/IP, Adres IP Przeznaczenia, Port TCP/IP Przeznaczenia, liczba wysłanych danych, liczba danych odebranych

33. Dla danych zebranych przy pomocy mechanizmu opisanego w punkcie 5.F można tworzyć dodatkowe pola w bazie danych w celu ich późniejszego szybkiego przywołania w prezentacji wyników i szablonów wyszukiwania.

**CECHY UŻYTKOWE – ZDARZENIA i PRZEPŁYWY, SPOSÓB PRZECHWOWYANIA I RETENCJI**

34. System SIEM musi umożliwiać zapis zdarzeń skompresowany w bazie (agregacja najważniejszych pól z bazy danych systemu SIEM w interwałach 60 sekundowych) i dodanie do tego skompresowanego zapisu wymieniającego liczbę ilości zdarzeń skompresowanych i payload szczegółowy ostatniego zdarzenia.

35. System musi umożliwiać wyłączenie kompresji zdarzeń opisanej w punkcie 34. i włączenie zapisu w bazie całego payloadu, zgodnie z ograniczeniami producenta systemu SIEM

36. System SIEM musi pozwalać włączyć opatrywanie każdego zdarzenia sumą kontrolną obliczaną według jednego z wybranych algorytmów: MD2; MD5; SHA-1; SHA-256; SHA-384; SHA-512

37. System SIEM musi pozwalać określić sposób retencji dla przechowywanych zdarzeń oraz przepływów i miejsca ich przechowywania w systemie plików rozwiązania SIEM

38. Musi istnieć możliwość włączenia indeksowania zarówno dla zawartości ang. Payload każdego zdarzenia jak i przepływu (zarejestrowanego mechanizmem w punkcie 5.F). Indeksowanie to pozwala zoptymalizować operacje wyszukiwania podczas analizy logów i przepływów.

39. Ponadto system SIEM musi umożliwiać włączenie mechanizmu automatycznego archiwizowania danych i konfiguracji systemu SIEM do katalogu w lokalnym systemie plików i określenie retencji dla przechowywanych w ten sposób danych. Jednocześnie musi istnieć możliwość określenia priorytetu dla operacji backupu, aby wskazać jaki ona może mieć wpływ na ogólne działanie systemu.

**CECHY UŻYTKOWE – ADMINISTRACJA SYSTEMEM**

40. Rozwiązanie musi pozwalać utworzyć strukturę adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów

41. Rozwiązanie musi być skonfigurowane w celu pobierania aktualizacji w sposób automatyczny, w zdefiniowanym przez użytkownika planie, wraz ze wskazaniem poszczególnych części składowych aktualizacji i konfiguracją czy powinna następować automatyczna ich instalacja. Aktualizacje mogą być pobierane bezpośrednio lub przy użyciu serwera proxy, który może działać w oparciu o uwierzytelnienie.

42. Rozwiązanie musi pozwalać zdefiniować ustawienia dla uwierzytelnienia i samego działania sesji konsoli takie jak: czas wygaśnięcia sesji, maksymalna liczba nieudanych prób zalogowania i okres trwania interwału gdy one wystąpiły, czas zablokowania konta po przekroczeniu nieudanej liczby logowań.

43. Rozwiązanie musi pozwalać na pobieranie danych z serwera WINS (rozwiązywanie nazw dla obiektów przechowywanych w bazie.

44. Rozwiązanie musi pozwalać na definicję powiadomień przesyłanych na zdefiniowany adres email administratora, które wysyłane są w momencie przekroczenia zdefiniowanego progu:

44.1 obciążenia systemu przez 1 minutę

44.2 obciążenia systemu przez 5 minut

44.3 obciążenia systemu przez 15 minut

44.4 ilości pamięci fizycznej przechowywanej na dysku (SWAP)

44.5 Ilości pakietów otrzymanych w ciągu sekundy

44.6 Ilości pakietów wysyłanych w ciągu sekundy

45. Rozwiązanie musi pozwalać zdefiniować synchronizację w oparciu o serwer czasu NTP i wybór strefy czasowej

46. Rozwiązanie musi pozwalać na konfigurację wymiennika poczty, przez który wysyłane są wiadomości pocztowe do Internetu

47. Rozwiązanie musi pozwalać włączyć przechowywanie payload, dla każdego zdarzenia

48. Rozwiązanie musi pozwalać stosować kompresję zdarzeń w określonym interwale czasu. Zdarzenia posiadające te same kluczowe wartości (określone w punkcie 16.) w tym interwale czasowym zapamiętywane są w postaci jednego wpisu w bazie i liczby informującej ile takich zdarzeń we wspomnianym interwale czasowym zostało zarejestrowanych. Jednocześnie w bazie zapisywany jest payload zdarzenia ostatniego w tej sekwencji w określonym interwale czasu.

49. Sposób przechowywania zdarzeń opisany w punkcie 48. może także zostać wyłączony i wtedy każde zdarzenie ma przechowywany payload w bazie.

50. Rozwiązanie musi pozwalć uwierzytelniać użytkowników do swojego web GUI przy pomocy jednego z dostępnych sposobów: kont lokalnych, bazy RADIUS, bazy TACACS, Active Directory i LDAP. O wyborze sposobu uwierzytelnienia decyduje administrator systemu.

51. Do konta każdego z użytkowników musi istnieć możliwość przypisania roli związanej z posiadanymi w tym systemie uprawnieniami oraz wskazać pule adresowe IP (wybrane ze zdefiniowanej struktury adresacji wspomnianej w punkcie 40.), dotyczące zawartości zdarzeń i przepływów rejestrowanych przez system. W ten sposób wewnątrz tej samej roli można dać użytkownikom dostęp do logów z tych samych systemów, ale dotyczących różnych adresacji IP (można uzyskać w ten sposób wybór tylko części logów firewall i przypisać tą część do konta użytkownika).

52. Do opisanych w puncie 51. ról musi istnieć możliwość przypisania listy poszczególnych źródeł logów.

53. Role muszą pozwalać na przypisanie uprawnień w oparciu o przyznanie praw do:

53.A Zarządzania innymi administratorami systemu

53.B Zarządzania systemem

53.C Konfiguracją struktury adresowej

53.D Tworzenia reguł dotyczących zdarzeń (opisanych w punkcie 65.)

53.E Tworzenia własnych szczegółów zdarzeń (nowych pól w tablicach zdarzeń – odniesienie do właściwości opisanych w punkcie 17.)

53.F Tworzenie trendów czasowych dla zdarzeń w zakresie prezentacji wyników wyszukiwania

53.G Podglądu przepływów (flows)

53.H Tworzenie trendów czasowych dla przepływów w zakresie prezentacji wyników wyszukiwania

53.I Tworzenia reguł dotyczących przepływów (opisanych w punkcie 65.)

53.J Tworzenia własnych szczegółów przepływów (nowych pól w tablicach przepływów – na podobnej zasadzie jak cechy opisane w punkcie 17.)

53.K Dostępu do opcji po wybraniu prawego klawisza myszki w GUI

53.L Tworzenia reguł incydentów bezpieczeństwa – opisanych w punkcie 66.

53.M Przypisywania incydentów bezpieczeństwa do użytkowników

53.N Usuwania danych o podatnościach z opisanych w systemie zasobów (w nawiązaniu do punktu 61.)

53.O Włączenia mechanizmów automatycznego wykrywania zasobów (w nawiązaniu do punktu 61.)

53.P Podglądu informacji o odkrytych podatnościach dla opisanych w systemie zasobów (w nawiązaniu do punktu 61.)

53.R Wykonywania automatycznych skanowań podatności na opisanych zasobach (w nawiązaniu do punktu 61.)

53.S Tworzenia szablonów raportów

53.T Dystrybucji raportów poprzez email

54. Rozwiązanie musi pozwalać skonfigurować automatyczny dostęp dla innych aplikacji, dzięki czemu można obsługiwać incydenty bezpieczeństwa z innych systemów obsługi zgłoszeń potocznie zwanych HelpDesk

55. Rozwiązanie musi pozwalać automatycznie wykrywać źródła logów, które przesyłane/pobierane są przy pomocy przynajmniej części mechanizmów opisanych w punkcie 15. i dotyczą następujących producentów i rodzin ich produktów:

* + 3COM 8800 SERIES SWITCH
  + AMBIRON TRUSTWAVE IPANGEL
  + APACHE HTTP SERVER
  + APC UPS
  + APPLE MAC OS X
  + ARUBA MOBILITY CONTROLLERS
  + ARRAY NETWORKS SSL VPN
  + BALABIT IT SECURITY
  + Barracuda Spam & Virus Firewall
  + Barracuda Web Application Firewall
  + BIT9 PARITY
  + BLUE COAT SG
  + BRIDGEWATER
  + CA TECHNOLOGIES CA ACF2
  + CA SiteMinder
  + CA Top Secret
  + Check Point FireWall-1
  + Check Point Provider-1
  + Cisco ACE Firewall
  + Cisco Aironet
  + Cisco ACS
  + Cisco ASA
  + Cisco CatOS for Catalyst Switches
  + Cisco CSA
  + Cisco FWSM
  + Cisco IDS/IPS
  + Cisco IronPort
  + Cisco NAC
  + Cisco Nexus
  + Cisco IOS
  + Cisco Pix
  + Cisco VPN 3000 Concentrator
  + Cisco Wireless Services Module
  + CITRIX NETSCALER
  + CRYPTOCARD CRYPTO-SHIELD
  + CYBER-ARK VAULT
  + CYBERGUARD FIREWALL/VPN APPLIANCE
  + DAMBALLA FAILSAFE
  + DIGITAL CHINA NETWORKS (DCN)
  + EMC VMWARE
  + Enterasys Dragon
  + Enterasys HiGuard Wireless IPS
  + Enterasys HiPath Wireless Controller
  + Enterasys Stackable and Standalone Switches
  + Enterasys XSR Security Router
  + Enterasys Matrix Router
  + Enterasys NetSight Automatic Security Manager
  + Enterasys Matrix K/N/S Series Switch
  + Enterasys NAC
  + EXTREME NETWORKS EXTREMEWARE
  + F5 Networks BIG-IP LTM
  + F5 Networks BIG-IP ASM
  + F5 Networks FirePass
  + FAIR WARNING
  + FIREEYE
  + FORESCOUT COUNTERACT
  + FORTINET FORTIGATE
  + FOUNDRY FASTIRON
  + GREAT BAY BEACON
  + HBGARY ACTIVE DEFENSE
  + HP ProCurve
  + HP Tandem
  + Hewlett Packard UNIX (HP-UX)
  + HUAWEI
  + IBM AIX
  + IBM AS/400 iSeries
  + IBM CICS
  + IBM Lotus Domino
  + IBM Proventia Management SiteProtector
  + IBM ISS Proventia
  + IBM RACF
  + IBM DB2
  + IBM WebSphere Application Server
  + IBM Informix Audit
  + IBM IMS
  + IBM Guardium
  + IBM Tivoli Access Manager for e-business
  + IBM z/OS
  + ISC BIND
  + IMPERVA SECURESPHERE
  + INFOBLOX NIOS
  + IT-CUBE AGILESI
  + ITRON SMART METER
  + Juniper Networks AVT
  + Juniper DX Application Acceleration Platform
  + Juniper EX-Series Ethernet Switch
  + Juniper NetScreen IDP
  + Juniper Networks Secure Access
  + Juniper Infranet Controller
  + Juniper Networks Firewall and VPN
  + Juniper Networks Network and Security Manager
  + Juniper JunOS
  + Juniper Steel-Belted Radius
  + Juniper Networks vGW Virtual Gateway
  + Juniper Security Binary Log Collector
  + LIEBERMAN RANDOM PASSWORD MANAGER
  + Linux DHCP
  + Linux IPtables
  + Linux OS
  + McAfee Intrushield
  + McAfee ePolicy Orchestrator
  + McAfee Application / Change Control
  + McAfee Web Gateway
  + METAINFO METAIP
  + Microsoft Exchange Server
  + Microsoft IAS Server
  + Microsoft DHCP Server
  + Microsoft IIS Server
  + Microsoft ISA
  + Microsoft SQL Server
  + Microsoft SharePoint
  + Microsoft Windows Security Event Log
  + Microsoft Operations Manager
  + Microsoft System Center Operations Manager
  + MOTOROLA SYMBOL AP
  + NETAPP DATA ONTAP
  + NAME VALUE PAIR
  + NVP Log Format
  + NIKSUN
  + NOKIA FIREWALL
  + Nortel Multiprotocol Router
  + Nortel Application Switch
  + Nortel Contivity
  + Nortel Ethernet Routing Switch 2500/4500/5500
  + Nortel Ethernet Routing Switch 8300/8600
  + Nortel Secure Router
  + Nortel Secure Network Access Switch
  + Nortel Switched Firewall 5100
  + Nortel Switched Firewall 6000
  + Nortel Threat Protection System
  + Nortel VPN Gateway
  + NOVELL EDIRECTORY
  + OPENBSD
  + OPEN LDAP
  + OPEN SOURCE SNORT
  + Oracle Audit Records
  + Oracle DB Listener
  + Oracle Audit Vault
  + Oracle OS Audit
  + Oracle BEA WebLogic
  + PALO ALTO NETWORKS
  + PROFTPD
  + RADWARE DEFENSEPRO
  + REDBACK ASE
  + RSA AUTHENTICATION MANAGER
  + SAMHAIN LABS
  + SENTRIGO HEDGEHOG
  + SECURE COMPUTING SIDEWINDER
  + SOLARWINDS ORION
  + SONICWALL
  + Sophos Enterprise Console
  + Sophos PureMessage
  + Sophos Astaro Security Gateway
  + Sophos Web Security Appliance
  + Sourcefire Intrusion Sensor
  + Sourcefire Defense Center (DC)
  + SQUID WEB PROXY
  + STARENT NETWORKS
  + STONESOFT MANAGEMENT CENTER
  + Sun Solaris
  + Sun Solaris DHCP
  + Sun Solaris Sendmail
  + Sun Solaris Basic Security Mode (BSM)
  + SYBASE ASE
  + Symantec Endpoint Protection
  + Symantec SGS
  + Symantec System Center
  + Symantec Data Loss Prevention (DLP)
  + SYMARK
  + TippingPoint Intrusion Prevention System
  + TippingPoint X505/X506 Device
  + TOP LAYER IPS
  + Trend Micro InterScan VirusWall
  + Trend Micro Control Manager
  + Trend Micro Office Scan
  + Trend Micro Deep Discovery
  + TRIPWIRE
  + TROPOS CONTROL
  + VERDASYS DIGITAL GUARDIAN
  + VERICEPT CONTENT 360
  + WEBSENSE V-SERIES
  + Websense TRITON
  + Websense V-Series Data Security Suite
  + Websense V-Series Content Gateway

56. Dla rozwiązań niewymienionych w punkcie 55. musi istnieć możliwość stworzenia własnych szablonów analizy przy pomocy modyfikacji danych dostarczonych przez producenta i wskazania sposobu poboru tych danych zgodnie z punktem 15.

57. Rozwiązanie musi pozwalać zdefiniować szczegółową politykę retencji dla przechowywanych danych w bazie w oparciu o wskazane wartości poszczególnych pól w bazie (w nawiązaniu do punktu 16. i 17.)

58. Rozwiązanie musi pozwalać zdefiniować szczegółową politykę retencji dla przepływów przechowywanych w bazie w oparciu o wskazane wartości poszczególnych pól w bazie (w nawiązaniu do punktu 32. i 33.)

60. Rozwiązanie musi pozwalać tworzyć grupy dla poszczególnych zdefiniowanych źródeł logów i następnie odwoływanie się do nich podczas tworzenia szablonów wyszukiwania

61. Rozwiązanie musi pozwalać gromadzić informację o zasobach widocznych w logach różnych systemów i gromadzonych przepływach.

62. Rozwiązanie musi pozwalać na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach (w nawiązaniu do punktu 61.) o bardziej szczegółowe dane do korelacji zdarzeń w oparciu o zidentyfikowane podatności i otwarte porty

63. Rozwiązanie musi pozwalać na integrację z produktami do zarządzania podatnościami:

* + eEye Digital Security: eEye REM oraz eEye Retina CS
  + Generic AXIS
  + IBM IBM Security AppScan Enterprise
  + Juniper NSM Profiler
  + Lumenison Patchlink
  + McAfee Foundstone Vulnerability Manger
  + nCircle ip360
  + Nessus
  + netVigilance SecureScout
  + nmap (produkt Open Source)
  + Qualys QualysGuard
  + Rapid7 NeXpose
  + Saint Corporation Saintscanner
  + Tenable Security Center

64. Rozwiązanie musi zawierać własną bazę adresów IP w Internecie, które rozpoznawane są jako znane źródła Malware, Botnet C&C (Command Control), a także tworzenie własnych zdalnych lub podejrzanych grup adresowych (np. adres pętli 127.0.0.1) i wyzwala incydenty gdy system SIEM zauważy próby połączeń do tych adresów (według reguł w nawiązaniu do punktu 66.)

**CECHY UŻYTKOWE – TWORZENIE I OBSŁUGA INCYDENTÓW BEZPIECZEŃSTWA**

65. Rozwiązanie musi pozwalać tworzyć reguły wykrywania gdy aktualna sytuacja odbiega w jakiś sposób od normy w odniesieniu do zdarzeń i przepływów przy pomocy następujących mechanizmów (nie łączy się w tych regułach zdarzeń z przepływami):

65.A Porównywanie wielkości odchylenia od wartości średniej przy zastosowaniu agregacji w oparciu o jeden wymiar i obserwacji innej zakumulowanej liczby różnych wartości innego wymiaru (jeden z wymiarów: adres IP źródłowy, adres IP przeznaczenia, nazwa zdarzenia, ilości zdarzeń, priorytetu zdarzeń , kategorii zdarzeń, nazwy protokołu, nazwy użytkownika) w ustalonym przedziale czasowym i jednoczesnym wskazaniu okresu (określonego datą początku i końca lub dni tygodnia i wskazanego przedziału godzin)

65.B Odchylenia przy zastosowaniu agregacji w oparciu o jeden wymiar i obserwacji innej zakumulowanej liczby różnych wartości innego wymiaru (nauczony obserwacją/próbkowaniem) (jeden z wymiarów: adres IP źródłowy, adres IP przeznaczenia, nazwa zdarzenia, ilości zdarzeń, priorytetu zdarzeń , kategorii zdarzeń, nazwy protokołu, nazwy użytkownika), a dokładnie poziomu tej zakumulowanej wartości, trendu (wzrost i spadek) oraz porównanie zakumulowanej wartości tego wymiaru do odpowiadającego mu poziomu w chwili w przeszłości. Reguły te pozwalają określić interwał czasowy (data startu i końca, albo dni o godziny w tygodniu)

65.C Przekroczenie ustalonego progu pewnego wymiaru (ilości jego różnych wartości) w stosunku do innego zagregowanego parametru ze wskazaniem długości trwania interwału czasowego, albo daty startu i końca, albo dni i godzin w tygodniu

66. Rozwiązanie musi posiadać przynajmniej 250 domyślnie dostępnych reguł generujących incydenty bezpieczeństwa na podstawie jednego z poniższych kryteriów, a także ich połączenia logiczne z wykorzystaniem także zaprzeczeń:

66.1 Reguły incydentów bazujące tylko na zdarzeniach

66.2 Reguły incydentów bazujące tylko na przepływach

66.3 Reguły incydentów bazujące jednocześnie na przepływach i zdarzeniach

66.4 Reguły bazujące na innych incydentach

67. Reguły bazujące na incydentach muszą umożliwiać zastosowanie następujących gotowych konstrukcji:

67.A Kiedy połączenie inicjowane jest przez jedną ze wskazanych sieci lokalnych (odniesienie do struktury adresacji opisanej w punkcie 40.)

67.B Kiedy połączenie inicjowane jest do jednej ze wskazanych sieci przeznaczenia (odniesienie do struktury adresacji opisanej w punkcie 40.)

67.C Kiedy dany protokół występujący w zdarzeniu jest jednym ze wskazanych

67.D Kiedy zdarzenie zawiera wskazany ciąg znaków

67.E Kiedy port źródłowy jest jednym ze wskazanych

67.F Kiedy port przeznaczenia jest jednym ze wskazanych

67.G Kiedy połączenie inicjowane jest przez jeden ze wskazanych adresów IP

67.H Kiedy połączenie inicjowane jest do jednego ze wskazanych adresów IP

67.I Kiedy adres źródłowy lub przeznaczenia jest jednym ze wskazanych

67.J Kiedy zdarzenie zostało dostarczone przez jedno ze wskazanych źródeł logów

67.K Kiedy zdarzenie zostało dostarczone przez jedno ze źródeł wskazanego typu

67.L Kiedy zdarzenie wydarzyło się we wskazanych dniach w miesiącu

67.M Kiedy zdarzenie wydarzyło się we wskazanych dniach w tygodniu

67.N Kiedy zdarzenie ma wartość jednego z parametrów składających się na priorytet większą niż wskazana wartość

67.O Kiedy ruch pochodzi z wybranej lokalizacji geograficznej (wskazanie nazwy kraju)

67.P Kiedy punkt przeznaczenia jest podatny na atak (określone na podstawie zgromadzonych informacji – w nawiązaniu do punktu 61. i 62.)

67.R Kiedy wszystkie ze wskazanych reguł będą miały miejsce w dowolnym porządku lub wskazanym i jeden z parametrów w nawiasie (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) będzie taki sam lub dowolny i jednocześnie kolejny parametr z nawiasu (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) będzie taki sam lub dowolny przez wskazany okres czasu

67.S Podobnie jak wyżej, ale można zdefiniować ile przynajmniej reguł musi znaleźć dopasowanie

67.T Kiedy zachodzi sekwencja reguł, w których zaangażowany jest ten sam adres IP źródłowy i przeznaczenia (w porównaniu z poprzednim dopasowaniem) przez wskazany czas

67.U Kiedy dowolny z parametrów w nawiasie (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) pasuje więcej lub mniej niż wskazana liczba reguł w odniesieniu do większej niż wskazana liczba parametrów w nawiasie (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) przez wskazany okres czasu

67.W Kiedy dowolny z parametrów w nawiasie (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) przez więcej lub mniej niż wskazana liczba reguł jest taki sam jak inny parametr z nawiasu (źródłowy adres IP, port źródłowy, port przeznaczenia, adres IP przeznaczenia, źródło zdarzenia) przez wskazany okres czasu

67.Y Kiedy zdarzenie nie zostało zarejestrowane z przynajmniej jednego ze wskazanych źródeł logów przez wskazany przedział czasu

67.Z Kiedy zdarzenia zostały przekazane przez jedno lub więcej ze wskazanych źródeł zdarzeń

67.A.1 Kiedy przynajmniej wskazana liczba reguł ze wskazanych reguł w określonym porządku/ lub dowolnym porządku z tym samym parametrem z nawiasu (nazwa użytkownika, adres źródłowy IP, źródłowy port, adres IP przeznaczenia, port przeznaczenia), w następstwie czego wystąpiło przynajmniej dopasowanie do wskazana liczby reguł w określonym/lub dowolnym porządku do/lub z tego samego jednego parametru wybranego z nawiasu (nazwa użytkownika, adres źródłowy IP, źródłowy port, adres IP przeznaczenia, port przeznaczenia) przez wskazany okres czasu

67.A.2 Kiedy wybrany parametr z nawiasu (nazwa użytkownika, nazwa użytkownika w odniesieniu do kierunku zdarzenia, nazwa hosta, nazwa hosta w odniesieniu do kierunku zdarzenia, system operacyjny, system operacyjny w odniesieniu do kierunku zdarzenia, zawartość logu) dopasowuje się do wskazanego wyrażenia regularnego

67.A.3 Kiedy wybrany parametr z nawiasu (MAC, nazwa użytkownika, nazwa hosta) zmienia się więcej niż wskazana liczba razy w ciągu wskazanego okresu czasu w odniesieniu do pojedynczego systemu, o którym rozwiązanie SIEM gromadzi informacje (w odniesieniu do punktu 61.)

67.A.4 Kiedy źródłowy adres IP wersja 6 jest jednym ze wskazanych adresów IP w wersji 6.

67.A.5 Kiedy jeden z parametrów w nawiasie (adres źródłowy, adres przeznaczenia, dowolny adres IP) jest częścią jednej z sieci określonych jako zdalne (w odniesieniu do struktury opisanej w punkcie 64)

67.A.6 Kiedy jeden z parametrów w nawiasie (adres źródłowy, adres przeznaczenia, dowolny adres IP) pochodzi ze wskazanego regionu geograficznego

67.A.7 Kiedy adres źródłowy lub przeznaczenia jest jednym ze wskazanych portów

67.A.8 Kiedy zdarzenie dopasuje się do wskazanego wyszukiwania (określonego parametrami z punktu 16. i własnych parametrów jak w punkcie części 17.)

67.A.9 Kiedy jakikolwiek z parametrów w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) dopasowuje się do wskazanego wyrażenia regularnego

67.A.10 Kiedy jakikolwiek z parametrów w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) zawiera jedną ze wskazanych wartości hexadecymalnie

67.A.11 Kiedy wskazana liczba zdarzeń zawiera ten sam wskazany jeden z parametrów wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) w ciągu wskazanego okresu czasu

67.A.12 Kiedy wskazana liczba zdarzeń zawiera ten sam wskazany jeden z parametrów wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) i jednocześnie różny inny wskazany jeden z parametrów wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) w ciągu wskazanego okresu czasu

67.A.13 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu

67.A.14 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu ze wskazanym tym samym jednym parametrem z wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.15 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu ze wskazanym tym samym jednym parametrem z wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) oraz różnym wskazanym jednym z parametrów wymienionych w nawiasie (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.16 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak dopasują się wcześniej wskazane reguły

67.A.17 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak dopasują się wcześniej wskazane reguły z tym samym wskazanym parametrem z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.18 Kiedy wskazane reguły dopasowują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak dopasują się wcześniej wskazane reguły z tym samym wskazanym parametrem z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) i różnym wskazanym jednym parametrem z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.19 Kiedy wskazane reguły dopasują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak inne wskazane reguły dopasują się z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.20 Kiedy wskazane reguły z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) dopasują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak inne wskazane reguły dopasują się z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.21 Kiedy wskazane reguły z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) i różnym innym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) dopasują się przynajmniej wskazaną liczbę razy w ciągu wskazanego okresu czasu po tym jak inne wskazane reguły dopasują się z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.22 Kiedy przynajmniej wskazana liczba zdarzeń wystąpi z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) i różnym innym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) przez wskazany okres czasu po tym jak wskazane reguły znajdą dopasowanie

67.A.23 Kiedy przynajmniej wskazana liczba zdarzeń wystąpi z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) przez wskazany okres czasu po tym jak wskazane reguły dopasują się z tym samym wskazanym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.24 Kiedy przynajmniej wskazana liczba zdarzeń wystąpi z tym samym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) i różnym innym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.) przez wskazany okres czasu po tym jak wskazane reguły dopasują się z tym samym wskazanym parametrem wybranym z nawiasu (pochodzące z głównych parametrów tabel jak w punkcie 16. oraz zdefiniowanych przez użytkownika w punkcie 17.)

67.A.25 Kiedy żadna ze wskazanych reguł nie dopasuje się w ciągu wskazanego okresu czasu po tym jak wskazane reguły znalazły dopasowanie

68. Rozwiązanie musi umożliwiać zastosowanie podobnych konstrukcji jak wymienione w punkcie 67., ale do przepływów (flows)

69. Rozwiązanie musi umożliwiać zastosowanie podobnych konstrukcji jak opisane w punkcie 67. ale w odniesieniu do połączonych informacji ze zdarzeń i przepływów

70. Rozwiązanie musi umożliwiać zapisanie konstrukcji reguł jako makr do użycia przy tworzeniu kolejnych bardzo złożonych reguł

71. System SIEM musi umożliwiać przeglądanie incydentów bezpieczeństwa w odniesieniu do adresów źródłowych IP, adresów IP przeznaczenia, a także incydentów przypisanych do użytkownika, który jest aktualnie zalogowany

72. Rozwiązanie musi umożliwiać grupowanie reguł opisanych w punktach 67. 68. i 69. w celu otrzymania tematycznej struktury i łatwego odszukania interesującej reguły

73. Dla poszczególnych incydentów prezentowane muszą być najważniejsze informacje takie jak nazwa reguły, która go wywołała, adresy źródłowe i przeznaczenia, a także daje możliwość bezpośredniego otwarcia informacji o zdarzeniach i przepływach, które spowodowały utworzenie tego incydentu, opisanie incydentu notatkami, przypisanie danego incydentu do użytkownika systemu SIEM oraz zamknięcie incydentu.

74. Dla poszczególnych incydentów prezentowane musza być także reguły powiązane

75. Musi być możliwe jest tworzenie reguł bazujących na samych incydentach i określanie dodatkowych akcji

76. Dla każdej reguły utworzonej przy pomocy konstrukcji opisanych w punktach 67., 68., 69. oraz 75. muszą być możliwe następujące akcje: przypisanie parametrów częściowych, na podstawie których wyliczana jest wartość priorytetu takiego zdarzenia, utworzenie incydentu prezentowanego w konsoli incydentów i dalsze nim zarządzanie, powołanie kolejnego zdarzenia, wysłanie email pod wskazany adres, wysłanie komunikatu SNMP Trap, wysłanie komunikatu do lokalnego serwera syslog, wysłanie komunikatu do zdefiniowanego serwera np. syslog, powiadomienie w konsoli.

77. System SIEM musi gromadzić informacje o działaniach administratorów w szczególności obsłudze incydentów

**CECHY UŻYTKOWE - RAPORTOWANIE**

78. Rozwiązanie musi pozwalać tworzyć raporty w oparciu o szablony wyszukiwania wraz z określonym w nich wymiarem agregacji lub też zapisanego trendu poszczególnych wartości w czasie

79. Zdefiniowane raporty muszą być generowane regularnie we wskazanym planie czasowym i wysyłane w postaci email na wskazane adresy.

80. Rozwiązanie musi pozwalać tworzyć raporty w następujących formatach: PDF, HTML, RTF, XML i XLS.

Obsługa flow:

a.      wymagana jest korelacja pomiędzy różnymi źródłami flow tego samego flow, czyli przepływ wykryty przez interfejs, netflow, sflow widziany jest w konsoli administratora jako jeden przepływ pochodzący od 3 źródeł informacji.

b.      Flow powinien być aktualizowany w czasie rzeczywistym na podstawie aktualizacji przesyłanych przez urządzenia, czyli 3 kolejne komunikaty netflow powiększają/zmieniają dane w wyświetlanym połączeniu, a nie dodają nowy wpis z tym samym IP, portem, aplikacją w systemie.

Wyklucza się zastosowanie technologii wirtualizacji serwerów w jakiejkolwiek postaci. Jedynym dopuszczalnym rozwiązaniem jest platforma sprzętowa i instalowane na niej bezpośrednio oprogramowanie właściwe.

**ELEMENT 5**

**Skaner podatności sieci**

1. System zarządzania podatnością musi zostać dostarczony albo jako dedykowany system (oprogramowanie oraz sprzęt) albo jako dodatkowy moduł do systemu SIEM.
2. System zarządzania podatnością musi umożliwiać skanowanie i wykrywanie podatności następujących systemów operacyjnych eksploatowanych przez Zamawiającego: Windows, Linux.
3. System zarządzania podatnością musi umożliwiać skanowanie i wykrywanie podatności następujących serwerów baz danych eksploatowanych przez Zamawiającego: Oracle, MS SQL
4. System zarządzania podatnością musi umożliwiać skanowanie i wykrywanie podatności urządzeń następujących producentów posiadanych przez Zamawiającego: Cisco, F5, Juniper, Checkpoint.
5. System zarządzania podatnością musi wykrywać podatności umożliwiające nieuprawniony dostęp do Systemu.
6. System zarządzania podatnością musi umożliwiać skanowanie podatności w trybie pracy bez agenta lokalnego.
7. Baza danych podatności wykorzystywana przez rozwiązanie musi być regularnie aktualizowana. Interwał aktualizacji nie może przekraczać 3 dni.
8. System zarządzania podatnością musi skanować systemy pod kątem aktualności zainstalowanych uzupełnień systemów operacyjnych.
9. System zarządzania podatnościami musi posiadać możliwość integracji z oferowanym systemem SIEM w zakresie:
   1. Podatności muszą być widoczne w systemie SIEM.
   2. Podatności musza być powiązane z assetami w systemie SIEM
   3. System zarządzania podatnością musi mieć możliwość powiązania podatności konkretnych systemów z analizowanym przez SIEM ruchem sieciowym w celu określenie wagi podatności i priorytetu jej usunięcia.
10. System zarządzania podatnością musi skanować otwarte porty na serwerach i urządzeniach sieciowych.
11. System zarządzania podatnością musi wykrywać usługi uruchomione na serwerach.
12. System zarządzania podatnością musi wykrywać konta użytkowników z podatnymi na atak hasłami.
13. System zarządzania podatnością musi prezentować wyniki skanowania w postaci raportów wraz z rekomendacjami usunięcia wykrytych podatności.
14. System zarządzania podatnością musi umożliwiać skanowanie dowolnej ilości urządzeń pracujących w dowolnej ilości podsieci.
15. System zarządzania podatnością musi umożliwiać harmonogramowanie zadań skanowania lub uruchamianie ich na żądanie.
16. System zarządzania podatnościami musi umożliwiać zaawansowane widoki wykorzystujące filtrowanie i agregowanie podatności aby pomóc zidentyfikować i oznaczyć najbardziej krytyczne podatności. Wśród dostępnych filtrów powinny być:
    1. Nieprzypisane podatności
    2. Status podatności (nowy, istniejący, naprawiane)
    3. Ryzyko
    4. CVSS Score większy niż X
    5. Podatność wyjątek
17. System zarządzania podatnością musi pozwalać na bezpłatną aktualizację bazy danych podatności przez okres 5 lat.

**ELEMENT 6**

**Rozbudowa klastra HPC**

## Opis ogólny

Przedmiotem rozbudowy jest środowisko klastra HPC obecnie użytkowane przez Zamawiającego. Zadaniem klastra jest efektywne realizowanie obliczeń naukowych, zarówno pod względem wydajności procesorów, sieci obliczeniowej oraz składowania danych tymczasowych. Obecna konfiguracja składa się z szesnastu węzłów serwerowych realizujących obliczenia, macierzy dyskowej oraz z serwera zarządzającego na którym zainstalowane jest oprogramowanie kolejkujące.

Wszystkie moduły klastra korzystają z sieci LAN 10Gb opartej na przełączniku Juniper model EX4200.

Przestrzeń dyskowa wymagana do realizacji obliczeń skonfigurowana jest na macierzy IBM V7000 i udostępniona poszczególnym węzłom poprzez sieć SAN. Każdy z węzłów oraz serwer zarządzający podłączony jest do macierzy w sposób redundantny połączeniem FC o prędkości pojedynczego linku 8Gb/s. Sieć SAN zbudowana jest na dwóch przełącznikach FC wykonanych w technologii 8Gb/s, wyposażonych w 24 aktywne porty FC. Każdy z przełączników tworzy niezależny fabric FC dla zapewnienia redundancji.

**Konfiguracja rozbudowywanego środowiska**

Pamięć masowa 1 komplet

|  |  |
| --- | --- |
| P/N | Opis |
| 2076-324 | IBM Macierz Storwize V7000 Disk Control Enclosure szt. 1 |
| 3251 | 146GB 2.5in. 15K SAS HDD szt. 22 |
| 3512 | 200GB 2.50inch SSD (E-MLC) szt. 2 |

Węzły obliczeniowe szt. 16

|  |  |
| --- | --- |
| P/N | Opis |
| 791283G | dx360 M4, 2xXeon 10C E5-2670v2 115W 2.5GHz/1866MHz/25MB, 4x8GB, O/Bay SS 3.5in SATA, szt.1 |
| 00D5048 | 16GB (1x16GB, 2Rx4, 1.5V) PC3-14900 CL13 ECC DDR3 1866MHz LP RDIMM szt. 6 |
| 42D0494 | Emulex 8Gb FC Dual-port HBA for IBM System x szt. 1 |
| 90Y6456 | Emulex Dual Port 10GbE SFP+ Embedded VFA III for IBM System x szt. 1 |
| 49Y4216 | Brocade 10Gb SFP+ SR Optical Tranceiver szt. 2 |
| 90Y3901 | IBM Integrated Management Module Advanced Upgrade szt. 1 |
|  | Red Hat Enterprise Linux Server 2 Skts 1 Guest szt. 1 |

Sieć SAN, 2 komplety

|  |  |
| --- | --- |
| P/N | Opis |
| a) 249824E | Express IBM System Storage IBM SAN24B-4 szt 1 |
| b) 45W0502 | 8-port Activation szt. 2 |
| c) 45W0501 | SFP 8Gbps SW 8-Pack szt. 3 |

## Wymagania szczegółowe dla rozbudowy klastra

1. Liczba dostarczanych węzłów klastra: minimum 16 sztuk.
2. Sieć SAN: minimum dwa przełączniki FC zapewniające redundatne połaczenie oferowanych węzłów do macierzy dyskowej wymienionej w opisie ogólnym klastra. Liczba portów w przełącznikach pozwalająca na podłączenie każdego węzła klastra wszystkim dostępnymi portami FC w węźle
3. Pamięć masowa: rozbudowa obecnie wykorzystywanej przestrzeni dyskowej o dodatkową pojemność 6.9TB RAW. Przestrzeń dyskowa po rozbudowie ma stanowić z obecną przestrzenią jeden wolumen udostępniony dla wszystkich nodów obecnych w konfiguracji klastra tj, węzłów zarówno w cześci dostarczanej oraz obecnie wykorzystywanej przez Zamawiającego. W ramach oferowanej rozbudowy należy przewidzieć minimum jeden dysk spare odpowiadający parametrom oferowanych dysków.
4. Sieć LAN: Porty 10Gb/s wymagane do podłączenia węzlów do sieci LAN Zamawiającego zostaną zapewnione w ramach obecnie wykorzystywanej infrastruktury.
5. Oprogramowanie zarządzające: oferowane węzły muszą posiadać możliwość integracji z obecnym środowiskiem kolejkującym, pozwalając na utworzenie jedenej domeny obliczeniowej. Wszelkie licencje wymagane do uruchomienie oprogramowania należy zapewnic w ramach dostawy klastra.
6. Dla zapewnienia spójności działania i zwiększenia jednolitości mechanizmów zarządzania wymagane jest, aby dostarczane węzły obliczeniowe oraz pamięć masowa były jednego producenta

### Wymagania szczegółowe Konfiguracja węzłów:

1. Procesory:
   1. Serwer musi być wyposażony w procesory o architekturze zgodnej z architekturą procesorów pracujących w obecnej farmie HPC.
   2. serwer musi posiadać zainstalowaną taką liczbę procesorów, aby osiągnąć łącznie minimum 20 rdzeni
   3. każdy rdzeń musi być taktowany zegarem minimum 2,3 GHz i realizować minimum 8 obliczeń zmiennoprzecinkowe w jednym cyklu zegarowym
   4. każdy procesor musi posiadać zintegrowany kontroler pamięci
   5. każdy serwer musi posiadać wydajność teoretyczną minimum 368 Gflops. Wydajnośc liczona przy załozeniu wykorzystania instrukcji AVX 1.0, z uwagi na charakterystykę aplikacji wykorzystywanych w środowisku Zamawiającego

Wydajność teoretyczna pojedyńczego procesora jest liczona wg. nastepującego wzoru:

Rproc = P \* C \* Z

gdzie,

P - to liczba rdzeni procesora,

C - prędkośc zegara natywna w GHz (bez turbo mode),

Z - liczba operacji zmiennoprzecinkowych typu dodawanie i mnożenie w podwójnej precyzji wykonywanych przez pojedynczy rdzeń procesora w jednym cyklu zegarowym. Dla procesorów Intel liczba operacji zmiennoprzecinkowych dla instrukcji AVX 1.0 wynosi 8

1. Pamięć operacyjna:
   1. łączna zainstalowana pamięć w pojedyńczym serwerze musi wynosić minimum 128 GB
   2. moduły pamięci muszą być wyposażone w mechanizm korekcji błędnych bitów i być równomiernie zainstalowane przy każdym procesorze;
   3. zastosowany musi być typ pamięci co najmniej PC3-14900
   4. Możliwość rozbudowy pamieci operacyjnej do 512GB
2. Dyski:
   1. brak dysków twardych
3. Interfejsy sieciowe:
   1. zainstalowane minimum dwa interfejsy sieciowe Gigabit Ethernet z funkcjonalnością uruchamiania serwera przez PXE;
   2. zainstalowane minimum dwa interfejsy 10 GbE
   3. zainstalowane minimum dwa interfejsy FC o przepustowości 8Gb/s
   4. wszystkie porty SAN oraz LAN dostepne w serwerze muszą być wyprowadzone z przodu obudowy z uwagi na zabudowę w serwerowni Zamawiającego
4. Porty:
   1. Dwa porty USB na przodzie obudowy
   2. Jeden wewnętrzny port USB
5. Rozszerzenia:
   1. Możliwość instalacji co najmniej dwóch kart GPU m.in Tesla K40 i innych Instalacji kart możliwa poprzez dodatkowy moduł rozszerzający
6. Obudowa:
   1. możliwość montażu w szafie rack 19 cali,
   2. szyny teleskopowe do montażu w szafie rack,
   3. zapewniająca wysoką gęstość upakowania węzłów, min 4 serwery na każde 2U wysokości dla oferowanych konfiguracji
   4. wysokość pojedyńczej obudowy maksimum 6U, z uwagi na ograniczone miejsce w szafach rack
   5. redundantne zasilacze o mocy wystarczającej do zasilenia wszystkich podzespołów w trybie zdegradowanym, wymienialne na gorąco (hot-swap), poziom redundancji N+1,
   6. redundantne wentylatory wymienialne na gorąco (hot-swap), poziom redundancji N+1,
7. Zarządzanie:
   1. zgodne z IPMI 2.0 lub lepsze
   2. dedykowany port zarzadzający z funkcjonalnościa przejęcia konsoli graficznej
   3. zdalny dostęp do serwera z obsluga klawiatury oraz myszki zdalnego klienta
   4. zdalne mapowanie napędów CD oraz DVD, USB, obrazów jako virtualne napędy
   5. zapewniające integrację z obecnie posiadanym przez klienta systemem zarządzania IBM Director. Zarządzanie jest rozumiane poprzez
      1. zdalne włączenie, wyłączenie i restart węzła
      2. autoryzację użytkowników
      3. administrację logami
      4. administrację ustawieniami sieciowymi
      5. pełen zdalny dostęp konsolowy umożliwiający pracę na węźle bez pośrednictwa systemu operacyjnego, przekierowanie standardowej konsoli (ttyX) w przypadku systemu Linux
      6. zdalne monitorowanie parametrów węzła
      7. wykonanie ww. operacji (oprócz dostępu konsolowego) na wielu węzłach jednocześnie z zastosowaniem skryptów, powinno to być możliwe takżę z uwzględnieniem autoryzacji użytkowników)
8. Systemy operacyjne:
   1. zainstalowany system operacyjny zgodny z obecnie użytkowanym systemem wymienionym w opisie ogólnym
   2. wspierane systemy: co najmniej RedHat Enterprise Linux, Microsoft Windows Server, VMware vSphere
9. Gwarancja producenta 5 lat z gwarantowanym czasem naprawy 24h.

### Wymagania szczegółowe przełączniki FC - 2 szt.

Konfiguracja pojedynczego przełącznika FC:

* Przełącznik FC musi być wykonany w technologii FC min. 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 gdy zastosowane są wkładki SFP 8Gb/s lub 4, 2, 1 Gb/s gdy zastosowane są wkładki SFP 4Gb/s.
* Przełącznik FC musi być wyposażony w taka liczbę aktywnych portów FC, aby podłączyć wszystkie węzły klastra do pamięci masowej zgodnie z wymaganiami opisanymi w SIWZ. Prędkość portów FC min. 8Gb/s.
* Wszystkie aktywne porty FC zaoferowanego przełącznika FC muszą być obsadzone wkładkami SFP 8Gb/s shortwave
* Rodzaj obsługiwanych portów, co najmniej: E, F oraz FL.
* Wszystkie zaoferowane porty przełącznika FC muszą działać bez tzw. over-subskrypcji pracując równocześnie z pełną prędkością 8Gb/s.
* Zsumowana przepustowość przełącznika FC musi wynosić minimum 384 Gb/s end-to-end full duplex.
* Przełącznik musi umożliwiać rozbudowę o funkcjonalność agregacji połączeń pomiędzy przełącznikami (trunking) na poziomie poszczególnych ramek. Konfiguracja logicznego połączenia „trunk” o przepustowości minimum 64 Gb/s.
* Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.
* Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
* Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
* Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:
  + Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric
  + Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP
  + Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP
  + Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów
  + Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
  + Konta użytkowników definiowane w środowisku RADIUS
  + Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
  + Obsługa SNMP v3
* Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
* Przełącznik FC musi zapewniać możliwość logowania zdarzeń poprzez mechanizm syslog.
* Przełącznik FC musi posiadać możliwość rozbudowy o mechanizm monitorowania wydajności „end-to-end” między wybranymi parami urządzeń inicjator-target.
* Przełącznik FC musi posiadać możliwość rozbudowy o mechanizm ciągłego monitorowania:
  + parametrów środowiskowych przełącznika takich jak temperatura czy status zasilaczy
  + parametrów pracy portów takich jak: zmiany stanu portu, liczniki błędów protokołu FC, parametry związane z ruchem FC i wydajnością
  + zasobów sieci fabric taki jak rekonfiguracje, zmiany zoningu, logowania administratorów
* Mechanizm monitorowania musi automatycznie powiadamiać administratora w przypadku przekroczenia zdefiniowanych wcześniej wartości granicznych. Powiadamianie musi być realizowane za pomocą wiadomości e-mail, trapów SNMP oraz wpisów do dziennika zdarzeń.
* Przełącznik FC musi umożliwiać instalację jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
* Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC
* Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)
* Przełącznik FC musi posiadać możliwość połączenia z innym przełącznikiem FC na odległość minimum 972km w trybie 1Gb/s, 486km w trybie 2Gb/s, 243km w trybie 4Gb/s oraz 121km w trybie 8Gb/s bez dodatkowych urządzeń buforujących.
* Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN
* Urządzenie musi wspierać mechanizm balansowania ruchem w oparciu o parametr OXID.
* Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

### Wymagania szczegółowe - przestrzeń dyskowa SAN

Wymagana jest rozbudowa przestrzeni dyskowej wymaganej do uruchomienia klastra HPC. Rozbudowywana przestrzen dyskowa musi byc udostepniona w docelowej konfiguracji jako jeden zasób uwzględniajac obecną przestrzeń klastra. Zasób dyskowy musi być widoczny dla wszystkich węzłów klastra.

Wymagania:

1. rozbudowa posiadanej przez Zamawiającego macierzy o min. jedną półkę dyskową z co najmniej 24 dyskami
2. Dyski o pojemności minimum 300GB i predkości obrotowej min. 15 000 rpm
3. redundante zasilanie
4. Redundantne pętle SAS do podłączenia do kontrolerów
5. Gwarancja producenta 5 lat z gwarantowanym czasem naprawy 24h

Zamawiający dopuszcza zastosowanie rozwiązania równoważnego w postaci nowej macierzy, przy czym oferowane rozwiązanie musi spełniać poniższe warunki równoważności:

1. Przestrzeń musi być zbudowana w oparciu o 46 dysków 300 GB oraz 2 dyski SSD 200GB. Wszystkie zainstalowane dyski talerzowe min. 15 000 rpm..
2. Macierz musi umożliwiać rozbudowę do co najmniej 240 dysków (w konfiguracji dysków 3,5”) oraz do co najmniej 480 dysków (w konfiguracji dysków 2,5”) poprzez mechanizm klastrowania lub dodawania par kontrolerów.
3. Macierz musi posiadać pamięć cache co najmniej 16GB, po 8GB na kontroler z możliwością rozbudowy łącznie do 64GB. Rozbudowa możliwa poprzez mechanizm klastrowania lub dodawania par kontrolerów.
4. Macierz musi zabezpieczać dyski mechanizmami RAID 0, 1, 5, 6, 10.
5. Macierz musi posiadać funkcjonalność automatycznie odbudowywania danych z uszkodzonego dysku na wolnej przestrzeni SPARE.
6. Półki dyskowe muszą być podłączone do każdego z kontrolerów przez min. 2 redundantne połączenia FC lub SAS.
7. Min. 2 redundantne kontrolery macierzowe.
8. Wszystkie kontrolery muszą pracować w trybie active-active.
9. Oferowana konfiguracja musi zawierać mechanizm nie powodujący wyłączenia cache do zapisu w przypadku awarii kontrolera, przy zapewnieniu redundancji pamięci write-cache.
10. Każdy kontroler musi być wyposażony w minimum 4 porty FC 8Gbit, 2 porty Ethernet 1Gbit oraz 2 porty 10GbE.
11. Macierz musi posiadać możliwość wykonywania kopii danych typu klon mechanizmami macierzy (licencja na wykonywanie kopii pełnych musi być zawarta w oferowanej cenie macierzy)
12. Macierz musi posiadać możliwość wykonywania kopii danych typu snapshot mechanizmami macierzy. Minimalna liczba kopii nie może być mniejsza niż 100, w tym możliwość wykonywania kopii z kopii oraz promowania migawki do trybu RW
13. Kopie typu snapshot muszą być wykonywane w taki sposób by nie było konieczności rezerwacji miejsca dla zmieniających się danych.
14. Macierz musi posiadać funkcjonalność LUN masking, LUN mapping
15. Macierz musi posiadać możliwość udostępniania wolumenów o większej pojemności niż aktualnie zaalokowana dla tego wolumenu. Funkcjonalność musi być oferowana dla całej pojemności macierzy.
16. Macierz musi posiadać możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy tymi samymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach. Z macierzą dostarczone muszą być licencje na replikacje danych między macierzami w Centrum Głównym a Zapasowym.
17. Replikacja pomiędzy macierzami musi zapewniać realizację planu Disaster Recovery, tzn. w przypadku całkowitego uszkodzenia jednej macierzy, jest możliwość uruchomienia zasobów na drugiej macierzy w sposób zautomatyzowany z zapewnieniem integracji z natywnymi mechanizmami dostarczanego oprogramowania wirtualizującego.
18. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej
19. Macierz musi mieć możliwość wykonania migracji wolumenów logicznych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach.
20. Macierz musi posiadać narzędzia do monitorowania i planowania wydajności oraz pojemności macierzy. Przechowywane historii wydajności musi być wykonywane mechanizmami macierzy.
21. Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych macierzach dyskowych, w szczególności pochodzących od HP, IBM, Oracle, Fujitsu, EMC i HDS. Wirtualizacja rozumiana jako możliwość udostepnienia zasobów innych macierzy poprzez kontrolery dostarczanej macierzy dla produkcyjnych środowisk. Funkcjonalność nie jest wymagana na etapie dostawy urządzenia
22. Macierz musi zapewniać techniczną możliwość montażu w szafie 19 cali oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie.
23. Macierz musi posiadać możliwość zabezpieczenia danych znajdujących się w pamięci cache w przypadku awarii zasilania na min. 3 dni
24. Macierz musi pozwalać na wymianę w trakcie pracy następujących elementów: dysków, kontrolerów, zasilaczy.
25. Macierz musi posiadać oprogramowanie do zarządzania zarówno przez interfejs graficzny GUI oraz tekstowy CLI. Możliwość zarządzania zdalnego macierzą przez tzw. „command line” z wykorzystaniem protokołu SSH.
26. Z macierzą musi zostać dostarczone oprogramowanie zarządzające wielościeżkowością połączeń MPIO dla wszystkich podłączanych do macierzy serwerów.
27. Gwarancja producenta z możliwościa bezpośredniego składania zgłoszeń w trybie 24x7, oraz trybie naprawy 24h

#### 

#### Konfiguracja oprogramowania:

1. Na każdym węźle klastra należy uruchomić, przy użyciu systemu wyboru systemów operacyjnych dostarczony system operacyjny
2. instalacja OS powinna zawierać wszystkie pakiety (opcja instalacyjna „FULL”),
3. partycjonowanie domyślne, bez partycji HOME,
4. zamontować dysk /home z zewnętrznej zasobu dyskowego,
5. konfiguracja sieci – pobieranie adresów i nazw z serwerów odbywać się będzie z serwerów DHCP i DNS zgodnie z opisem poniżej,
6. konfiguracja kont – zgodna z polityką bezpieczeństwa w Instytucie,
7. obraz powinien posiadać zainstalowane konieczne biblioteki np. BLAS
8. w zależności od dostarczonego systemu kolejkowego obraz powinien posiadać zainstalowanego klienta tego systemu, np. pakiet pbs-client dla PBS Pro,
9. obsługa sieci, w tym środowisko MPI, powinna być wbudowane w OS i nie wymagać dalszej konfiguracji lub obraz będący w bibliotece powinien posiadać skonfigurowaną tą funkcjonalność,
10. konfiguracja usług – włączone powinny być jedynie następujące usługi: acpid, aksusbd, autofs, cpuspeed, ip6tables, ipoib, iptables, irqbalance, jexec, lvm2-monitor, mdmonitor, messagebus, netfs, network, nfslock, nscd, ntpd, nullmailer, openibd, pbs, rawdevices, rpcgssd, rpcidmapd, rsyslog, smartd, sshd oraz pozostałe wymagane przez użytkowników:
11. wszystkie usługi sieciowe dotyczące klastra powinny otwierać porty jedynie na interfejsie Ethernet wewnętrznym,
12. usługi iptables i ip6tables – konfiguracja pusta (brak firewall),
13. usługa ntpd skonfigurowana do korzystania z lokalnego serwera czasu,
14. usługa nullmailer skonfigurowana do korzystania z lokalnego serwera poczty,
15. usługa pbs (lub innego systemu kolejkowego) – wskazany adres węzła głównego klastra jako serwera systemu kolejkowego,
16. usługa sshd – zgodna z polityką bezpieczeństwa w Instytucie, włączona minimum obsługa HostBased,
17. usługa rsyslog – skonfigurowane wysyłanie wszystkich logów na węzeł główny i oraz jednoczesne składowanie lokalne,
18. pozostałe usługi – konfiguracja domyślna jest prawidłowa i wystarczająca,
19. Interfejs Ethernet wewnętrzny klastra:
    1. metoda przyznawania adresu interfejsu i adresu bramy zgodna z konfiguracją sieci
    2. MTU 1500,
    3. hostname nadawane według schematu: wn${NUMER}, gdzie NUMER jest zgodny z 4-tym oktetem adresu IP z zerami wiodącymi (01, 02, …, 12),
20. Interfejs Ethernet dla zarządzania IPMI:
    1. metoda przyznawania adresu interfejsu i adresu bramy zgodna z konfiguracją sieci Zamawiającego
    2. MTU 1500,
    3. użytkownik domyślny, hasło nadane przez administratora zgodnie z polityką bezpieczeństwa Zamawiającego,
    4. hostname taki sam jak na interfejsach wewnętrznych,
21. Interfejs Ethernet dla dostępu do głowicy NAS:
    1. metoda przyznawania adresu interfejsu i adresu bramy zgodna z konfiguracją sieci Zamawiającego
    2. MTU minimum 8192 w zależności od możliwości karty i sterownika,
    3. hostname taki sam jak na interfejsach wewnętrznych, ale z przyrostkiem „f”,
22. Interfejs 10GbE:
    1. konfiguracja narzucona statycznie na podstawie adresu interfejsu wewnętrznego
    2. zalecana klasa adresowa nierutowalna,
    3. hostname taki sam jak na interfejsach wewnętrznych, ale z przyrostkiem „i”,

Dyski lokalne – każdy węzeł jest bezdyskowy, posiada podłączenie do zasobu dyskowego poprzez sieć FC.

Wymagane jest załączenie do oferty schematu topologii połączeń elementów klastra z wykazaniem przepustowości poszczególnych połączeń

**ELEMENT 7**

**System poczty elektronicznej**

Przedmiotem zamówienia jest zakup oraz wdrożenie centralnego systemu poczty elektronicznej. System poczty elektronicznej będzie miał za zadanie obsługę poczty firmowej, zarówno dla użytkowników znajdujących sie w biurze (podłączonych do sieci lokalnej), jak i w trybie pracy zdalnej dla użytkowników znajdujących sie poza biurem (podłączonych zdalnie). Dostęp zdalny będzie możliwy w trybie web poprzez aplikacje www, oraz w standardowym trybie pracy klient-serwer. Projektowany system będzie w pełni redundantny, co oznacza, iż awaria któregokolwiek centrum danych nie wpłynie na funkcjonowanie serwisu poczty elektronicznej. System będzie zapewniać kodowaną komunikację, przez co zapewniona zostanie poufność wiadomości e-mail. Autenentykacja użytkowników pocztowych będzie odbywać się w oparciu o Active Directory. System pocztowy będzie dodatkowo wyposażony w zintegrowany kalendarz, współdzielony pomiędzy pracowników firmy, zadania oraz foldery publiczne.

System poczty będzie składał się z następujących bloków funkcjonalnych:

1. serwerów pocztowych obsugującego pocztę w obrębie przedsiębiorstwa, serwery te będą odbierały i wysyłały wiadomości e-mail od użytkowników wewnątrz firmy
2. konektorów, umieszonego w dmz, które będą pośrednikiem pomiędzy światem zewnętrznym a serwerem, które będą obsługiwać pocztę przychodzącą z poza przedsiębiorstwa.
3. system pocztowy będzie integrował się z usługą katalogową active directory, dzięki czemu zaimplementowana zostanie zcentralizowana metoda uwierzytelniania klientów poczty
4. system pocztowy będzie połączony z storage SAN, na którym przechowywane będą wiadomości użytkowników

Poniżej przedstawiono krótką charakterystykę modułów systemu pocztowego:

* **Mailbox Server** przechowuje skrzynki pocztowe użytkowników składowane w bazach danych, które mogą być replikowane w ramach Database Availability Group (DAG)
* **Client Access** pośredniczy w ruchu od klienta wewnętrznego (poza MAPI/RPC) jako OWA (Outlook Web Access), ActiveSync, Outlook Anywhere (RPC over HTTPS) lub internetowego (SMTP) do serwera Mailbox przechowującego jego skrzynkę pocztową.
* **Edge Transport** jest umieszczany poza wewnętrzną siecią i zapewnia na tym obszarze zintegrowane zabezpieczenie poczty e–mail, usługi antywirusowe i antyspamowe dla Exchange.
* **Unified Messaging** pozwala na integrację z centralą PBX (Private Branch Exchange, centrala prywatna połączona z miejską siecią telefoniczną), aby umożliwić przesyłanie poczty głosowej i faksów do skrzynek pocztowych serwera Exchange, a także funkcje głosowego (telefonicznego) łączenia się z Exchange Server i odbierania poczty, gdy np. dostęp do internetu nie jest możliwy.

W każdej z dwóch lokalizacji założono wykorzystanie ról: Mailbox, , Client Access w konfiguracji wysokiej dostępności. Dwa serwery pełniące role Client Access, i Mailbox, umieszczone odpowiednio jeden w centrum podstawowym i jeden w centrum zapasowym. Funkcje Gateway oraz ochronę poczty zapewni urządzenie OE opisane w pkt Ochrona poczty.

## Opis konfiguracji docelowej

Dzięki utworzeniu redundantnego systemu pocztowego uszkodzenie serwera, systemu operacyjnego i oprogramowania na jednej z maszyn nie powoduje przerwy w działaniu poczty., Client Access, Mailbox w celu redundancji są postawione na redundantnych serwerach. Serwery smarthost bronią dostępu do systemu poczty pracując w DMZ i filtrując wiadomości.

W ramach klastra dla roli Mailbox wykorzystana zostanie funkcjonalność Exchange 2013 czyli Database Availability Group (DAG). Na serwerach przechowywane są bazy pocztowe użytkowników. W DAG serwery Exchange replikują asynchronicznie pliki dzienników po TCP/IP a dodatkowo wspierają szyfrowanie. Dzięki temu w każdej chwili np. w przypadku uszkodzenia serwera podstawowego można przełączyć na serwer pasywny. Oczywiście można równoważyć obciążenie po obu serwerach. W przypadku wykorzystania DAG potrzebna jest podwójna przestrzeń dyskowa.

Użytkownicy wykorzystujący MS Outlook (od wersji 2003) mogą posiadać skonfigurowany tryb buforowany optymalizujący pasmo i umożliwiający pracę w trybie offline. Dodatkowo dla użytkowników wewnętrznych i zewnętrznych skonfigurowany może zostać dostęp Outlook Anywhere (RPC over HTTPS) oraz OWA (Outlook Web Access) i dla urządzeń mobilnych ActiveSync. Użytkownicy komunikują się bezpośrednio lub pośrednio (proxy) do serwerów Client Access. Dostęp do skrzynek pocztowych powinien być realizowany również za pomocą dowolnego klienta pocztowego. Dostęp do skrzynek pocztowych dla pracowników będących poza siecią lokalną Zamawiającego powinien odbywać się na zasadzie dwustopniowego uwierzytelniania.

## Opis obecnego systemu pocztowego

System pocztowy aktualnie działa na platformie Opensource. Aplikacja pocztowa działa na wirtualnym serwerze, opartym o Hyper-V. Konta użytkowników pocztowych przechowywane są w lokalnej bazie LDAP. Każde z nich posiada swój katalog domowy. Średni rozmiar konta każdego użytkownika dla przechowywanej poczty ograniczony był pojemnością dysków fizycznego serwera. Każdy użytkownik ma stworzone konto, do którego ma przywiązany alias *imie.nazwisko(at)ilot...* Oprócz tego stworzone są aliasy, czyli adresy mailowe, do których przywiązane są konkretne skrzynki. Liczba kont pocztowych, oprócz aliasów, wynosi ok. 400 sztuk. W większości przypadków poczta ściągana jest lokalnie na dysk użytkownika przez odpowiednio skonfigurowany program pocztowy. Zapewniony jest również dostęp przez przeglądarkę internetową.

## Wymagania szczegółowe dla infrastruktury pocztowej

### Licencje systemu

Przedmiotem zamówienia jest:

* zakup licencji serwera MS Exchange Server 2013 w wersji Standard wraz z licencjami dostępowymi lub oprogramowania równoważnego
* zakup licencji Windows Server Standard 2012 lub oprogramowania równoważnego,
* instalacja w/w systemów na dostarczanych serwerach,
* wdrożenie - w tym: konfiguracja, migracja istniejących rozwiązań, danych przechowywanych obecnie na serwerze poczty Zamawiającego
* zapewnienie wsparcie dla wdrożonego rozwiązania w określonym dla zamówienia terminie 5 lat od daty odbioru końcowego przedmiotu zamówienia:
* dostępność poprawek oraz aktualizacji do nowych wersji dla dostarczanego oprogramowania w okresie obowiązywania umowy
* wsparcie producenta oprogramowania na wszystkich poziomach w okresie obowiązywania umowy. Musi istnieć możliwość konfiguracji personalnego konta na stronach producenta umożliwiającego przesyłanie zgłoszeń serwisowych
* wykonanie innych, niewykazanych w opisie przedmiotu zamówienia czynności niezbędnych dla osiągnięcia zakładanej funkcjonalności systemu

1. **Exchange Server Standard 2013 – 2szt. lub równoważny; za równoważne rozumie się system pocztowy, który posiada następujące cechy:**
   1. Obsługa poczty elektronicznej, załączników;
   2. Zarządzanie kalendarzem, tworzenie zaproszeń, współdzielenie kalendarzy;
   3. Tworzenie i zarządzanie zadaniami, delegacja zadań;
   4. Tworzenie i zarządzanie kontaktami i grupami kontaktów;
   5. Korzystanie z dostępu do systemu z urządzeń przenośnych;
   6. System musi zapewniać uwierzytelnienie zewnętrznym certyfikatem wykorzystywanym w ramach istniejącej infrastruktury Zamawiającego
   7. Skrzynki współdzielone dla stron SharePoint (posiadane przez Zamawiającego);
   8. Współdzielenie kalendarzy pomiędzy sfederowanymi (poprzez AD) organizacjami;
   9. Możliwość rozbudowy do integracji usług Poczty głosowej – możliwość nagrywania przez system przychodzącej poczty głosowej i dostarczenie w postaci mp3 oraz transkrypcji tekstowej;
   10. Możliwość dostępu do klienta poczty przy pomocy przeglądarki internetowej (np. usługa OWA) w trybie tym pełna funkcjonalność aplikacji (np. wymiana plików poprzez Drag and drop);
   11. Pełna integracja kont pocztowych z domenowymi (posiadana przez Zamawiającego domena AD);
   12. Licencja przenoszalna, nieograniczona czasowo i terytorialnie.
2. **Exchange Standard CAL 2013 – 500 szt. lub równoważny tzn.:**

Rozszerzenie powyższego systemu pocztowego, który zgodnie z licencją pozwala na korzystanie pięciuset użytkownikom Zamawiającego; licencja typu *per user* nielimitowana czasowo i terytorialnie.

1. **System Windows Server Standard 2013 w wersji standard 2 szt. lub równoważny**

Zgodny z oferowanym oprogramowaniem pocztowym

1. **Wymagania w zakresie licencji**

Zamawiający wymaga dostarczenia licencji spełniających poniższe kryteria:

* 1. Bezterminowa licencja na użytkowanie zamawianego oprogramowania dla produktów, w przypadku których powstanie wymaganie dostawy licencji;
  2. Dostarczenie kompletu kluczy aktywacyjnych dla produktów w przypadku których powstanie wymaganie dostawy kluczy aktywacyjnych;
  3. Dostarczenie dokumentów pozwalających na stwierdzenie legalności dostarczonych licencji i oprogramowania dla celów inwentaryzacyjnych i audytowych.
  4. Dostarczenie kompletu nośników umożliwiających zainstalowanie wyspecjalizowanego oprogramowania opisanego w punktach 1, 2 i 3.

1. **Instalacja ww. oprogramowania będzie realizowana w sposób następujący:**

Wykonanie projektu technicznego zawierający co najmniej opis wszystkich wymaganych procedur niezbędnych do instalacji i uruchomienia zaoferowanego rozwiązania oraz migracji poczty, szczegółową analizę środowiska informatycznego Zamawiającego, analizę wymagań funkcjonalnych i biznesowych Zamawiającego, o których mowa powyżej wraz z koncepcją implementacji tych wymagań, harmonogram wdrożenia, opracowanie założeń dla uruchomienia wysokiej dostępności (rozwiązania wysokiej dostępności -High Availability – HA- mają zapewnić ciągły dostęp do krytycznych aplikacji i danych. Rozwiązania HA uniezależniają funkcjonowanie systemu od tzw. pojedynczego punktu awarii. Oznacza to, że w przypadku systemów redundantnych awaria dowolnego elementu systemu nie spowoduje utraty jego funkcjonalności.) i zabezpieczeń przed awarią. Wykonawca jest zobowiązany w terminie 2 tygodni od dnia podpisania umowy przedłożyć Zamawiającemu projekt techniczny do akceptacji.

Przeszkolenie dla dwóch administratorów Zamawiającego z wdrożonego systemu pocztowego, w ilości min. 40h/osobę.

Migracja obecnego środowiska pocztowego m.in skrzynek użytkowników, folderów, kalendarzy do nowo tworzonego systemu pocztowego. W trakcie procesu migracji musi być zapewniony pełny dostęp do poczty dla użytkowników w zakresie godzin pracy instytutu Zamawiającego.

1. **Równoważność przedmiotu zamówienia**

Zamawiający uzna, że uruchomienie zaoferowanego rozwiązania posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z wyposażeniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia.

W przypadku zaproponowania usługi równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia, w tym zgodność posiadanego wyposażenia z zaproponowanym rozwiązaniem.

Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia Wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego.

1. **Przestrzeń dyskowa dla systemu poczty**

Wymagana jest rozbudowa obecnie posiadanych macierzy dyskowych IBM V7000 Unified o półkę dyskową w związku z koniecznością zapewnienia przestrzeni na potrzeby systemu pocztowego.

Wymagana jest rozbudowa macierzy w każdym z centrów (podstawowym i zapasowym) o przestrzeń min. 21,6TB RAW, na której będą składowane skrzynki pocztowe użytkowników, oraz repozytoria usług systemu pocztowego.

Wymagania dla pojedyńczej macierzy:

1. rozbudowa posiadanej przez Zamawiającego macierzy IBM V7000 Unified o min jedną półkę dyskową z co najmniej 24 dyskami
2. Dyski o pojemności maksymalnie 900GB i predkości obrotowej min. 10 000 rpm
3. redundante zasilanie
4. Redundantne pętle SAS do podłączenia do kontrolera
5. Komplet okablowania wymaganego do podłącznia pólki do kontrolera
6. Gwarancja producenta 5 lat z gwarantowanym czasem naprawy 24h

Zamawiający dopuszcza zastosowanie rozwiązania równoważnego w postaci nowej macierzy, przy czym oferowane rozwiązanie musi spełniać poniższe warunki równoważności:

Centrum podstawowe

1. Macierze muszą posiadać pojemność surową co najmniej 89,6 TB
2. Przestrzeń musi być zbudowana w oparciu o dyski SSD (co najmniej 2szt.)

o pojemności nie mniejszej niż 200GB, o dyski SAS/FC 10K (co najmniej 46szt.)

o pojemności 900GB oraz dyski NL-SAS (co najmniej 12szt.) o pojemności 4TB.

Centrum zapasowe

1. Macierze muszą posiadać pojemność surową co najmniej 69,6 TB
2. Przestrzeń musi być zbudowana w oparciu o dyski SAS/FC 10K (co najmniej 24szt.) o pojemności 900GB oraz dyski NL-SAS (co najmniej 12szt.) o pojemności 4TB.

Wymagania wspólne dla centrum podstawowego oraz centrum zapasowego

1. Macierz musi umożliwiać rozbudowę do co najmniej 240 dysków (w konfiguracji dysków 2,5”) oraz do co najmniej 480 dysków (w konfiguracji dysków 2,5”) poprzez mechanizm klastrowania lub dodawania par kontrolerów.
2. Macierz musi posiadać pamięć cache co najmniej 16GB, po 8GB na kontroler z możliwością rozbudowy łącznie do 64GB. Rozbudowa możliwa poprzez mechanizm klastrowania lub dodawania par kontrolerów.
3. Macierz musi zabezpieczać dyski mechanizmami RAID 0, 1, 5, 6, 10.
4. Macierz musi posiadać funkcjonalność automatycznie odbudowywania danych z uszkodzonego dysku na wolnej przestrzeni SPARE.
5. Półki dyskowe muszą być podłączone do każdego z kontrolerów przez min. 2 redundantne połączenia FC lub SAS.
6. Min. 2 redundantne kontrolery macierzowe.
7. Wszystkie kontrolery muszą pracować w trybie active-active.
8. Oferowana konfiguracja musi zawierać mechanizm nie powodujący wyłączenia cache do zapisu w przypadku awarii kontrolera, przy zapewnieniu redundancji pamięci write-cache.
9. Każdy kontroler musi być wyposażony w minimum 4 porty FC 8Gbit, 2 porty Ethernet 1Gbit oraz 2 porty 10GbE.
10. Macierz musi posiadać możliwość wykonywania kopii danych typu klon mechanizmami macierzy (licencja na wykonywanie kopii pełnych musi być zawarta w oferowanej cenie macierzy)
11. Macierz musi posiadać możliwość wykonywania kopii danych typu snapshot mechanizmami macierzy. Minimalna liczba kopii nie może być mniejsza niż 100, w tym możliwość wykonywania kopii z kopii oraz promowania migawki do trybu RW
12. Kopie typu snapshot muszą być wykonywane w taki sposób by nie było konieczności rezerwacji miejsca dla zmieniających się danych.
13. Macierz musi posiadać funkcjonalność LUN masking, LUN mapping
14. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej
15. Macierz musi posiadać możliwość udostępniania wolumenów o większej pojemności niż aktualnie zaalokowana dla tego wolumenu. Funkcjonalność musi być oferowana dla całej pojemności macierzy.
16. Macierz musi posiadać możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy tymi samymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach. Z macierzą dostarczone muszą być licencje na replikacje danych między macierzami w Centrum Głównym a Zapasowym.
17. Replikacja pomiędzy macierzami musi zapewniać realizację planu Disaster Recovery, tzn. w przypadku całkowitego uszkodzenia jednej macierzy, jest możliwość uruchomienia zasobów na drugiej macierzy w sposób zautomatyzowany z zapewnieniem integracji z natywnymi mechanizmami dostarczanego oprogramowania wirtualizującego.
18. Macierz musi mieć możliwość wykonania migracji wolumenów logicznych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach.
19. Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych macierzach dyskowych, w szczególności pochodzących od HP, IBM, Oracle, Fujitsu, EMC i HDS. Wirtualizacja rozumiana jako możliwość udostepnienia zasobów innych macierzy poprzez kontrolery dostarczanej macierzy dla produkcyjnych środowisk. Funkcjonalność nie jest wymagana na etapie dostawy urządzenia
20. Macierz musi posiadać narzędzia do monitorowania i planowania wydajności oraz pojemności macierzy. Przechowywane historii wydajności musi być wykonywane mechanizmami macierzy.
21. Macierz musi zapewniać techniczną możliwość montażu w szafie 19 cali oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie.
22. Macierz musi posiadać możliwość zabezpieczenia danych znajdujących się w pamięci cache w przypadku awarii zasilania na min. 3 dni
23. Macierz musi pozwalać na wymianę w trakcie pracy następujących elementów: dysków, kontrolerów, zasilaczy.
24. Macierz musi posiadać oprogramowanie do zarządzania zarówno przez interfejs graficzny GUI oraz tekstowy CLI. Możliwość zarządzania zdalnego macierzą przez tzw. „command line” z wykorzystaniem protokołu SSH.
25. Z macierzą musi zostać dostarczone oprogramowanie zarządzające wielościeżkowością połączeń MPIO dla wszystkich podłączanych do macierzy serwerów.
26. Macierz musi posiadać dwa redundantne moduły udostępniające przestrzeń dyskową z wykorzystaniem protokołu SMB i NFS.
27. Moduł musi posiadać co najmniej 2 porty 1GbE, 2 porty 10GbE, 2 porty 8Gb FC.
28. Moduły muszą zapewniać dostęp do danych z wykorzystaniem protokołu SMB i NFS.
29. Moduły muszą posiadać możliwość integracji z Active Directory.
30. Rozwiązanie macierzy i modułów musi pochodzić od jednego producenta i być oferowane w ramach jednej rodziny produktowej.
31. Moduły muszą posiadać redundantne zasilacze.
32. Moduły muszą zapewniać techniczną możliwość montażu w szafie 19” oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie.

### Serwery na potrzeby systemu pocztowego

Wymagana jest dostawa 2 szt. serwerów rozmieszczonych po jednym w centrum podstawowym oraz zapasowym. Serwery zostaną podłączone do sieci LAN oraz SAN Zamawiającego.

Wymagania:

1. Serwer musi posiadać obudowę typu RACK.
2. Serwer musi posiadać dwa dziesięciordzeniowe procesory taktowane zegarem co najmniej 2,3 GHz. Serwer musi posiadać co najmniej 32GB pamięci RAM min. 2133 MHz oraz możliwość instalacji do co najmniej 768 GB pamięci.
3. Oferowane procesory muszą osiągać wynik 832 w teście SPECint\_rate\_base2006 w konfiguracji dwuprocesorowej. Wynik musi być opublikowany na stronie [www.spec.org](http://www.spec.org/) na moment złożenia oferty
4. Serwer musi posiadać co najmniej 4 dyski o pojemności co najmniej 300GB i prędkości obrotowej 15000 rpm z możliwością rozbudowy do 16 dysków.
5. Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1, 5, 10 z pamięcią 1GB cache podtrzymywanego bateryjnie lub flash-backed
6. Serwer musi posiadać co najmniej 3 sloty PCI-E 2.0 x16 (elektrycznie), oraz 3 sloty PCI-E 2.0 x8 (elektrycznie)
7. Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód, tył), oraz 2 wewnętrzne porty SD lub USB
8. Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000, 2 porty 10Gb Ethernet na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.
9. Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym
10. Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0
11. Serwer musi posiadać minimum dwa porty FC 8Gb/s.
12. Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 750W
13. Serwer musi posiadać kartę VGA
14. Serwer musi posiadać wysokość maksymalnie 2U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi
15. Wsparcie dla oferowanego oprogramowania systemowego.
16. Gwarancja producenta 5 lat z gwarantowanym czasem naprawy 24h

**ELEMENT 8**

**Szafa Rack**

Wymagana jest dostawa 1 szt. szafy Rack spełniającej poniższe minimalne wymagania:

1. Wysokość zestawu: 2200 [mm]
2. Głębokość zestawu: 1000 [mm]
3. Szerokość zestawu: 800 [mm]
4. Dostępna przestrzeń dla montażu infrastruktury IT w standardzie rack 19 cali: 42 U
5. Współpraca z podniesioną podłogą techniczną
6. 2 sztuki PDU dla każdego stelażu rack 19 cali
7. PDU trójfazowe pionowe, zamontowane z tyłu stelażu nie zasłaniające torów wentylacyjnych sprzętu, o wysokości całkowitej dedykowanej do montażu w szafie 42U.
8. Rozdział mocy PDU na 6 sekcji jednofazowych zabezpieczonych wkładkami 16A w klasie C
9. Kontrolki obecności napięcia dla każdej sekcji PDU z możliwością niezależnego wyłączenia każdej sekcji
10. 24 sztuki gniazd CEE7/5, heavy duty, 16A dla każdego PDU
11. Dopuszczalna moc dla zainstalowanej infrastruktury IT: min. 6 [kW] dla pojedynczego stelażu rack.