**Pakiet nr 1: Firewall**

### 1.Dostawa systemu firewall

Zamawiający posiada w swojej infrastrukturze aktywnie działające urządzenie Barracuda CloudGen Firewall F280 o numerze seryjnym 1154645 z aktywnymi serwisami: EnergizeUpdates, Instant Replacement, MalwareProtection, Advanced ThreatProtection.

W celu uruchomienia klastra wysokiej dostępności należy dostarczyć subskrypcje na okres 36-miesięcy dla budowanego klastra w skład którego będzie wchodzić nowo dostarczone urządzenie oraz posiadane urządzenie Barracuda CloudGen Firewall F280 o numerze seryjnym 1154645. Okres wygaśnięcia subskrypcji dla posiadanego urządzenia musi pokrywać się z terminem wygaśnięcia subskrypcji na nowo dostarczonym urządzeniu.

W celu prawidłowego zarządzania regułami bezpieczeństwa i planowania typu licencji potrzebnych do obsługi systemu ochrony aplikacyjnej wymagany jest system cyklicznego raportowania pracujący w cyklu godzinnym, dobowym, tygodniowym i miesięcznym na obecnie posiadanym urządzeniu Barracuda CloudGen Firewall F280 o numerze seryjnym 1154645:

* Raport o najczęstszych atakach pod względem kategorii ataku
* Raport o klientach wykonujących największą liczbę ataków
* Najczęściej atakowane aplikacje i adresy URL
* Kraje pochodzenia największej liczby ataków
* Liczba zapytań aplikacyjnych w funkcji czasu
* Liczba połączeń do aplikacji w funkcji czasu
* Wykorzystywana przepustowość w funkcji czasu
* Podsumowanie wykorzystywanej przepustowości
* 36-miesięcznasubskrypcja

W ramach postępowania należy dostarczyć i wdrożyć nowe urządzenia typu Zapora Sieciowa Nowej Generacji (NGFW) , kompatybilne z posiadanym przez Zamawiającego urządzeniem, które wymuszać będą przyjętą/wdrożoną politykę bezpieczeństwa. NGFW musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall’a, systemu ochrony IPS oraz usług sieciowych takich jak np. DHCP.

Oferowany w ramach postępowania sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce.

Zapora sieciowa musi spełniać następujące kryteria:

#### Parametry zapora sieciowa (Firewall), typ 1

a) Urządzenie musi posiadać dysk SSD o pojemności nie mniejszej niż 100 GB.

b) Urządzenie w formie fizycznego urządzenia posiadającego:

- przynajmniej 12 portów 1000Base-T RJ45,

- przynajmniej 4 portów 1GbE SFP,

- przynajmniej 2 porty USB.

c) Wysokość urządzenia nie może przekroczyć 1U.

e) Przepustowość firewalla: min. 4,8 Gb/s.

f) Wydajność firewalla (włączona kontrola IPS): min. 2.0 Gb/s.

g) Wydajność z włączonymi modułami ochrony IPS, Application Control, URL Filtering i Anti-Virus: min. 1.6 Gbps w warunkach produkcyjnych (pakiety i sesje charakterystyczne dla ruchu do Internetu).

h) Przepustowość SD-WAN throughput przy szyfrowaniu AES-128: min. 1.5 Gbps.

i) Obsługa sieci logicznych min. 256 VLAN

j) Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 12 000 nowych sesji/sekundę.

k) Rozwiązanie musi mieć możliwość rozbudowy do działania w układzie klastra niezwodnościowego HA w trybie Active/Pasive.

#### Parametry zapora sieciowa (Firewall), typ 2

a) Urządzenie musi posiadać dysk SSD o pojemności nie mniejszej niż 100 GB.

b) Urządzenie w formie fizycznego urządzenia posiadającego:

- przynajmniej 12 portów 1000Base-T RJ45,

- przynajmniej 4 portów 1GbE SFP,

- przynajmniej 2 porty USB.

c) Wysokość urządzenia nie może przekroczyć 1U.

e) Przepustowość firewalla: min. 3.2 Gb/s.

f) Wydajność firewalla (włączona kontrola IPS): min. 1.0 Gb/s.

g) Wydajność z włączonymi modułami ochrony IPS, Application Control, URL Filtering i Anti-Virus: min. 1.2 Gbps w warunkach produkcyjnych (pakiety i sesje charakterystyczne dla ruchu do Internetu).

h) Przepustowość SD-WAN throughput przy szyfrowaniu AES-128: min. 800 Mb/s.

i) Obsługa sieci logicznych min. 256 VLAN

j) Liczba równoczesnych sesji - min. 150 000 i nie mniej niż 12 000 nowych sesji/sekundę.

#### Minimalne wymagania dla oferowanych urządzeń – Firewalli typ 1 i typ 2

a) Urządzenie musi umożliwiać inspekcję stanową (full-stateInspection) opartą na granularnej analizie komunikacji sieciowej oraz rozpoznawaniu i analizie warstwy aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu.

b) Urządzenie ma obsługiwać translacje adresów NAT typu: n:1, NAT1:1; PAT; Network MAP/NAT.

c) Urządzenie musi posiadać możliwość ustawienia trybu pracy jako router/brama warstwy trzeciej, jako bridge warstwy drugiej (Transparent mode) oraz w trybie analizatora ruch TAP monitor port.

d) Graficzny Interface(GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Administrator musi mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, serwisy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

e) Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola Quality Of Service, godziny oraz dnia obwiązywania (aktywności) reguły.

f) Administrator ma możliwość zdefiniowania minimum sześciu (niezależnie konfigurowalnych) typów reguł/polityk na firewall’u.

g) Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, pozwalający na sprawdzanie jaka reguła będzie stosowana dla danego typu ruchu i eliminujący sprzeczności w konfiguracji reguł

h) Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, zewnętrzny serwer LDAP; Microsoft Active Directory z możliwością wdrożenia strategii autoryzacji wieloskładnikowej (Multi-Factor-Authentication MFA)

l) Urządzenie powinno wspierać tworzenie tuneli VPN za pomocą graficznego interfejsu w modelu Drag&Drop bez potrzeby użycia narzędzi konsolowych (commandline).

m) Urządzenie musi zapewniać możliwość integracji z platformą zarządzania firewallami, pracującymi w strukturze geograficznie rozproszonej w wielu lokalizacjach jednocześnie. Platforma zarządzania, o której mowa, musi być tego samego producenta, co dostarczone urządzenia firewall i współpracować z posiadanym przez Zamawiającego urządzeniem.

n) Urządzenie musi posiadać dedykowany port konsoli ze złączem RS232 lub RJ45

o) Wyposażenie w elementy umożliwiające montaż urządzenia w 19” szafie stelażowej.

r) Poszczególne użyte do budowy zestawu komponenty sprzętowe nie mogą w żaden sposób ograniczać maksymalnej przepustowości i prędkości pracy zestawu.

#### IntrusionPrevention System (IPS)

a) Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.

b) Moduł IPS musi posiadać bazę „na urządzeniu” co najmniej 10 000 sygnatur które są utrzymane i aktualizowane przez producenta.

c) Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

d) Moduł IPS powinien wykrywać oraz blokować szkodliwą zawartość w kodzie HTML oraz Javascript.

e) Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POPS oraz SMTPS.

f) Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie.

g) Moduł skanujący musi działać na urządzeniu (firewall’u). Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.

h) Urządzenie w ramach działania modułu IPS musi posiadać możliwość powiadamiania o wykrytych podatnościach w ruchu wraz z informacją o kodzie CVE.

i) Administrator musi mieć możliwość konfiguracji jednego z trybów pracy modułu proaktywnej ochrony i inspekcji pakietów IPS w zakresie: tryb aktywny IPS, tryb passywnyIDS; musi być możliwość konfiguracji baza wyjątkówmodułu IPS dla wybranych adresów IP (źródłowych i docelowych), portów docelowych; sygnatur bazy CVE.

#### Kształtowanie pasma (TrafficShapping)

a) Urządzenie musi pozwalać na kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

b) Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia z uwzględnieniem kierunku przesyłanych danych (upload / download). KwalfikacjaTrafficShapping z uwzględnienim adresu IP(źródłowego i docelowego), portów docelowych; autoryzowanego użytkownika

c) Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

d) Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

e) TrafficShapping powinien działać w oparciu o profile QoS Band tzw. klasyfikatory ruchu które będą kolejkowane do fizycznych lub logicznych interfejsów firewall’a

#### Ochrona antywirusowa

a) Rozwiązanie ma umożliwiać inspekcję przez skaner antywirusowy, co najmniej jeden silnik antywirusowy powinien być dostarczony przez firmę inną niż producent rozwiązania

b) Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

c) Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. Proponowany system powinien umożliwiać wysyłanie powiadomienia email o załączniku, który został zablokowany.

####  8. Wirtualne sieci prywatne (VPN)

a) Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) isite-to-site (lokalizacja-lokalizacja).

b) Odpowiednio kanały VPN można budować w oparciu o:

- PPTP VPN,

- L2TP VPN

- IPSec VPN,

- SSL VPN

c) SSL VPN musi działać w trybach Tunel i Portal.

d) Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

f) Urządzenie ma posiadać wsparcie dla technologii XAuth oraz Hub ‘n’ Spoke.

g) Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię RouteBased.

h) Urządzenie musi być dostarczone wraz z dedykowanym klientem IPSec VPN.

i) Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.

j) Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych.

k) Rozwiązanie ma zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN.

l) Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora.

#### Filtr dostępu do stron WWW (URL filtering)

a) Urządzenie musi posiadać wbudowany filtr URL.

b) Filtr URL ma działać w oparciu o klasyfikację URL zawierającą kategorie tematyczne stron internetowych; wymagana ilość rozpoznawanych kategorii 86.

c) Urządzenie powinno wspierać mechanizmy białych i czarnych list

d) Urządzenie nie może posiadać ograniczenia w postaci limitu ilości białych i czarnych list definiowanych przez administratora

e) Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.

f) Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:

- ·blokowanie dostępu do adresu URL,

- ·zezwolenie na dostęp do adresu URL,

- ·blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

g) Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.

h) Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.

i) Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

j) Urządzenie musi dawać możliwość utworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. Baza wyjątków tworzona co najmniej przy użyciu dwóch metod: a. wskazanie/wpisanie docelowej domeny (np. \*.skype.com; \*.microsoft.com) ; b. wskazanie kategorii ruch (np. Bankowość i Finanse)

k) Urządzenie musi umożliwiać włączenia pamięci cache dla ruchu http.

l) Urządzenie musi wbudowany i rekonfigurowany WEB portal powiadomień zwrotnych służący do informowania użytkowników o nałożonych restrykcjach/ograniczeniach wynikających z wdrożonej polityki bezpieczeństwa (np. zablokowanie strony WWW danego portalu z powodu niedozwolonej kategorii)

#### Uwierzytelnianie

a) Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:

- lokalną bazę użytkowników,

- zewnętrzną bazę użytkowników (zewnętrzny LDAP),

- usługę katalogową Active Directory.

b) Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.

c) Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:

- SSL,

- Radius,

- Kerberos.

d) Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.

e) Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

#### Administracja łączami do Internetu (ISP)

a) Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing).

b) Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

- równoważenie względem adresu źródłowego,

- równoważenie względem połączenia.

c) Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

d) Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

e) Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.

f) Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

g) Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

h) Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

i) Rozwiązanie powinno wspierać technologię Link Aggregation.

#### Pozostałe usługi i funkcje rozwiązania

a) Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.

b) Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.

c) Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.

d) Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci z możliwością określenia różnych bram, a także serwerów DNS

e) Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.

f) Urządzenie musi posiadać usługę DNS Proxy.

#### Administracja urządzeniem

a) Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.

b) Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w zakresie konfiguracji podstawowej i zaawansowanej.

c) Urządzenie posiada możliwość eksportu informacji przez syslog. Wysyłanie logów powinno być możliwe do wielu serwerów, równocześnie.

d) Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogicznynp.protokołu IPFIX

e) Komunikacja z interfejsem zarządzania może odbywać się na porcie innym niż https (443 TCP).

f) Urządzenie powinno umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

g) Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.

h) Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową lub poprzez dedykowaną aplikację do zarządzania a komunikacja musi być zabezpieczona (autoryzacja i szyfrowanie ruchu).

i) Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.

j) Urządzenie musi pozwalać na odtworzenie backupu konfiguracji w sposób:

- bezpośrednio z centralnej konsoli zarządzania;

- przywrócenie konfiguracji z lokalnego graficznego interfejsu zarządzania GUI

- przywrócenie konfiguracji z lokalnego tekstowego interfejsu zarządzania (console port)

- przywrócenie konfiguracji ze zdalnego trybu tekstowego zarządzania (SSH)

- przywrócenie systemu operacyjnego i konfiguracji z użyciem klucza USB-Stick

k) Zapory sieciowe muszą być wyposażone w aplikację lub system umożliwiający zdalne zarządzanie firewallem, serwerem VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej przynajmniej pod kontrolą systemu Windows lub Linux.

#### Raportowanie

Dostarczony system zapór sieciowych musi posiadać minimalne parametry raportowania:

1. Dostępne widoki
* Pulpit nawigacyjny SD-WAN
* Pulpit nawigacyjny stanu tunelu SD-WAN
* Pulpit nawigacyjny bezpieczeństwa i ruchu sieciowego
1. Ogólne typy raportów:
* Raporty konfigurowalne
* Raporty na żądanie
* Raporty zaplanowane
* Raporty administracyjne
* Raporty zaawansowane
* Predefiniowane raporty produktywności
* Predefiniowane raporty aktywności internetowej
* Predefiniowane raporty bezpieczeństwa i odpowiedzialności
* Predefiniowane raporty aktywności sieciowej
* Predefiniowane raporty zagrożeń i bezpieczeństwa
* Predefiniowane raporty aktywności infekcji - Predefiniowane raporty ruchu

Raporty muszą być dostarczone w postaci plików: PDF, HTML,CSV,Text.

Raporty muszą mieć możliwość dostarczenia przez: serwer zewnętrzny (FTP lub SMB), Email, przeglądarkę internetową.

Raporty wyświetlać minimum następujące parametry:

* Pulpit nawigacyjny oferowanych zapór sieciowych oraz zapory sieciowej posiadanej przez Zamawiającego: przegląd dozwolonych i zablokowanych sesji wraz z wyjaśnieniem; przegląd zagrożeń według użytkownika, źródła i miejsca docelowego; aktywność w sieci i wydajność: kategorie, użytkownicy i domeny, do których uzyskano dostęp według liczby żądań, przepustowości i czasu przeglądania
* Raporty zbiorcze: bezpieczeństwo i odpowiedzialność; aktywność sieciowa; podsumowanie zagrożeń; podsumowanie ruchu w sieci; całkowite wykorzystanie
* Raporty dotyczące bezpieczeństwa i odpowiedzialności (na podstawie użytkownika i żądań): ruch do witryn z oceną dla dorosłych; strony anonimizujące; wymiana plików i P2P; nietolerancja i hate; oprogramowanie szpiegowskie; przemoc i terroryzm; na podstawie użytkownika i żądań
* Raporty dotyczące bezpieczeństwa według podtypu (na podstawie użytkownika, czasu, źródłowego IP): ATP; IPS; wirus; malware; spyware; zablokowana zawartość plików
* Raporty aktywności internetowej: dostępne kategorie; czas przeglądania; domeny; użytkownicy; agenci użytkownika w oparciu o porę dnia, sesje, żądania pasma, źródło i użytkownika
* Raporty produktywności dotyczące żądań, przepustowości i czasu przeglądania m. in. dla: Facebook, gaming, streaming, użytkownicy YouTube według żądań, przepustowości i czasu przeglądania

#### Instalacja

p) Dostarczenie kompletu kabli kat 7A oraz OM4, wszystkich wkładek SFP, które mogą pochodzić od producenta innego niż producent zaaferowanych urządzeń. Wkładki SFP muszą być w pełni kompatybilne z zaoferowanymi urządzeniami oraz posiadać co najmniej roczną gwarancję producenta.

q) Uruchomienie zestawu w tym szczególnie instalacja i pełna konfiguracja firewalli według ustaleń projektowych zaakceptowanych przez Zamawiającego. Wymagany jest podstawowy i zaawansowany zakres konfiguracji.

#### Licencje

Wszystkie dostarczone licencje w ramach rozwiązania muszą obejmować wymagany okres 36-miesięcy i nie mogą posiadać limitu użytkowników.

Wraz z urządzeniem wykonawca dostarczy wymagane do prawidłowej pracy licencje:

- 36-miesięczna subskrypcja na aktualizację: systemu operacyjnego; aktualizację sygnatur dla silnika IPS, aktualizację sygnatur dla silnika dynamicznego rozpoznawania aplikacji.

- 36-miesięczna subskrypcja na ochronę antywirusową; aktualizacje sygnatur spamu oraz dostęp do serwerów RBL DNS.

- 36-miesięczna subskrypcja na poszerzoną ochronę Advanced ThreatProtection (Sanboxing) w zakresie zawansowanej analizy załączników i ochrona przed zagrożeniami dnia zerowego; ochrona przed atakami typu ransomware.

- 36-miesięczna subskrypcja, na rozszerzone funkcje raportowania w zakresie pulpitu nawigacyjnego, konfigurowalnych raportów w fomatach PDF, HTML, CSV i Text z możliwością dostarczenia przez zewnętrzny serwer, email lub przeglądarkę internetową.

#### Gwarancja i wsparcie techniczne producenta

Minimum 36-miesięcznagwarancja producenta obejmująca wszystkie elementy urządzenia zapewniająca w przypadku awarii wysłanie sprawnego sprzętu na wymianę na następny dzień roboczy od momentu zgłoszenia do serwisu producenta. Wymagany poziom serwisu SLA 8x5xNBD

Gwarancja musi zapewniać również dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00 (e-mail; telefon)

Po upływie co najwyżej 4 lat Zamawiający musi posiadać możliwość nieodpłatnej wymiany sprzętu na fabrycznie nowe urządzenie w aktualnej (na moment wymiany) wersji sprzętowej w ramach tej samej serii/linii produktowej.

#### Dodatkowe wymagania wdrożeniowo-instalacyjne

Wykonawca zobowiązuje się do wykonania uruchomienia zestawu(ów) kierując się zasadą utrzymania ciągłości dotychczas dostępnych usług u Zamawiającego. Dopuszcza się możliwość odejścia od tej zasady z zastrzeżeniem każdorazowego uzgadniania z Zamawiającym.

SYSTEM OCHRONY APLIKACYJNEJ – WYMAGANIA MINIMALNE

W ramach postępowania należy dostarczyć system ochrony aplikacji internetowych składający się z modułów ochrony aplikacji WWW (aplikacji używającej protokołu HTTP/HTTPS) i systemu zarządzania ochroną.

Ochrona aplikacji i system zarządzania i konfiguracji powinny być dostarczone w formie usługi SaaS.

Moduły ochrony aplikacji powinny realizować funkcje ochronne na trzech poziomach:

1. Poziom transakcji HTTP/HTTPS: ataki na elementy transakcji takie jak adresy URL, nazwy parametrów, wartości parametrów, nazwy nagłówków i wartości nagłówków, metody HTTP i transmitowane dane.
2. Poziom nawigacji: śledzenie i filtrowanie aktywności użytkowników w czasie ich pracy z aplikacją, weryfikacja aktywności (np. kody CAPTCHA)
3. Poziom ochrony logiki aplikacji: filtrowanie botów, identyfikacja przeglądarek, śledzenie ryzyka związanego z pracą osób i automatów

**Funkcjonalność Polityki Ochrony Aplikacyjnej**

Wymuszanie ograniczeń związanych z żądaniami HTTP:

* maksymalna limity żądań
* maksymalna długość pól URL, Query
* maksymalne wielkości związanych z obiektami typu *cookie*: liczba obiektów, długość nazwy obiektu *cookie*, długość wartości obiektu *cookie*
* maksymalne wielkości związane z nagłówkami *s*): nazwa nagówka, wartość nagłówka

Ochrona adresu URL w transakcji HTTP:

* maksymalna wielkość transakcji wykonywanej za pomocą metody POST
* maksymalna liczba parametrów i wczytywanych do aplikacji plików
* ochrona przed atakiem *Cross Site RequestForgery* w obszarze pola URL
* blokada adresów URL zawierających znak tyldy („~”) lub sekwencję znaków *slash-dot* („/.”)
* wykrywanieiblokowanieataków z zakresu OWASP Top 10, conajmniej: SQL Injection, OS Injection, LDAP Injection, HTTP Injection, ataki Python-PHP, *Cross-Site Scripting*, *Remote File Inclusion*
* budowa listy dozwolonych metod HTTP (GET, POST i innych)
* budowa listy dozwolonych formatów danych (na przykład *text/xml*, *application/json*etc)
* system normalizacji zawartości pola URL: wymuszenie standardowego zestawu znaków (np. UTF-8), filtracja wartości pola URL zakodowanych dwupoziomowo (*double decoding*), wymuszenie jednolitych separatorów parametrów w polu URL (np. tylko znak „&”).
* szyfrowanie pola URL
* budowa reguł URL pozwalających na ominięcie systemu bezpieczeństwa, czasowe lub stałe przekierowanie do innego adresu URL, blokowanie dostępu do URL z blokadą adresu IP klienta, blokowanie dostępu do URL z wyświetleniem klientowi wyzwania CAPTCHA

Ochrona nagłówków transakcji HTTP:

* blokowanie wskazanych metaznaków w nagłówkach(np. blokowanie „% $ @ !” )
* blokowanie wartości nagłówka dłuższych niż dopuszczalne maksimum
* wykrywanieiblokowanieataków z zakresu OWASP Top 10, co najmniej: SQL Injection, OS Injection, LDAP Injection, HTTP Injection, ataki Python-PHP, Cross-Site Scripting, Remote File Inclusion, Directory Traversal

Reguły pozwalające na modyfikacje pól URL i nagłówków w przychodzących żądaniach HTTP:

* Rewrite URL
* Redirect URL
* Rewrite header
* Remove header
* Insert header

Ochrona parametrów transakcji:

* wykrywanie ataków w nazwach parametrów
* wykrywanie ataków w wartościach parametrów
* blokowanie wskazanych meta-znaków takich jak %, $, @, !
* dekodowanie wartości w formacie Base64
* wykrywanie i blokowanie ataków z zakresu OWASP Top 10, co najmniej: SQL Injection, OS Injection, LDAP Injection, HTTP Injection, ataki Python-PHP, Cross-Site Scriptiog, Remote File Inclusion
* blokada wczytywania plików i selektywne wczytywanie plików o wskazanych rozszerzeniach lub typach MIME
* możliwość budowy listy wyjątków związanych ze wskazanymi parametrami

Ochrona obiektów typu cookie

* możliwość szyfrowania obiektów cookie (ochrona przed odczytem i modyfikacją)
* możliwość podpisywania cyfrowego obiektów typu cookie (zezwolenie na odczyt, ochrona przed modyfikacją)
* blokowanie nierozpoznanych obiektów cookie
* możliwość blokowania obiektów cookie starszych niż wskazana liczba minut
* ochrona przed próbami przechwytywania i powtórnego użycia obiektów cookie ze zmienionym adresem IP (*Client IP Cookie Replay*) lub zmienionymi wartościami nagłówków *(HTTP Header Cookie Replay*)
* możliwość budowy listy wyjątków związanych ze wskazanymi obiektami cookie

Możliwość budowy listy hostów zaufanych:

* ruch generowany przez hosty zaufane jest zawsze uznawany za legalny

Możliwość budowy reguł blokujących lub zezwalających na ruch IP:

* ze wskazanego kraju (geolokalizacja)
* z adresów o złej reputacji (blacklista)
* z systemów anonimizacji ruchu
* z sieci TOR
* możliwość budowy listy wyjątków od reguł blokujących na poziomie adresów IP

System buforowania zawartości i kompresji zawartości z regułami budowanymi w oparciu o rozszerzenia plików i/lub typów zawartości

Ochrona przed aplikacyjnymi atakami DoS/DdoS: ataki *slow-and-low*, *web scraping*, *bruteforce*

Moduł ochrony ruchu typu REST API w standardzie JSON

Obsługa HTTP2

Obsługa WebSockets

System ochrony aplikacyjnej powinien umożliwiać selektywne włączenie i wyłączenie obsługiwanych wersji i opcji szyfrowania SSL:

* SSL 3.0 (protokół uznawany za niebezpieczny, dostępny ze względu na testowanie kompatybilności)
* TLS 1.0 (protokół uznawany za niebezpieczny, dostępny ze względu na testowanie kompatybilności)
* TLS 1.1
* TLS 1.2
* TLS 1.3
* opcja Perfect Forward Secrecy

Moduł Data Protection pozwalający blokować dane lub częściowo zamazywać dane płynące z aplikacji do klienta (np. maskowanie środkowych cyfr numeru karty kredytowej wysyłanego przez serwer do przeglądarki klienta korzystającego z aplikacji)

**Funkcjonalność Zarządzania:**

System ochrony aplikacyjnej powinien zawierać podsystem automatycznego generowania certyfikatu publicznego dla zdefiniowanych w nim aplikacji

System ochrony aplikacyjnej powinien umożliwiać import własnego publicznego lub prywatnego certyfikatu HTTPS

System ochrony aplikacyjnej powinien umożliwiać zdefiniowanie strony wyświetlanej użytkownikom, których ruch został zablokowany

System ochrony aplikacyjnej musi obsługiwać co najmniej dwa tryby pracy:

* tryb monitorowania: informacje o wykrytych zagrożeniach są logowane ale ruch nie jest blokowany
* tryb blokujący: zagrożenia są logowane i ruch jest blokowany
* przełączenie między trybami pracy musi być pojedynczą operacją, wykonywaną globalnie dla wszystkich modułów i funkcji ochrony jednocześnie, dostępną na poziomie każdej zdefiniowanej aplikacji

Budowa polityki na podstawie skanowania podatności:

* Możliwość cyklicznego skanowania chronionej aplikacji pod kątem podatności za pomocą skanera podatności aplikacyjnych
* Automatyczna modyfikacja polityki bezpieczeństwa na podstawie wyników skanowania w celu zablokowania wykrytych podatności

Możliwość eksportu logów bezpieczeństwa z systemu ochrony aplikacyjnej do serwerów syslog

System zarządzania powinien pozwalać na definiowanie dodatkowych administratorów, których prawa dostępu do konfiguracji są kontrolowane przez role, w ramach ról wymagane są co najmniej następujące uprawnienia:

* administrator z prawem zarządzania kontami innych administratorów, z prawem pełnej lub częściowej konfiguracji reguł bezpieczeństwa związanych z aplikacją, prawem monitorowania i kontroli logów
* administrator częściowy, bez prawa zarządzania kontami innych użytkowników
* użytkownik systemu ochrony aplikacyjnej z dostępem tylko do odczytu (read-only)
* system zarządzania powinien pozwalać tworzyć nowe role o granularnie przyznawanych uprawnieniach do aplikacji i do funkcji konfiguracyjnych

System zarządzania powinien gromadzić logi operacji administracyjnych i konfiguracyjnych wykonanych przez administratorów na aplikacjach (*audit log*); musi istnieć możliwość eksportu logów w postaci tabelarycznej (np. w formacie CSV).

**Raportowanie**

W celu prawidłowego zarządzania regułami bezpieczeństwa i planowania typu licencji potrzebnych do obsługi systemu ochrony aplikacyjnej wymagany jest system cyklicznego raportowania pracujący w cyklu godzinnym, dobowym, tygodniowym i miesięcznym:

* Raport o najczęstszych atakach pod względem kategorii ataku
* Raport o klientach wykonujących największą liczbę ataków
* Najczęściej atakowane aplikacje i adresy URL
* Kraje pochodzenia największej liczby ataków
* Liczba zapytań aplikacyjnych w funkcji czasu
* Liczba połączeń do aplikacji w funkcji czasu
* Wykorzystywana przepustowość w funkcji czasu
* Podsumowanie wykorzystywanej przepustowości

System ochrony aplikacyjnej musi być dostarczony na okres 24-miesięcy

Dostawca zobowiązany jest do wdrożenia systemu ochrony aplikacyjnej w sieci Zamawiającego, tak, aby wskazane przez Zamawiającego aplikacje były aktywnie chronione. Harmonogram prac i szczegółowy zakres zostanie uzgodniony z wykonawcą na etapie wdrożenia.

**Pakiet nr 2 - LTO**

| **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Potwierdzenie spełnienia parametru, podać:****TAK/NIE** |
| --- | --- | --- |
| Wykorzystana technologia | LTO-8 Ultrium wspierające technologię partycjonowania nośników. Urządzenie musi mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO szóstej, siódmej i dziewiątej generacji |  |
| Wbudowane napędy | Dwa napędy LTO-8 wyposażone w złącze z interfejsem FC 8GB. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO z interfejsem dual SAS 6Gb oraz wspierać technologię LTFS (LinearTape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu LTO-8 bez kompresji – minimum 300 MB/sek. Zainstalowane napędy powinny mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speedmatching) w przedziale od 100 do 300 MB/sek. oraz stosować szyfrowanie danych metodą AES 256-bit |  |
| Ilość slotów i magazynki | Minimum 24 kieszenie na taśmy (urządzenie musi być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka. |  |
| Pojemność | Pojemność bez kompresji – minimum 288TB |  |
| Obudowa | Typu rack 19”. Wszystkie elementy do montażu winny być dostarczone wraz z urządzeniem, wysokość maksymalnie 2U |  |
| Zarządzanie | Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.  |  |
| Dodatkowe interfejsy | Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI |  |
| Obsługa urządzenia | Wymagana możliwość wymiany napędów, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napędy jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.  |  |
| Partycjonowanie | Wymagane stworzenie 2 logicznych partycji – jeżeli do tej operacji konieczna jest dodatkowa licencja, należy ją dostarczyć wraz z urządzeniem |  |
| Wyposażenie | Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli koniecznych do podłączenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabli min. 2m. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 12,0 TB każdy w ilości odpowiadającej ilości wszystkich dostępnych slotów na nośniki w dostarczonym urządzeniu plus 1 wraz z nośnikiem czyszczącymi, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia – wszystkie nośniki muszą być wyposażone w naklejki z kodami kreskowymi. Instrukcja instalacji - w języku polskim lub angielskim |  |
| Gwarancja i oświadczenia | 36 miesięcy w miejscu instalacji urządzenia z czasem reakcji na zgłoszenia do 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim.Pisemne oświadczenia wystawione przez producenta:- o gwarancji świadczonej w miejscu instalacji urządzenia w rygorze 24x7x4 realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy. W oświadczeniu wymagane jest podanie wszystkich danych kontaktowych z serwisem (mail, telefon, adres) oraz potwierdzenie wykupienia przez wykonawcę wymienionych usług serwisowych u producenta.- że oferowane urządzenie jest zgodne z zapisami specyfikacji technicznej przetargu oraz zgodne z europejskimi normami dotyczącymi CE i WEEE – oświadczenie musi być podpisane i wystawione nie wcześniej niż 1 miesiąc przed ogłoszeniem postępowania przetargowego Wymaga się, aby wdrożenie i konfigurację urządzenia przeprowadziła osoba posiadająca certyfikat techniczny producenta urządzenia wystawiony w roku wdrożenia systemu  |  |

**serwer Backup**

| **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Potwierdzenie spełnienia parametru, podać:****TAK/NIE** |
| --- | --- | --- |
| Obudowa | * Typu RACK, wysokość nie więcej niż 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Opcjonalne ramię porządkujące ułożenie przewodów z tyłu serwera;
* Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;
* Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
* Zainstalowane 2 szt. dysków SSD SATA 960GB Hot-Plug;
* Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray;
* Możliwość zainstalowania wewnętrznego napędu LTO;
 |  |
| Płyta główna | * Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera
* Możliwość instalacji procesorów 38-rdzeniowych;
* Zainstalowany moduł TPM 2.0;
* 7 złącz PCI Express generacji 4 w tym:
	+ 4 fizyczne złącza o prędkości x16;
	+ 3 fizyczne złącza o prędkości x8;
	+ Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	+ Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 4TB pamięci RAM DDR4;
* Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna
* Wsparcie dla technologii:
	+ Memory Scrubbing
	+ SDDC
	+ ECC
	+ Memory Mirroring
	+ ADDDC;
* Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
 |  |
| Procesory | * Jeden procesor 12-rdzeniowy
* Taktowanie 2,1GHz
* architektura x86\_64

osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 189 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/cpu2017.html> |  |
| Pamięć RAM | * 64 GB pamięci RAM
* DDR4 Registered
* 3200Mhz
 |  |
| Kontrolery LAN | * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
* Dodatkowa karta LAN 4x 10Gbit SFP+;
 |  |
| Kontrolery I/O | * Zainstalowane dwie karty FC 16G dwuportowe
 |  |
| Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 port USB 3.0 wewnętrzne;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
* 2 porty USB 3.0 na panelu przednim
 |  |
| Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W;
* Redundantne wentylatory hotplug;
 |  |
| Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
	+ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
		- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
		- procesory CPU
		- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
		- wbudowany na płycie głównej nośnik pamięci M.2 SSD
		- status karty zrządzającej serwera
		- wentylatory
		- bateria podtrzymująca ustawienia BIOS płyty główne
		- zasilacze

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera;
	+ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	+ Dostęp poprzez przeglądarkę Web, SSH;
	+ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	+ Zarządzanie alarmami (zdarzenia poprzez SNMP)
	+ Możliwość przejęcia konsoli tekstowej
	+ Możliwość zarządzania przez 6 administratorów jednocześnie
	+ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
	+ Obsługa serwerów proxy (autentykacja)
	+ Obsługa VLAN
	+ Możliwość konfiguracji parametru Max. Transmission Unit (MTU)
	+ Wsparcie dla protokołu SSDP
	+ Obsługa protokołów TLS 1.2, SSL v3
	+ Obsługa protokołu LDAP
	+ Integracja z HP SIM
	+ Synchronizacja czasu poprzez protokół NTP
	+ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
* BIOS UEFI w specyfikacji 2.7;
 |  |
| Wspierane OS | * Microsoft Windows Server 2022, 2019, 2016
* VMWare vSphere 6.7, 7.0
* Suse Linux Enterprise Server 15
* Red Hat Enterprise Linux 7.9, 8.3
* Hyper-V Server 2016, 2019
 |  |
| Gwarancja | * 36 miesięcy gwarancji producenta serwera w trybie on-site. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
 |  |
| Dokumentacja, inne | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
* Zgodność z normami: CB, RoHS, WEEE, GS oraz CE;
 |  |
| System operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. * 1. Zdalna dystrybucja oprogramowania na stacje robocze.
	2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. * 1. Szyfrowanie plików i folderów.
	2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	4. Serwis udostępniania stron WWW.
	5. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	6. Wsparcie dla algorytmów Suite B (RFC 4869),
	7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, Obsługi ramek typu jumbo frames dla maszyn wirtualnych. Obsługi 4-KB sektorów dysków Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunkmode) 1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
 |  |

 **Serwery NAS typ I**

| **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Potwierdzenie spełnienia parametru, podać:****TAK/NIE**  |
| --- | --- | --- |
| Procesor | Min. 1.7, GHz 4 rdzeniowy |  |
| Zainstalowana pamięć | 4 GB SODIMM DDR4 |  |
| Pojemność maksymalna | Możliwość zainstalowania pamięci 16 GB |  |
| Slot pamięci | 1 x SODIMM DDR4 |  |
| Pamięć FLASH | Min. 512 MB ( zapewniona ochrona systemu operacyjnego przed podwójnych rozruchem) |  |
| Wnęki dyskowe | Wnęki na 8 dysków 3,5-calowych SATA 6 Gb/s |  |
| Kompatybilność dysków | 3,5-calowe wnęki:3,5-calowe dyski twarde SATA2,5-calowe dyski twarde SATA2,5-calowe dyski SSD SATA |  |
| HOT-SWAP (Wymieniany podczas pracy) | TAK |  |
| Porty | 2 x 2,5 Gigabit sieci Ethernet (2,5G/1G/100M)2 x 10GbE SFP+3 x Port USB 3.2 Gen 1 |  |
| Wskaźniki LED | Stan systemu, LAN, USB, HDD |  |
| Przyciski | Zasilanie, Reset, Kopiowanie USB |  |
| Zasilacz | Max. 250 W |  |
| Obudowa | Tower |  |
| Zainstalowane dyski | 6x10TB (dyski do pracy ciągłej przeznaczone do rozwiązań typu NAS) |  |
| Gwarancja | 3 lata na serwer NAS (gwarancja producenta serwera NAS)3 lata na zaoferowane dyski (gwarancja producenta dostarczonych dysków) |  |

**typ II**

| **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Potwierdzenie spełnienia parametru, podać:****TAK/NIE** |
| --- | --- | --- |
| Procesor | Min. 2.2 Ghz 4 rdzeniowy |  |
| Zainstalowana pamięć | 8 GB UDIMM DDR4 |  |
| Pojemność maksymalna | Możliwość zainstalowania 64 GB (2 x 32) |  |
| Slot pamięci | 2 x UDIMM DDR4 |  |
| Pamięć FLASH | 5GB MB ( zapewniona ochrona systemu operacyjnego przed podwójnych rozruchem) |  |
| Wnęki dyskowe | 12 x 3.5’ SATA 6Gb/s, 3Gb/s |  |
| Kompatybilność dysków | 3,5-calowe dyski twarde SATA2,5-calowe dyski twarde SATA2,5-calowe dyski SSD SATA |  |
| HOT-SWAP (Wymieniany podczas pracy) | TAK |  |
| Obsługa przyspieszenia pamięci podręcznej SSD | TAK |  |
| Wake on LAN | Port 2,5GbE |  |
| Porty | 2 x Port 2,5 Gigabit Ethernet (2,5G/1G/100M)Możliwość zainstalowania portu 5 Gigabit Ethernet (5G/2,5G/1G/100M)Możliwość zainstalowania portu 10 Gigabit sieci Ethernet2 x PCIe Gen3 x41 x Port USB 3.2 Gen 1 typ APort USB 3.2 Gen 2 (10 Gb/s) – w tym 2 x typ C, 1 x typ AUrządzenie musi być wyposażone w interfejs Fibre Channel 16/8/4 Gb/sFC (dopuszcza się zastosowanie karty na porcie PCIe) |  |
| Wskaźniki LED | HDD 1-12, stan, LAN, USB, zasilanie |  |
| Przyciski | Zasilanie, reset |  |
| Zasilacz | Max 300W |  |
| Obudowa | 2U, do montażu stelażowego |  |
| Montaż | Wymagane szyny montażowe |  |
| Zainstalowane dyski | 8x10TBZaoferowane dyski muszą znajdować się na liście kompatybilnych dysków opublikowanej przez producenta oferowanego urządzenia lub muszą być przez niego rekomendowane. |  |
| Gwarancja | 3 lata na serwer NAS (gwarancja producenta serwera NAS)3 lata na zaoferowane dyski (gwarancja producenta dostarczonych dysków) |  |

**Zasilacz UPS**

|  |  |  |
| --- | --- | --- |
| **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Potwierdzenie spełnienia parametru, podać:****TAK/NIE** |
| Moc znamionowa | 3000VA / 3000W |  |
| Obudowa | Układ Rack/Tower 2U lub Układ Rack/Tower 3U |  |
| Technologia | Line-Interactive o wysokiej częstotliwości (czysta sinusoida, booster + fader) |  |
| Zakres napięcia wejściowego bez użycia baterii | 160 V-294 V (regulowany do 150 V-294 V) |  |
| Zakres częstotliwości wejściowej bez użycia baterii | 47 do 70 Hz (system 50 Hz), 56,5 do 70 Hz (system 60 Hz), 40 Hz w trybie niskiej czułości |  |
| Napięcie wyjściowe | 230 V (+6/-10%) (regulowane do 200 V\* / 208 V / 220 V / 230 V / 240 V), 50/60 Hz +/- 0,1 Hz (autodetekcja) |  |
| Wejścia | IEC C20 (16A) |  |
| Wyjścia | 8 x IEC C13 (10A)2 x IEC C19 (16A) |  |
| Wyświetlacz | LCD zawierający informacje o stanie ipomiarach zasilacza UPS |  |
| Opcjonalne baterie zewnętrzne | Złącze modułu baterii zewnętrznejMożliwość dodania do 4 zewnętrznych modułów bateryjnychwymienialnych „na gorąco” |  |
| Zarządzanie bateriami | Automatyczny test baterii, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie zewnętrznych modułów baterii |  |
| Porty komunikacyjne | 1 port USB + 1 port szeregowy RS232 + 1 mini złącze dla zdalnego zał./wył. + 1 mini złącze dla zdalnego wył. + 1 mini złącze dla wyjściowego styku przekaźnikowego |  |
| Gniazdo komunikacyjne | Slot na kartę sieciową zarządzającą |  |
| Temperatura pracy | Od 0 do 40°C |  |
| Poziom hałasu | <40 dB przy standardowym obciążeniu |  |
| Baterie | Wymaga się aby dostarczone urządzenie było wyposażone w baterię (nie dopuszcza się dostawy urządzenia bez zainstalowanej baterii) |  |
| Gwarancja | 3 lata na elektronikę/urządzenie, 2 lata na baterie |  |

**Uwaga: Brak spełnienia minimalnego wymagania ( odpowiedz NIE) spowoduje odrzucenie oferty na podstawie art. 226 ust 1 pkt 5 ustawy Prawo zamówień publicznych**

 **Instalacja i wdrożenie:**

* Fizyczna instalacja serwera i LTO w szafie RACK wskazanej przez Zamawiającego.
* Połączenie i skonfigurowanie serwera oraz LTO ze sobą za pomocą sieci FC (wymagane okablowanie/wkładki FC dostarcza wykonawca)
* Połączenie i skonfigurowanie serwera za pomocą sieci FC z posiadaną infrastrukturą SAN Zamawiającego (wymagane okablowanie/wkładki FC dostarcza wykonawca).
* Połączenie i skonfigurowanie serwera za pomocą złącz SFP/SFP+ z posiadaną infrastrukturą LAN Zamawiającego (wymagane okablowanie/wkładki SFP/SFP+ dostarcza wykonawca).
* Fizyczna instalacja serwera NAS typ II w szafie RACK wskazanej przez Zamawiającego.
* Połączenie i skonfigurowanie serwera NAS typ II za pomocą sieci FC z posiadaną infrastrukturą SAN Zamawiającego (wymagane okablowanie/wkładki FC dostarcza wykonawca).
* Połączenie i skonfigurowanie serwera NAS typ II za pomocą złącz SFP/SFP+ z posiadaną infrastrukturą LAN Zamawiającego (wymagane okablowanie/wkładki SFP/SFP+ dostarcza wykonawca).
* Fizyczna instalacja serwera NAS typ I oraz UPS w lokalizacji wskazanej przez Zamawiającego.
* Połączenie i skonfigurowanie serwera NAS typ I za pomocą złącz SFP/SFP+ z posiadaną infrastrukturą LAN Zamawiającego (wymagane okablowanie/wkładki SFP/SFP+ dostarcza wykonawca).
* Migracja posiadanego oprogramowania do backupu Acronis Cyber Backup 15 Advanced na zainstalowany serwer.
* Migracja konfiguracji zasobów backapowych na nowy serwer.
* Konfiguracja polityk backupu według wytycznych Zamawiającego.
* Szkolnie administratorów z obsługi LTO oraz serwerów NAS.

Rekonfiguracja sieci SAN oraz LAN wymagane do prawidłowego działania systemu Backupu po migracji na nowy serwer leżą po stronie Wykonawcy.

**Pakiet nr 3 - Szkolenia**

Przeprowadzenie szkoleń z zakresu:

* Bezpieczeństwo miejsca pracy
* Bezpieczeństwo osobiste
* Bezpieczeństwo informacji
* Zagrożenia i ryzyka w IT
* Czynniki ryzyka zagrożenia
* Ataki socjotechniczne
* Czym jest phishing
* Czym jest spyware
* Czym jest sniffing
* Określenie potencjalnych zagrożeń
* Zapobieganie zagrożeniom
* Bezpieczeństwo danych
* Aktualność oprogramowania
* Jak zachować bezpieczeństwo

Szkolenie powinno odbyć się w przeciągu 2 dni w ramach dwóch grup dziennie – łącznie ok. 200 osób. Czas szkolenia jednej grupy to od 3 do 3.5 godziny.