**przetarg nieograniczony na dostawę sprzętu komputerowego dla Gminy Miasto Stargard w ramach Programu Operacyjnego Polska Cyfrowa**

**CZĘŚĆ I ZAMÓWIENIA - dostawa serwerów i firewalla dla Urzędu Miejskiego w Stargardzie**

# Opis przedmiotu zamówienia / specyfikacja techniczna – załącznik nr 7 SWZ

## Dostawa i wdrożenie sprzętu komputerowego wraz z oprogramowaniem

W ramach zadania wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie".
Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

a) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
b) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane
c) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
d) Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
e) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
f) Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
    i. połączenie urządzeń będzie zrealizowane w sposób nieograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
    ii. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
    iii. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
    iv. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
    v. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

# 1.Urządzenie typu Firewall – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.

- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

### Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

### Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 18 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

### Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 280 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 13 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.

### Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach zamówienia zostaną dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.

13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

## Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

## Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

## Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

## Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

### Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

### Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach zamówienia musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

### Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

### Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

### Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach zamówienia musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach zamówienia zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wymagania ogólne

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. **dokumenty dostarczane Zamawiającemu na etapie realizacji zamówienia**
2. **Wykonawca przedłoży oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań**.

# 2.System uwierzytelniania, autoryzacji i kontroli dostępu wraz z kluczami sprzętowymi -1 szt.

Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

Parametry systemu

Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę:

- 4 wirtualnych interfejsów sieciowych.
- Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI.

Parametry wydajnościowe i licencyjne

System musi obsługiwać co najmniej:

- Uwierzytelnianie dla 200 użytkowników.
- 400 tokenów dla uwierzytelniania dwuskładnikowego.
- 50 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu).
- Możliwość zdefiniowania co najmniej 20 grup użytkowników,
- 10 lokalnych centrów certyfikacji (CA).
- Możliwość wygenerowania 500 certyfikatów dla użytkowników.

Wymagania ogólne

System musi zapewniać nie mniej niż:

1. Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.
2. Graficzną reprezentację statusu uwierzytelnionych użytkowników.
3. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:

a. Lokalnie.

b. Zdalnie w oparciu o protokół Syslog.

4. Konfigurację Captive Portalu.

Wymagania funkcjonalne – uwierzytelnianie

Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:

1. Lokalną, wbudowaną bazę użytkowników.
2. Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo.
3. Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.
4. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV.
5. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:

a. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),

b. czasu ważności hasła,

6. Konfigurowalną politykę blokowania kont, która będzie uwzględniać:

a. ilość nieudanych logowań,

b. czas blokowania konta,

c. okres nieaktywności, po którym konto jest blokowane.

7. Możliwość odzyskiwania haseł:

a. z wykorzystaniem adresu email,

b. z wykorzystaniem pytania pomocniczego.

8. Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:

a. wbudowany serwer RADIUS,

b. integrację z zewnętrznymi serwerami RADIUS – praca jako klient.

9. Obsługę protokołu LDAP, w tym zakresie system musi oferować:

a. wbudowany serwer LDAP,

b. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).

10. Obsługę protokołu SAML - Identity Provider (IdP) proxy.
11. Realizację funkcji SSO (Single Sign On) w oparciu o:

a. integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,

b. dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,

c. kontekst użytkownika przesyłany z serwera RADIUS,

d. informacje uzyskiwane poprzez protokół Syslog,

Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe

Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:

1. Obsługę dla tokenów sprzętowych (hardware):

a. wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania.

2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
3. Dla tokenów na system iOS i Android wymaga się:

a. aktywacji z centralnego systemu uwierzytelniania (seed provisioning),
b. możliwości konfiguracji ilości generowanych cyfr (6 lub 8),
c. generowania kodu (cyfr) co 30 lub 60 sekund,
d. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
e. ochrony dostępu poprzez konfigurowalny kod PIN,

6. Możliwość integracji z logowaniem do systemu Windows.

Wymagania funkcjonalne – 802.1x

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

1. Obsługa co najmniej poniższych protokołów EAP:
a. PEAP,
b. EAP-TTLS,
c. EAP-TLS,
d. EAP-GTC.
2. Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).
3. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.

Wymagania funkcjonalne – zarządzanie certyfikatami

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

1. Obsługa wbudowanego CA (Certificate Authority).
2. Obsługa CA pośredniczących (Intermediate CA).
3. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego.
4. Możliwość pobrania wygenerowanych certyfikatów.
5. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP.
6. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.
7. Możliwość generowania certyfikatów typu wildcard.
8. Realizacja CRL (Certificate Revocation List).
9. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).
10. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Zarządzanie

1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki.
2. System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.
3. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu, kiedy proces ma się rozpocząć.
4. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Serwis, szkolenia i usługi

Wymaga się, aby dostawa obejmowała również serwis producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Tokeny Sprzętowe

Zamawiający wymaga **dostarczenia 200 kluczy sprzętowych** do uwierzytelniania. Klucz ma służyć do ochrony komputerów przed atakami phishingowymi.

Wymagania:

1. Wsparcie dla protokołów:
   - WebAuthn,
   - Yubico OTP,
   - OATH HOTP,
   - OATH TOTP,
   - U2F,
   - Smart Card (PIV),
   - OpenPGP,
   - FIDO2
2. Uwierzytelnianie za pomocą portu USB lub NFC
3. Zabezpieczenie wielu usług za pomocą jednego klucza
4. Uwierzytelnianie jedno-, dwu- i wieloskładnikowe
5. Wodoodporność oraz wstrząsoodporność
6. Nie wymaga baterii ani połączenia internetowego

Tokeny muszą współpracować z systemem zaproponowanym systemem uwierzytelniania.

# 3. System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania – 1 szt.

W ramach postepowania wymaganym jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.
Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

Parametry systemu ochrony dla stacji roboczych.

1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:
   - Kontrola antywirusowa.
   - Funkcja analizy plików w zewnętrznym systemie Sandbox.
   - Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.
   - URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
   - Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
   - Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
   - Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
   - Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
   - Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
   - Mechanizmy uwierzytelniania dwuskładnikowego
   - AntiExploit,
   - blokowanie dysków przenośnych typu USB,

2. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit),Windows Serwer 2019, Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.

3. Wymaganym jest, aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach zamówienia powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. **W ramach zamówienia dostarczone zostaną niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji**.

**Parametry systemu centralnego zarządzania.**

1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się, aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.

2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.

3. Ponadto wymagane jest aby system zapewniał:
   - integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,
   - definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,
   - zautomatyzowany proces zarządzania aplikacja kliencką,
   - przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.
   - możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,
   - panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,
   - panel, w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,
   - możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,
   - automatyczne wykrywanie stacji klienckich w grupach roboczych,
   - logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,
   - generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.
   - definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,
   - zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,
   - automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,
   - możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,
   - możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
   - możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.

4. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.

5. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach zamówienia koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

### Licencje oraz serwisy.

Wykonawca wraz z konsolą centralnego zarządzania dostarczy niezbędne licencje upoważniające do:

1. Zainstalowania i centralnego zarządzania 200 aplikacjami klienckimi na stacjach roboczych.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:
   a) Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, centralne zarządzanie na okres 24 miesięcy.

System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

## 4.Serwery wirtualizacyjne -3 sztuki

| Minimalne wymagania Techniczne | |
|---|---|
| Obudowa | • Typu RACK, wysokość nie więcej niż 1U;<br>• Szyny umożliwiające wysunięcie serwera z szafy stelażowej;<br>• Ramię porządkujące ułożenie przewodów z tyłu serwera;<br>• Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;<br>• Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;<br>• Zainstalowane 2 szt. dysków SSD SATA 240GB DWPD>3,5;<br>• Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. |
| Płyta główna | • Dwuprocesorowa;<br>• Wyprodukowana i zaprojektowana przez producenta serwera<br>• Możliwość instalacji procesorów 40-rdzeniowych;<br>• Możliwość zainstalowania modułu TPM 2.0;<br>• 4 złącz PCI Express generacji 4 w tym:<br>  ○ 3 fizyczne złącza o prędkości x16;<br>  ○ 1 fizyczne złącza o prędkości x8;<br>  ○ Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości;<br>• 32 gniazda pamięci RAM;<br>• Obsługa minimum 4TB pamięci RAM DDR4;<br>• Obsługa minimum 10TB pamięci (RAM DDR4 + pamięć nieulotna)<br>• Wsparcie dla technologii:<br>  ○ Memory Scrubbing<br>  ○ SDDC<br>  ○ ECC<br>  ○ Memory Mirroring<br>  ○ ADDDC;<br>• 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)<br>• 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 16-rdzeniowy |

| | |
|---|---|
| | • Taktowanie 2,4GHz<br>• architektura x86_64<br>osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 238 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta. |
| Pamięć RAM | • 512 GB pamięci RAM<br>• DDR4 Registered<br>• 3200Mhz |
| Kontrolery LAN | • Karta/y LAN, nie zajmujące żadnego z dostępnych slotów PCI Express, wyposażona/e minimum w 8 interfejsów sieciowych, w tym minimum 4x 10Gbit SFP+.<br>• Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; |
| Kontrolery I/O | • Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50 |
| Porty | • Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;<br>• 1 port USB 3.0 wewnętrzne;<br>• 2 porty USB 3.0 dostępne z tyłu serwera;<br>• 2 porty USB 3.0 na panelu przednim<br>• Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;<br>• 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; |
| Zasilanie, chłodzenie | • Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W;<br>• Redundantne wentylatory hotplug; |
| Zarządzanie | • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii<br>o informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:<br>▪ karty rozszerzeń zainstalowane w dowolnym slocie PCI Express<br>▪ procesory CPU<br>▪ pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM<br>▪ wbudowany na płycie głównej nośnik pamięci M.2 SSD<br>▪ status karty zrządzającej serwera<br>▪ wentylatory<br>▪ bateria podtrzymująca ustawienia BIOS płyty główne<br>▪ zasilacze<br>• system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym)<br>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:<br>• Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;<br>o 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;<br>o Dostęp poprzez przeglądarkę Web, SSH; |

| | |
|---|---|
| | ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;<br>○ Zarządzanie alarmami (zdarzenia poprzez SNMP)<br>○ Możliwość przejęcia konsoli tekstowej<br>○ Możliwość zarządzania przez 6 administratorów jednocześnie<br>○ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)<br>○ Obsługa serwerów proxy (autentykacja)<br>○ Obsługa VLAN<br>○ Możliwość konfiguracji parametru Max. Transmission Unit (MTU)<br>○ Wsparcie dla protokołu SSDP<br>○ Obsługa protokołów TLS 1.2, SSL v3<br>○ Obsługa protokołu LDAP<br>○ Integracja z HP SIM<br>○ Synchronizacja czasu poprzez protokół NTP<br>○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej<br>• 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);<br>• Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;<br>• Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;<br>• 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.<br>• BIOS UEFI w specyfikacji 2.7; |
| Wspierane OS | • Microsoft Windows Server 2022, 2019, 2016<br>• VMWare vSphere 6.7, 7.0<br>• Suse Linux Enterprise Server 15<br>• Red Hat Enterprise Linux 7.9, 8.3<br>• Hyper-V Server 2016, 2019 |
| Gwarancja | • 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.<br>• Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;<br>• Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;<br>• 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;<br>• 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; |

| | |
|---|---|
| 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;<br>• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;<br>• Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera. Wykonawca poda link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;<br>• 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;<br>• Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;<br>• Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;<br>• Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; |

# 5.Macierz dyskowa -1sztuka

| Lp. | Nazwa parametru | Minimalna wartość parametru |
|---|---|---|
| 1. | Obudowa | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. |
| 2. | Pojemność: | System musi zostać dostarczony w konfiguracji zawierającej minimum:<br><br>8 dysków 3800GB NVMe, (Nośniki SED – Self Encryption Drives)<br><br>System musi ponadto wspierać dyski:<br><br>- NVME: od 1900GB do 15TB<br>- SSD, NL-SAS oraz SAS 10k<br><br>System musi mieć możliwość rozbudowy do minimum 250TB przestrzeni RAW oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami) jeżeli istnieje model wyższy. Jeżeli nie istnieje model wyższy zamawiający wymaga dostarczenia macierzy z 256GB Cache.<br><br>Macierz musi mieć możliwość rozbudowy o dyski HDD tj. NL-SAS oraz SAS 10krpm oraz dyski flash łączone po 12Gb SAS (SSD). Obsługa dysków HDD może się odbywać poprzez dołożenie dodatkowej półki dyskowej, zarządzanie całą przestrzenią dyskową (NVMe oraz NL-SAS lub SAS) musi się odbywać przez te same dwa kontrolery macierzy. |
| 3. | Kontroler | Dwa kontrolery wyposażone w przynajmniej 16GB cache każdy.<br><br>W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. |
| 4. | Interfejsy | Oferowana macierz musi mieć minimum:<br><br>• 8 portów 10GbE z wkładkami SFP+ |

| | | |
|---|---|---|
| | | System musi pozwalać na wymianę ww. portów na porty:<br>• 100Gb NVMe over InfiniBand lub NVMe over RoCE<br>• 25GbE<br>System musi wspierać rozbudowę o porty SAS dla zewnętrznych półek dyskowych |
| 5. | RAID | Wsparcie dla RAID: 0, 1, 5, 6, 10<br>Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych w tym 15TB SSD.<br>Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w<br>sposób sprzętowy przez dedykowany układ w macierzy. |
| 6. | Obsługiwane protokoły | FC, iSCSI, NVMe Over FC, RoCE, Infiniband, CIFS, NFS, S3<br>Zamawiający dopuszcza zaoferowania rozwiązania, które realizuje CIFS, S3 i NFS za pomocą oprogramowania typu Software Define Storage. |
| 7. | Inne wymagania | Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:<br>Microsoft Windows Server, Red Hat Enterprise Linux, Novell SUSE Linux Enterprise Server, VMware ESX, Oracle Solaris, HP HP-UX, IBM AIX,<br>Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen.<br>Macierz musi posiadać funkcjonalność klonowania danych<br>Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie<br>Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji.<br>Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.<br>Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID<br>Z poziomu graficznego interfejsu do zarządzania istnieje możliwość sprawdzenia stanu zużycia dysków flash.<br>Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków<br>Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:<br>- wydajności i opóźnień na wolumenach<br>- wydajności I/Ops, MB/s<br>- trafności w cache |

| | | |
|---|---|---|
| | | Macierz musi docelowo pozwalać na osiągnięcie 600 000 IOps przy ruchu random dla bloku 8KB 100% odczytów.<br><br>Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem uwierzytelniania i dostępu dla użytkowników/administratorów.<br><br>Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:<br><br>- Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter<br>- VMware VASA<br>- Microsoft Virtual Disk Service (VDS)<br>- Microsoft Virtual Shadow Service (VSS)<br>- Oracle Enterprise Manager – monitoring zasobów macierzowych<br><br>Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.<br><br>Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. |
| 8. | Gwarancja i serwis | 3 lata serwisu producenta lub partnera serwisowego z 30 min czasem odpowiedzi na awarie krytyczne i dostawę elementów zastępczych na następny dzień roboczy od diagnozy problemu.<br><br>Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |

# 6.Serwerowy system operacyjny (SSO) – 3 sztuki

Dla każdego oferowanego serwera należy dostarczyć serwerowy system operacyjny (SSO) spełniający poniższe wymagania: (licencja dożywotnia nie może być ograniczona czasowo)
Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie nielimitowanej ilości 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:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d) 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:
    a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) 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:
    a) Login i hasło,
    b) Karty z certyfikatami (smartcard),
    c) 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:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) 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:
    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    iii. Obsługi 4-KB sektorów dysków
    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) 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.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

# 7.Oprogramowanie do wirtualizacji -1 sztuka

Licencja dla 3 serwerów fizycznych posiadających do 2 procesorów z gwarancją utrzymania aktualnej wersji przez okres min. 1 roku,

- Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
- Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć
- i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych
- z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.

- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
- Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X.
- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
- Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
- Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
- Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
- System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
- Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
- Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
- Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych.
- Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
- Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

# 8.Wdrożenie

### Firewall

a) Montaż urządzeń szafie rack

b) Nadanie adresu IP
c) Konfiguracja dostępu SSH
d) Zmiana haseł dostępu
e) Aktualizacja oprogramowania do najnowszej możliwej wersji
f) Stworzenie do 500 reguł bezpieczeństwa
g) Konfiguracja tuneli VPN (Site-to-Site i Client-to-Site), po stronie wykonawcy będzie instalacja odpowiednich klientów VPN na komputerach użytkowników
h) Konfiguracja routingu
i) Utworzenie polityk bezpieczeństwa
j) Wdrożenie funkcjonalności DPI
k) Wdrożenie deszyfracji protokołu SSL
l) Stworzenie klastra wysokiej dostępności
m) Przepisanie konfiguracji VLAN z obecnego rozwiązania Sonicwall
n) Konfiguracja firewall, reguły przychodzące i wychodzące na podstawie obecnie działających usług
o) Konfiguracja ochrony przed malware, exploitami oraz stronami zawierającymi złośliwy kod
p) Uruchomienie i konfiguracja systemu do zbierania logów z systemu firewall
q) Wdrożenie PKI oraz konfiguracja polityki za pomocą których przeprowadzona zostanie dystrybucja certyfikatów.
r) Rekonfiguracja wykorzystywanych przeglądarek www przez zamawiającego do pracy z włączoną deszyfracją protokołu SSL na firewall.
s) Transfer wiedzy do klienta na temat obsługi zaproponowanej konfiguracji

### Serwery z macierzą

a) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego
b) Podłączenie macierzy dyskowej i serwerów fizycznych z posiadaną przez Zamawiającego infrastrukturą teleinformatyczną z zachowaniem redundancji połączeń fizycznych obsługujących sieć LAN i SAN wraz z zapewnieniem dostępu do modułów konfiguracyjnych urządzeń za pomocą wydzielonej sieci zarządzania.
c) Konfiguracja:
    i. Konfiguracja dostarczonych serwerów, macierzy dyskowej i oprogramowania, w celu uruchomienia protokołu ISCSI (należy dostarczyć niezbędne moduły SFP+ oraz okablowanie)– wymagana jest pełna konfiguracja hypervisora oraz dostarczonych systemów operacyjnych i sprzętu. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość dla serwera i macierzy dyskowej z wykorzystaniem protokołu ISCSI. System musi działać w klastrze wysokiej dostępności.
    ii. Konfiguracja wirtualizacji
    iii. Środowisko oparte o 3 serwery fizyczne oraz współdzielony zasób macierzowy.
    iv. Konfiguracja klastra HA dla maszyn virtualnych na 3 maszynach fizycznych
    v. Automatyczne przenoszenie i uruchomienie maszyn virtualnych podczas awarii jednego z serwerów fizycznych na host nieuszkodzony.
    vi. Konfiguracja virtualnych switchy
d) Przeniesienie baz danych oraz kluczowych aplikacji Zamawiającego na nowy system operacyjny. Migracją objęty jest silnik bazy danych wraz z konfiguracją, jak również wszystkie bazy danych. Wykonawca przeprowadzi testy poprawności działania przeniesionego oprogramowania (baz danych), oraz wykonywania połączeń z zasobami sieciowymi, logowaniem i autoryzacją użytkowników, zasadami użytkowników, dostępem do sieci Internet, działaniem baz danych obsługiwanych przez serwery.
e) Przeniesienie wszystkich niezbędnych aplikacji z punktu widzenia Zamawiającego wraz z testami poprawności działania po migracji na nowy system operacyjny.
f) Migracja usług systemu operacyjnego:
    i. Migracja usługi kontrolera domeny Windows (wraz z przeniesieniem wszystkich ustawień, kont użytkowników i urządzeń przyłączonych do domeny itd.). Po migracji serwer obsługujący domenę (kontroler domeny)zachowa dotychczasowy adres IP.
    ii. Migracja usługi DHCP - wymagane przeniesienie pełnej dotychczasowej konfiguracji dotyczącej zakresów, zasad i zastrzeżeń, wraz z zachowaniem dotychczasowego adresu IP. Migracja nie może wpłynąć na pracę użytkowników końcowych i infrastruktury sieciowo-serwerowej.

iii. Migracja zasobów sieciowych protokołu SMB do nowego systemu operacyjnego wraz z zachowaniem dotychczasowych list ACL. Dodatkowo zamawiający wymaga konfiguracji i uruchomienia prywatnych folderów sieciowych dla użytkowników. Użytkownik powinien mieć dostęp do swojego zasobu ze stacji roboczej. Skonfigurowana lista dostępowa do zasobów powinna zawierać wyłącznie nieograniczony dostęp do prywatnych plików przez poszczególnych użytkowników i administratora domeny. Utworzenie i konfiguracja zasobów musi odbywać się automatycznie bez ingerencji Administratora Systemów Zamawiającego. Zasoby powinny być ograniczone do zapisu wyłączenie konkretnych rodzajów plików oraz posiadać ograniczenie co to wielkości zajmowanego miejsca na serwerze plików.

iv. Rozszerzenie grupy dyskowej na posiadanym przez Zamawiającego serwerze fizycznym o dodatkowe cztery dyski fizyczne. Konfiguracja systemu operacyjnego dla lokalnego zasobu musi wspierać magazynowanie dla oprogramowania kopii bezpieczeństwa. Serwer fizyczny (backupowy) w ramach zadania należy przenieść do innej lokalizacji wskazanej przez Zamawiającego, oraz przeprowadzić rekonfigurację w celu poprawnego działania.

g) Szkolenie min. 8h dotyczące replikacji serwerów wirtualnych w zakresie:

i. konfiguracji

ii. Obsługi

### Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

a) przeprowadzić testy poprawności działania całej infrastruktury

b) przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów

c) Ze względu na krytyczne aplikacje, które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embeded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
  - określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
  - wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
  - Badaniu będą podlegały następujące systemy:
    - ✓ rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
    - ✓ Linux 2.4.x, 2.6.x, 3.x.x;
    - ✓ IBM AIX;
    - ✓ CISCO IOS;
    - ✓ Microsoft SQL;
    - ✓ MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez dział informatyki Zamawiającego przed zakończeniem projektu.

# 9.Wymagania wykonawcy

Ze względu na zaawansowane wdrożenie dotyczące krytycznych aplikacji Zamawiającego, wymaga się, aby Wykonawca dysponował odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia tj. do wykazania, że dysponuje lub będzie dysponować co najmniej:

- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie implementacji środowisk sieciowych i systemowych opartych na posiadanych przez Zamawiającego platformach Microsoft Server, obejmujące instalowanie i konfigurowanie elementów systemów oraz wiedzę i doświadczenie w zakresie zarządzania tymi

środowiskami i rozwiązywania dotyczących ich problemów, obejmujące administrowanie systemami i obsługę ich użytkowników przy spełnieniu wymagań dla Microsoft Certified Solutions Associate (MCSA) lub wymagań równoważnych, tj., określonych na nie niższym poziomie jakości, potwierdzone certyfikatem Microsoft Certified Solutions Associate (MCSA) lub innym równoważnym dokumentem (zaświadczeniem);

- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie definiowania i charakteryzowania najważniejszych technik ataków stosowanych przez hakerów oraz identyfikowania i analizowania podatności na ataki hakerów w organizacji a także w tworzeniu polityki na urządzeniach IDS/IPS dotyczącej wykrywania włamań, spełniającej wymagania dla Certified Ethical Hacker (CEH) lub inne równoważne, tj. określone na nie niższym poziomie jakości niż CEH, potwierdzone certyfikatem ukończeniem szkolenia Certified Ethical Hacker (CEH) lub innym tożsamym dokumentem (zaświadczeniem) ;
- minimum 2 osobami posiadającymi wiedzę i doświadczenie w z zakresu konfiguracji i rozwiązywania problemów na posiadanych przez Zamawiającego przełącznikach sieciowych Extreme Networks przy użyciu praktyk spełniających wymagania określone dla Extreme Certified Specialist Campus EXOS lub inne równoważne, tj. określone na nie niższym poziomie jakości niż ECS Campus EXOS , potwierdzone certyfikatem Extreme Certified Specialist Campus EXOS lub innym równoważnym dokumentem (zaświadczeniem)
- minimum 2 osobami posiadającymi wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów na oferowanym systemie kontroli dostępu do sieci klasy NAC, wymagany jest certyfikat inżynierski z zakresu konfiguracji i rozwiązywania problemów na oferowanym systemie kontroli dostępu do sieci klasy NAC (zaświadczeniem)
- minimum 1 osobą posiadającą wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów na posiadanych przez Zamawiającego obecnie firewallach Sonicwall przy użyciu praktyk spełniających wymagania określone dla Certified SonicWall Security Professional lub inne równoważne, tj. określone na nie niższym poziomie jakości niż Certified SonicWall Security Professional, potwierdzone certyfikatem Certified SonicWall Security Professional lub innym równoważnym dokumentem (zaświadczeniem)
- minimum 1 osobą posiadającą wiedzę i doświadczenie z zakresu tworzenia skryptów i programów w języku Python na posiadanym przez zamawiającego oprogramowaniu lub systemach operacyjnych. Przy użyciu praktyk spełniających wymagania dla PCAP - Certified Associate in Python Programming lub inne równoważne, tj. określone na nie niższym poziomie jakości niż PCAP - Certified Associate in Python Programming, potwierdzone certyfikatem PCAP - Certified Associate in Python Programming lub innym równoważnym dokumentem (zaświadczeniem).
- minimum 1 osobę posiadającą certyfikat inżynierski z zakresu konfiguracji i rozwiązywania problemów na zaproponowane rozwiązanie Firewall