Załącznik nr 9

SPIS TREŚCI

[CZĘŚĆ I 2](#_Toc182395262)

[1. Rozbudowa systemu backup 2](#_Toc182395263)

[**1.1.** **Serwer NAS – typ 1** 2](#_Toc182395264)

[**1.2.** **Serwer NAS – typ 2** 4](#_Toc182395265)

[**1.3.** **Dodatkowe dyski do serwera NAS** 5](#_Toc182395266)

[2. AV - system bezpieczeństwa 6](#_Toc182395267)

[3. Zasilacz awaryjny UPS – 1 szt. 18](#_Toc182395268)

[4. Serwer - 3 szt. 20](#_Toc182395269)

[**4.1.** **Serwer - typ 1 - 1 szt.** 20](#_Toc182395270)

[**4.2.** **Serwer Typ 2 - 2 szt.** 22](#_Toc182395271)

[CZĘŚĆ II 25](#_Toc182395272)

[1. Przełączniki sieciowe – 2 szt. 25](#_Toc182395273)

[2. UTM – 1 szt. 30](#_Toc182395274)

[3. Wznowienie UTM - 1 szt. 36](#_Toc182395275)

[4. Ochrona poczty elektronicznej (wznowienie) 42](#_Toc182395276)

# CZĘŚĆ I

## Rozbudowa systemu backup

### **Serwer NAS – typ 1**

|  |  |
| --- | --- |
| **Procesor** | 1. Wielordzeniowy procesor o architekturze 64-bit. |
| **Obudowa** | 1. Typu rack o wysokości maksymalnej 2U z szynami przesuwnymi do instalacji w szafie rack w zestawie. |
| **Pamięć RAM** | 1. Minimum 8GB DDR4 ECC z możliwością rozbudowy do 32GB. |
| **Interfejsy sieciowe** | 1. Minimum 2 porty 1GbE RJ-45, Minimum 1 port 10GbE RJ-45, Minimum 2 porty 10GbE SFP+ 2. Obsługa agregacji łączy. |
| **Ilość obsługiwanych dysków** | 1. Minimum 12 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, 2. po podłączeniu modułów rozszerzających minimum 24 dyski. |
| **Zainstalowane dyski** | 1. 12 dysków o pojemności 12TB każdy zgodnych z listą kompatybilności oferowanego serwera NAS oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, 2. - pamięć cache: minimum 256 MB, 3. - MTBF: minimum 1 milion, - gwarancja: minimum 36 miesięcy, 4. - możliwość aktualizowania oprogramowania dysków w czasie rzeczywistym podczas pracy serwera bez potrzeby demontażu dysków. |
| **Wskaźniki LED** | 1. Status, HDD 1-12, zasilanie, LAN 1-3 |
| **Obsługa RAID** | 1. Pojedynczy, JBOD, RAID 0, 1, 5, 6, 10 wraz z obsługa dysków typu hot spare. |
| **Funkcje RAID** | 1. Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| **Szyfrowanie** | 1. Możliwość szyfrowania wybranych udziałów sieciowych. |
| **Protokoły** | 1. SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| **Usługi** | 1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Serwer i klient LDAP, możliwość utworzenia kilku wolumenów  w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych  z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. |
| **Zarządzanie dyskami** | 1. SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów. |
| **Język GUI** | 1. Polski |
| **Gwarancja i serwis** | 1. Minimum 36 miesięcy gwarancji producenta. |
| **Pobór mocy** | 1. Maksymalnie 125W w trybie pracy. |
| **Certyfikaty** | 1. FCC, CE |
| **System plików** | 1. Dyski wewnętrzne: BTRFS.  Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+. |
| **Zasilanie** | 1. Pojedynczy zasilacz o mocy minimum 300W. |

### **Serwer NAS – typ 2**

|  |  |
| --- | --- |
| **Procesor** | 1. Wielordzeniowy procesor o architekturze 64-bit. |
| **Obudowa** | 1. Typu tower. |
| **Pamięć RAM** | 1. Minimum 16GB pamięci RAM DDR4 ECC tego samego producenta co serwer. |
| **Interfejsy sieciowe** | 1. Minimum 2 porty 1GbE RJ-45 z obsługą agregacji łączy. |
| **Ilość obsługiwanych dysków** | 1. Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 9 dysków. |
| **Zainstalowane dyski** | 1. 4 dyski o pojemności 16TB każdy zgodne z listą kompatybilności oferowanego serwera NAS oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256 MB, - MTBF: minimum 1 milion, - gwarancja: minimum 36 miesięcy, - możliwość aktualizowania oprogramowania dysków w czasie rzeczywistym podczas pracy serwera bez potrzeby demontażu dysków. |
| **Wskaźniki LED** | 1. Status, HDD 1-4, zasilanie, LAN 1-2 |
| **Obsługa RAID** | 1. Podstawowy, RAID 0, 1, 5, 6, 10 wraz z obsługa dysków typu hot spare. |
| **Funkcje RAID** | 1. Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| **Szyfrowanie** | 1. Możliwość szyfrowania wybranych udziałów sieciowych. |
| **Protokoły** | 1. SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| **Usługi** | 1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów  w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. |
| **Zarządzanie dyskami** | 1. SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów. |
| **Język GUI** | 1. Polski |
| **Gwarancja i serwis** | 1. Minimum 36 miesięcy gwarancji producenta. |
| **Pobór mocy** | 1. Maksymalnie 45W w trybie pracy. |
| **Certyfikaty** | 1. CE, FCC |
| **System plików** | 1. Dyski wewnętrzne: BTRFS.  Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+. |
| **Zasilanie** | 1. Zasilacz zewnętrzny o mocy minimum 100W. |

### **Dodatkowe dyski do serwera NAS**

|  |  |
| --- | --- |
| **Rozmiar dysku** | 1. 3.5” |
| **Interfejs** | 1. SATA 6Gb/s |
| **Pojemność** | 1. Minimum 16TB |
| **Prędkość obrotowa** | 1. 7200 RPM |
| **MTBF** | 1. Minimum 1.2 miliona |
| **Gwarancja** | 1. Minimum 36 miesięcy |
| **Funkcjonalności** | 1. Możliwość aktualizowania oprogramowania dysków w czasie rzeczywistym podczas pracy serwera NAS. |

## AV - system bezpieczeństwa

1. **LICENCJA**
   1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres minimum 24 miesiące
   2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 24 miesiące gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).
   3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.
   4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.
   5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.
   6. Ilość licencji dla komputerów: 49 szt.
   7. Ilość licencji dla serwerów: 3 szt.
2. **Ochrona punktów końcowych urządzeń komputerowych** – *w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania*
   1. Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.
   2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.
   3. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.
   4. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:
      1. Microsoft Windows 10
      2. Microsoft Windows 11
      3. MacOS version 14 "Sonoma"
      4. MacOS version 13 "Ventura"
      5. MacOS version 12 "Monterey"
   5. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:
      1. Microsoft Internet Explorer
      2. Microsoft Edge
      3. Mozilla Firefox
      4. Google Chrome
      5. Safari
   6. Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.
   7. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.
   8. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej
   9. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
   10. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
   11. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
   12. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.
   13. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
   14. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
       1. dostęp do pliku;
       2. tworzenie nowego procesu;
       3. nawiązane połączenia sieciowe;
       4. wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
       5. zawartość skryptów uruchamianych na monitorowanej stacji.
   15. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
   16. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
   17. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
   18. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
   19. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
   20. Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
   21. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
   22. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
   23. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.
   24. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
   25. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
   26. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
   27. Każda detekcja zawiera co najmniej następujące informacje:
       1. Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
       2. Data i czas wystąpienia podejrzanych zdarzeń.
       3. Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
       4. Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
       5. Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
       6. Poziom ryzyka, określający istotność danej detekcji.
       7. Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
   28. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
   29. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
   30. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
   31. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
   32. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
   33. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
   34. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
   35. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
   36. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
   37. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
   38. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
   39. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
   40. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
   41. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
   42. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
   43. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
   44. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
   45. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
   46. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
   47. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
   48. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
   49. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
   50. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
   51. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
   52. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
   53. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
   54. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
   55. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
   56. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
   57. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
   58. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
   59. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
   60. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
   61. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
   62. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
   63. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
   64. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
   65. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
   66. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
   67. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
   68. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
   69. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
   70. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
   71. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
   72. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
   73. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
   74. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
   75. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
   76. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
   77. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
   78. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
   79. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
   80. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
   81. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
   82. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
   83. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
   84. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
   85. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
   86. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
   87. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
   88. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
   89. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
   90. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
   91. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
   92. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
   93. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
   94. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
   95. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
   96. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
   97. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
   98. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
   99. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
   100. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
   101. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
   102. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
   103. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
   104. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
   105. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
   106. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
   107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
   108. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
   109. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
   110. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
   111. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
   112. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
   113. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
   114. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
   115. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
   116. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
   117. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
   118. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
   119. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
   120. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
   121. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
   122. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
   123. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
   124. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
   125. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
   126. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
   127. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
   128. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
   129. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
   130. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
   131. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
   132. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
   133. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
   134. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
   135. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
   136. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
   137. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
   138. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
   139. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
   140. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
   141. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
   142. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
   143. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
   144. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
   145. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
   146. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
   147. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
   148. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
   149. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
   150. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
   151. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
   152. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
   153. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.
3. **Centralna administracja**
   1. Portal zarządzający jest dostępny w języku polskim.
   2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
   3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
   4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
   5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
   6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
   7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
   8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
   9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
   10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
   11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
   12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
   13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
   14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
   15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.
   16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
   17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
   18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
   19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
   20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
   21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
   22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
   23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
   24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
   25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
   26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
   27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
   28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
   29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
   30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
   31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
   32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
   33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
   34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
   35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
   36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji
4. **Certyfikaty i standardy**
   1. system musi posiadać certyfikaty:
      1. OPSWAT (dla EDR na poziomie min. Platinium),
      2. AV Comperative Advance +
      3. AV-TEST (ochrona w 2023 na poziomie min.6)
   2. Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6
   3. producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem.
   4. Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację ISAE 3000 assurance-based SOC 2 Type 2
   5. Producent systemu lub autoryzowany dystrybutor producenta musi być aktywnym członkiem Cloud Security Alliance
   6. Zespół reagowania na incydenty od producenta systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację CREST i NCSC
5. **Rozszerzone wsparcie serwisowe**
   1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [24] miesięcy.
   2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:
      1. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
      2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
      3. Doradztwo w zakresie konfiguracji.
      4. Zdalne wsparcie techniczne.
      5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
      6. Przygotowanie do zdalnej konfiguracji.
      7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
      8. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
      9. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
      10. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.
   3. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.
   4. Oferent winien przedłożyć dokumenty:
      1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
      2. Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.

## Zasilacz awaryjny UPS – 1 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry**  **techniczne** |
| Technologia | online, VFI-SS-111, |
| Moc wyjściowa | 3kVA/3kW; PF=1 |
| Obudowa | Rack/Tower |
| Napięcie wejściowe | 110 ÷ 300 V AC ± 2 % |
| Napięcie znamionowe (wartość skuteczna) | 230V AC |
| Prąd znamionowy (wejście) | 15,6A |
| Częstotliwość napięcia wejściowego (zakres oraz tolerancja) | 45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz |
| Częstotliwość znamionowa napięcia wejściowego | 50Hz / 60Hz |
| Zniekształcenia prądu wejściowego THDi | < 5% |
| Zakres napięcia wyjściowego | 200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC |
| Zniekształcenia napięcia wyjściowego THDu | < 1% dla Pmax (liniowe)  < 5% (nieliniowe wg PN EN 62040-3) |
| Gniazda wyjściowe | 4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A) |
| Akumulatory wewnętrzne UPS | Minimum 6szt akumulatorów 12V9Ah |
| Moduły bateryjne | możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah) |
| Wymagany czas podtrzymania dla obciążenia 2,4kW | 46 min (akumulatory umieszczone w UPS i maksymalnie 2 Modułach Bateryjnych) |
| Przeciążalność | 105-125% - 5min / 125-150% - 30s / >150% - 500ms |
| EPO | Wymagane – standard NC |
| Sygnalizacja | akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass |
| Język oprogramowania | polski i angielski do wyboru z poziomu interfejsu użytkownika |
| Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu) | Wymagane, konfigurowalne z poziomu oprogramowania (przez USB) |
| Wymagane certyfikaty | CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument) |
| Komunikacja z urządzeniem | RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – wymagana na wyposażeniu |
| Wymiary UPS (rack) (wys x szer x gł) | Nie więcej niż 86 x 439 x 600 mm |
| Wsporniki do montażu w szafie RACK | Wymagane |
| Oprogramowanie do monitorowania pracy zasilacza UPS | Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania) |
| Oprogramowanie - funkcjonalność | możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS’ów w oprogramowaniu |
| Oprogramowanie - funkcjonalność | Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku. |
| Oprogramowanie - funkcjonalność | Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS. |
| Serwis producenta | wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty |
| Gwarancja | Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych |
| Dokumentacja | Instrukcja w języku polskim |

## Serwer - 3 szt.

### **Serwer - typ 1 - 1 szt.**

|  |  |
| --- | --- |
| **Parametr, cecha, funkcjonalność** | **Opis wymagań minimalnych** |
| **Płyta główna** | 1. Serwerowa, jednoprocesorowa z zainstalowanym modułem TPM, posiadająca 4 złącza DIMM z obsługą do 128GB pamięci RAM |
| **Procesor** | 1. Jeden procesor o bazowym taktowaniu minimum 2.9Ghz, co najmniej 6 rdzeniowy, 12 wątkowy, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie minimum 22330 punktów w teście PassMark |
| **Złącza PCI** | 1. 1 x PCI-e 5.0 x8 |
| **Zarządzanie** | 1. Zintegrowany moduł zarządzający z dedykowanym portem RJ45 i pełnym przekierowaniem konsoli KVM |
| **Karta graficzna** | 1. Zintegrowana z płytą, pozwalająca wyświetlić obraz w rozdzielczości 1920 x 1200 |
| **Pamięć** | 1. 1x 32GB RAM ECC DDR5 |
| **Karta sieciowa** | 1. Zintegrowana z płytą, dwuportowa 1Gb Ethernet (niezależna od karty zarządzającej) |
| **Kontroler RAID** | 1. Zintegrowany z płytą kontroler SATA umożliwiający utworzenie macierzy RAID 0,1,10. 2. Obsługa co najmniej 8 urządzeń SATA. |
| **Dysk twardy** | 1. Cztery dyski SATA o pojemności min 2TB, prędkość obrotowa min 7200. Dyski klasy Enterprise przeznaczone do pracy w serwerach. |
| **Obudowa** | 1. Obudowa Rack 1U wyposażona w teleskopowe szyny montażowe. Jeden zasilacz o mocy co najmniej 350W (certyfikat 80 PLUS Platinum). 4 zatoki hot-swap na dyski twarde 3,5” (wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania przez użytkownika własnego dysku 3,5” bez konieczności zakupu specjalnej ramki) |
| **Porty** | 1. na tylnym panelu: 2 x USB 2.0, 2 x USB 3.2, 1x COM. 2. 1 port USB 3.0 Typ A wewnątrz obudowy serwera. 3. Dodatkowo pinheader 4x USB 2.0, 2x USB 3.2 |
| **Gwarancja** | 1. Minimum 3 lata gwarancji 2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. 3. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) 4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 5. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 6. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 7. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 8. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
| **Inne** | 1. Możliwość sprawdzenia konfiguracji i pobrania sterowników ze strony www producenta serwera po podaniu nr seryjnego. Wymagane podanie strony wwww. |
| **Certyfikaty i oświadczenia (dokumenty załączyć do oferty)** | 1. Certyfikat PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014, PN-EN ISO 50001:2018 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis, 2. Certyfikat SA8000 3. Oznaczenie CE |
| **System operacyjny/dodatkowe oprogramowanie** | 1. Windows Server 2022 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 2 maszyn wirtualnych. 2. Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania: 3. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 4. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 5. 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. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; 11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 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 2 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 23. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016. |

### **Serwer Typ 2 - 2 szt.**

|  |  |
| --- | --- |
| **Płyta główna** | 1. Serwerowa, jednoprocesorowa z zainstalowanym modułem TPM, posiadająca 4 złącza DIMM z obsługą do 128GB pamięci RAM |
| **Procesor** | 1. Jeden procesor o bazowym taktowaniu minimum 2.9Ghz, co najmniej 6 rdzeniowy, 12 wątkowy, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie minimum 22330 punktów w teście PassMark |
| **Złącza PCI** | 1. 1 x PCI-e 5.0 x16 (elektrycznie x8), 1 x PCI-e 5.0 x8, 2 x PCI-e 4.0 x8 (elektrycznie x4) |
| **Zarządzanie** | 1. Zintegrowany moduł zarządzający z dedykowanym portem RJ45 i pełnym przekierowaniem konsoli KVM |
| **Karta graficzna** | 1. Zintegrowana z płytą, pozwalająca wyświetlić obraz w rozdzielczości 1920 x 1200 |
| **Pamięć** | 1. 1x 32GB RAM ECC DDR5 |
| **Karta sieciowa** | 1. Zintegrowana z płytą, dwuportowa 1Gb Ethernet (niezależna od karty zarządzającej) |
| **Kontroler RAID** | 1. Zintegrowany z płytą kontroler SATA umożliwiający utworzenie macierzy RAID 0,1,10. 2. Obsługa co najmniej 8 urządzeń SATA. |
| **Dysk twardy** | 1. Dwa dyski SATA o pojemności min 960GB, parametr DWPD nie mniejszy niż jeden. 2. Jeden dysk SATA o pojemności min 4TB, prędkość obrotowa min 7200. Dysk klasy Enterprise przeznaczony do pracy w serwerach. |
| **Obudowa** | 1. Obudowa Rack 2U wyposażona w teleskopowe szyny montażowe. Dwa zasilacze o mocy co najmniej 600W każdy (certyfikat 80 PLUS Platinum). Wentylatory hot-swap. 8 zatok hot-swap na dyski twarde 3,5” (wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania przez użytkownika własnego dysku 3,5” bez konieczności zakupu specjalnej ramki) |
| **Porty** | 1. na tylnym panelu: 2 x USB 2.0, 2 x USB 3.2, 1x COM. 2. 1 port USB 3.0 Typ A wewnątrz obudowy serwera. 3. Dodatkowo pinheader 4x USB 2.0, 2x USB 3.2 |
| **Gwarancja** | 1. Minimum 3 lata gwarancji    * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.    * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)    * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.    * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.    * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.    * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 2. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
| **Inne** | 1. Możliwość sprawdzenia konfiguracji i pobrania sterowników ze strony www producenta serwera po podaniu nr seryjnego. Wymagane podanie strony wwww. |
| **Certyfikaty i oświadczenia (dokumenty załączyć do oferty)** | 1. Certyfikat PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014, PN-EN ISO 50001:2018 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis, 2. Certyfikat SA8000 3. Oznaczenie CE |
| **System operacyjny/dodatkowe oprogramowanie** | 1. Windows Server 2022 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 2 maszyn wirtualnych. 2. Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania: 3. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 4. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 5. 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. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; 11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 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 2 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 23. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016. |

# CZĘŚĆ II

## Przełączniki sieciowe – 2 szt.

1. **Wymagania ogólne**
   1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
2. **Wymagane parametry fizyczne**
   1. Wymagane parametry fizyczne
      1. możliwość montażu w szafie 19”
      2. jeden wewnętrzny zasilacze 230V AC
      3. port USB umożliwiający podłączenie zewnętrznej pamięci flash
      4. Urządzenie musi cechować się bezwiatrakową obudową (chłodzenie pasywne)
3. **Wymagana konfiguracja portów**
   1. Przełącznik musi posiadać minimum:
      1. 48 portów gigabitowych w standardzie 100/1000BaseT
      2. Minimum 2 porty typu COMBO 1Gb SFP/RJ45
      3. Minimum 2 porty typu 10Gb SFP+
   2. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4. **Przełącznik**
   1. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
      1. Zarządzanie stosem poprzez jeden adres IP
      2. Do min. 4 jednostek w stosie
      3. Magistrala statkująca o wydajności 40 Gb/s
      4. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie
      5. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
      6. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów statkujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
   2. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą (dwóch dodatkowych niezależnych od portów podstawowych) portów SFP+ w takim wypadku wymagane jest aby z przełącznikiem musi być dostarczony kabel do stackowania 10GE SFP+ od długości minimum 1m.
   3. UWAGA: Przełącznik powinien wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerwania pracy całego stosu przełączników
5. **Matryca przełączająca**
   1. Matryca przełączająca o wydajności min. 140 Gbps
   2. Obsługa min 16 000 adresów MAC
   3. Wbudowana pamięć RAM min. 1 GB
   4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
   5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
   6. Obsługa ramek jumbo o wielkości min. 9 216 bajtów
   7. Obsługa protokołu GVRP lub równoważny
   8. Wsparcie dla protokołów:
      1. IEEE 802.1w Rapid Spanning Tree
      2. IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.
   9. Obsługa min. 64 tras dla routingu IPv4
   10. Obsługa min. 32 tras dla routingu IPv6
   11. Obsługa protokołów routingu minimum:
       1. IPv4: minimum: statyczny
       2. IPv6: minimum: statyczny
   12. Obsługa protokołów LLDP i LLDP-MED
   13. Przełącznik musi posiadać funkcjonalność DHCP Server
   14. Obsługa ruchu multicast:
       1. IGMP Snooping v1, v2 i v3
       2. Obsługa 1000 grup multicast
   15. Obsługa mechanizmu DHCP snooping
   16. Obsługa mechanizmu ARP spoof protection
6. **Mechanizmy związane z zapewnieniem bezpieczeństwa sieci**
   1. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
      1. min. 4 poziomy dostępu administracyjnego poprzez konsolę
      2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
      3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www
      4. zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6
      5. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
      6. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),
   2. Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.
7. **Wymagane opcje zarządzania**
   1. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN,
   2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC),
   3. urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
   4. dedykowany port konsoli zgodny ze standardem RS-232,
   5. Obsługa skryptów BASH oraz Python
   6. Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
   7. Wraz z urządzeniami muszą zostać dostarczone:
      1. pełna dokumentacja w języku polskim lub angielskim,
      2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
   8. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
   9. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
   10. Przełącznik być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie.
   11. Dodatkowo: zamawiający wymaga, aby przełącznik posiadał 2 letni serwis gwarancyjny na sprzęt wraz z dostępem do najnowszych wersji oprogramowania.
8. **Architektura i zarządzanie**
   1. Dedykowane oprogramowanie służące do zarządzania i monitorowania pracy wszystkimi przełącznikami opisanymi w tym zamówieniu. Należy zapewnić licencję na obsługę min. 10 aktywnych urządzeń sieciowych (przełączniki)
   2. System Zarządzania i Monitoringu musi być tego samego producenta co urządzania LAN
   3. Oprogramowanie musi mieć możliwość instalacji w środowisku wirtualnym Vmware, Hyper-V i KVM
   4. Obsługa musi być możliwa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW
   5. Oprogramowanie musi pracować w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień),
   6. Funkcja definiowania poziomu dostępu dla administratorów (wymagana jest możliwość profilowania kont administratorskich a użytkownikami Active Directory) z przypisanymi:
      1. Rolami
      2. Segmentami sieci, do których uzyskuje się dostęp
   7. Oprogramowanie musi umożliwiać zbieranie statystyk w wykorzystaniem SNMP;
   8. Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania.
   9. Możliwość podglądu obecnej aktywnej konfiguracji z konfiguracją aktywną w zadanym historycznym momencie z podglądem elementów: dodanych, usuniętych, zmienionych względem danych konfiguracji.
   10. Możliwość wysyłania alarmów mailem i SMS'em w przypadku wystąpienia zdarzeń określonych jako krytyczne
   11. Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
   12. Lokalizowanie użytkowników po adresie nazwie sieciowej użytkownika, IP oraz MAC
   13. Oprogramowanie musi posiadać narzędzia do automatycznego wykrywania urządzeń sieciowych instalowanych w sieci,
   14. Oprogramowanie musi umożliwiać aktualizację oprogramowania w urządzeniach sieciowych,
   15. Oprogramowanie musi posiadać narzędzia pozwalające na:
       1. graficzną prezentację topologii sieci, w tym również graficzną, prezentację/budowę serwerowni lub dowolnego węzła sieciowego
       2. konfigurację i monitoring sieci VLAN,
       3. lokalizację oraz uzyskanie informacji o aktywności urządzeń w sieci,
   16. Obrazowanie sieci w postaci mapki w tym lokalizacją urządzeń za pomocą Google Maps wraz z wyróżnianiem kolorami występujących alarmów na danych urządzeniach
   17. Oprogramowanie musi umożliwiać zbieranie informacji o nieprawidłowych parametrach pracy zainstalowanego sprzętu wraz z możliwością generowania alertów o błędach czy przekroczeniu założonych parametrów (środowiskowych, wydajnościowych, dotyczących bezpieczeństwa),
   18. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA w szczególności funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration.
   19. Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
   20. Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń, które powinno odbywać się za pomocą:
       1. Autoprovisioningu urządzeń – czyli urządzenie podpięte do sieci bez konfiguracji powinno zgłosić się do oprogramowania do zarzadzania siecią o dedykowną dla urządzenia konfiguracje
       2. Konfiguracja za pomocą Web GUI min. VLAN, IP Interfejsy, QoS, ACL
       3. CLI Scripting – czyli możliwość przygotowania zbiorowej konfiguracji dla przełączników wraz ze zmiennymi w zależności modelu urządzenia
9. **Moduł zabezpieczenie dostępu do sieci LAN**
   1. Oprogramowanie musi umożliwiać Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x w tym musi posiadać wewnętrzny serwer uwierzytelniający, pozwalający na integracje z usługami Active Directory
   2. Licencje oprogramowania muszą umożliwiać integracja z Active Directory/LDAP w tym profilowanie użytkowników poprzez atrybuty AD/LDAP minimalnie:
      1. Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od przypisania użytkownika do grupy AD/LDAP
      2. Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od posiadanego systemu operacyjnego.
      3. Poprzez profilowanie rozumiane jest:
         1. przypisanie urządzeń użytkownika do zdefiniowanego VLAN
         2. nadanie urządzeniom polityk QoS
      4. nadanie urządzeniom dostępu lub uniemożliwienie dostępu do konkretnych segmentów sieci (ACL L2/L3/L4 oraz L7 – warstwa aplikacyjna)
10. **Moduł dostęp gościnny**
    1. Samodzielna rejestracja klientów gościnnych w oparciu o:
       1. Adres e-mail
       2. Numer telefonu ( wiadomość SMS)
    2. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
    3. Logowanie w oparciu o portale społecznościowe min. Google, Facebook
    4. Funkcja personalizacji strony gościnnej w tym obsługa portalu WiFi4EU
11. **Gwarancja**
    1. Na oprogramowanie powinno być dostarczone wsparcie na okres min. 3 lat, umożliwiające min. kontakt z działem technicznym, rozwiązywanie problemów, możliwość aktualizacji oprogramowania do najnowszej wersji.

## UTM – 1 szt.

**Szczegółowe wymagania techniczne dla zapory UTM:**

1. **Wymagania Ogólne**
   1. 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.
   2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   3. 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 3 administratorów do poszczególnych instancji systemu.
   4. System musi wspierać IPv4 oraz IPv6 w zakresie:
      1. Firewall.
      2. Ochrony w warstwie aplikacji.
      3. Protokołów routingu dynamicznego.
2. **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.
3. **Interfejsy, Dysk, Zasilanie:**
   1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.
   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 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
   4. System musi być wyposażony w zasilanie AC.
4. **Parametry wydajnościowe:**
   1. W zakresie Firewall’a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
   2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
   3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
   4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,1 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 1,4 Gbps.
   6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.
   7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
5. **Funkcje Systemu Bezpieczeństwa:**
   1. 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).
   2. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
   3. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać 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.
   4. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
   5. 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
6. **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:
      1. Translację jeden do jeden oraz jeden do wielu.
      2. 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.
      1. Amazon Web Services (AWS).
      2. Microsoft Azure
      3. Google Cloud Platform (GCP).
      4. OpenStack.
      5. VMware NSX.
7. **Połączenia VPN**
   1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
      1. Wsparcie dla IKE v1 oraz v2.
      2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
      3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
      4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
      5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
      6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
      7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
      8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
      9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
   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.

1. **Routing i obsługa łączy WAN**
   1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
      1. Routingu statycznego.
      2. Policy Based Routingu.
      3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. **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.
3. **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.
4. **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 postępowania 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.
5. **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.
6. **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.
7. **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.
8. **Uwierzytelnianie użytkowników w ramach sesji**
   1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
      1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
      2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
      3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
   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.
9. **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.
10. **Logowanie**
    1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania 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.
11. **Certyfikaty**
    1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.
12. **Serwisy i licencje**
    1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 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.
13. **Gwarancja oraz wsparcie**
    1. 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.
    2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

## Wznowienie UTM - 1 szt.

Szczegółowe wymagania techniczne dla zapory UTM

1. **Wymagania Ogólne**
   1. 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.
   2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   3. 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 3 administratorów do poszczególnych instancji systemu.
   4. System musi wspierać IPv4 oraz IPv6 w zakresie:
      1. Firewall.
      2. Ochrony w warstwie aplikacji.
      3. Protokołów routingu dynamicznego.
2. **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.
3. **Interfejsy, Dysk, Zasilanie:**
   1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.
   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 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
   4. System musi być wyposażony w zasilanie AC.
4. **Parametry wydajnościowe:**
   1. W zakresie Firewall’a obsługa nie mniej niż 1,5 mln. Jednoczesnych połączeń oraz 35 tys. Nowych połączeń na sekundę.
   2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
   3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
   4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,1 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 1,4 Gbps.
   6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.
   7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
5. **Funkcje Systemu Bezpieczeństwa:**
   1. 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 postępowania powinny zostać 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. 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
6. **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:
      1. Translację jeden do jeden oraz jeden do wielu.
      2. 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.
      1. Amazon Web Services (AWS).
      2. Microsoft Azure
      3. Google Cloud Platform (GCP).
      4. OpenStack.
      5. VMware NSX.
7. **Połączenia VPN**
   1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
      1. Wsparcie dla IKE v1 oraz v2.
      2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
      3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
      4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
      5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
      6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
      7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
      8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
      9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
   2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
      1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
      2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
      3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
8. **Routing i obsługa łączy WAN**
   1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
      1. Routingu statycznego.
      2. Policy Based Routingu.
      3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9. **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.
10. **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.
11. **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 postępowania 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.
12. **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.
13. **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.
14. **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.
15. **Uwierzytelnianie użytkowników w ramach sesji**
    1. 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
       1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
       2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
       3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
    2. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
    3. 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. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
16. **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.
17. **Logowanie**
    1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania 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.
18. **Certyfikaty**
    1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.
19. **Serwisy i licencje**
    1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 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.
20. **Gwarancja oraz wsparcie**
    1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.
    2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

## Ochrona poczty elektronicznej (wznowienie)

1. **Wymagania ogólne**
   1. System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
   2. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.
   3. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.
   4. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:
      1. Tryb Gateway.
      2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
2. **Parametry fizyczne systemu antyspamowego**
   1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.
3. **Funkcja serwera poczty**
   1. W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
4. **Funkcje serwera poczty** 
   1. W tym zakresie dostarczony system musi zapewniać:
      1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
      2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
      3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
      4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
      5. Polski interfejs użytkownika przy dostępie przez WebMail.
      6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
      7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
5. **Ogólne funkcje systemu ochrony poczty**
   1. Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
      1. Wsparcie dla co najmniej 20 domen pocztowych.
      2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
      3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
      4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
      5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
      6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
      7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
      8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
      9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
      10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
      11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
      12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
      13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
      14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
      15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
      16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
      17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
6. **Kontrola antywirusowa i ochrona przed malware**
   1. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
      1. Skanowanie antywirusowe wiadomości SMTP.
      2. Kwarantannę dla zainfekowanych plików.
      3. Skanowanie załączników skompresowanych.
      4. Definiowanie komunikatów powiadomień w języku polskim.
      5. Blokowanie załączników w oparciu o typ pliku.
      6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
      7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
      8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
      9. Ochronę typu wirus outbrake.
7. **Kontrola antyspamowa** 
   1. System musi zapewniać poniższe funkcje i metody filtrowania spamu:
      1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
      2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
      3. Szczegółowa kontrola nagłówka wiadomości.
      4. Analiza Heurystyczna.
      5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
      6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
      7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
      8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
      9. Kontrola w oparciu o Greylisting oraz SPF.
      10. Filtrowanie treści wiadomości i załączników.
      11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
      12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
      13. Ochrona typu outbrake.
      14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
      15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
8. **Ochrona przed atakami na usługę poczty**
   1. System musi zapewniać poniższe funkcje i metody filtrowania:
      1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
      2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
      3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
      4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
      5. Weryfikacja poprawności adresu e-mail nadawcy.
9. **Funkcje logowania i raportowania**
   1. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
      1. Logowanie do zewnętrznego serwera SYSLOG.
      2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
      3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
      4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
      5. Możliwość analizy przebiegu sesji SMTP.
      6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
      7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
      8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
10. **Funkcje pracy w trybie wysokiej dostępności (HA)**
    1. System ochrony poczty musi zapewniać poniższe funkcje:
       1. Konfigurację HA w każdym z trybów: gateway, transparent.
       2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
       3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
       4. Monitorowanie stanu pracy klastra.
11. **Aktualizacje sygnatur, dostęp do bazy spamu** 
    1. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
       1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
       2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
12. **Zarządzanie** 
    1. System ochrony poczty musi zapewniać poniższe funkcje:
       1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
       2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
       3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
13. **Certyfikaty**
    1. Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:
       1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
14. **Serwisy i licencje**
    1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
    2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
    3. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 24 miesięcy.
    4. System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7