**Znak sprawy: 31/2022** **Załącznik nr 7 do SWZ**

# OPIS PRZEDMIOTU ZAMÓWIENIA

## 1. Oprogramowanie antywirusowe typu ESET PROTECT Essential ON-PREM + 36 miesięcy - licencja (400 sztuk)

### Stacje robocze Linux

1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop 18.04 / 20.04 LTS 64-bit, Red Hat Enterprise Linux 7, 8 64-bit, SUSE Linux Enterprise Desktop.

2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.

4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.

7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.

10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

11. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.

12. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

13. Rozwiązanie musi posiadać możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.

14. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.

15. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

17. Aktualizacje silnika detekcji muszą być dostępne z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).

18. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.

19. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

20. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień lokalnie oraz zdalnie za pomocą dedykowanego narzędzia.

21. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Ochrona stacji roboczych - Mac OSX**

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Mac OS X 10.12 lub nowszych.

2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

3. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.

4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

6. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.

7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

9. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).

10. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.

11. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.

12. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

13. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.

14. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

15. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody

heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

16. Rozwiązanie musi posiadać możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.

17. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

18. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

19. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

20. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".

21. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych. Funkcja musi umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.

22. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację. silnika detekcji.

23. Aktualizacja silnika detekcji rozwiązania musi być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.

24. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.

25. Rozwiązanie musi umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.

26. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

27. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji silnika detekcji i samego oprogramowania oraz dokonanym skanowaniu komputera.

28. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.

29. Rozwiązanie musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.

30. Rozwiązanie musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.

31. Rozwiązanie musi umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.

32. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.

33. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

34. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

35. Rozwiązanie musi umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.

36. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.

37. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

38. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Ochrona stacji roboczych - Windows**

1. Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11.

2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.

3. Rozwiązanie musi wspierać architekturę ARM64.

4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.

7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. Ochrona antywirusowa i antyspyware

8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.

11. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.

12. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

13. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.

14. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.

15. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

16. Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

17. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.

18. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.

19. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.

20. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

21. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.

22. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.

23. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.

24. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.

25. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.

26. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.

27. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

28. Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.

29. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.

30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

31. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

32. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

33. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.

34. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.

35. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.

36. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

37. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

38. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.

39. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.

40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.

41. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.

43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.

44. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.

45. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

46. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.

47. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

48. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.

49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

50. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.

51. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.

52. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.

53. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.

54. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

55. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.

56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.

57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.

58. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

59. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.

60. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

61. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.

62. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

63. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

64. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

65. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).

66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

69. Rozwiązanie musi posiadać zaawansowany skaner pamięci.

70. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.

71. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

72. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

73. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.

74. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

75. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.

76. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.

77. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.

78. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.

79. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).

80. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

81. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.

82. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.

83. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.

84. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.

85. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.

86. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

87. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.

88. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.

89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.

90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.

91. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.

92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

93. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.

94. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.

95. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

96. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

97. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

98. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.

99. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.

100. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.

101. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.

102. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

103. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

104.Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

105.Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

106.Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.

107.Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.

108.Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

109.Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi wspierać system co najmniej Android 5.0.

2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.

3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.

4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.

5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".

6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.

9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.

10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.

11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). Skanowanie na żądanie:

12. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.

13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.

14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.

15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia. Ochrona przed kradzieżą:

16. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.

17. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

- usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych,
- zablokowania urządzenia,
- uruchomienie sygnału dźwiękowego,
- lokalizację GPS. Polityka ustawień:

18. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:

- połączenie Wi-Fi,
- GPS,
- usługi lokalizacyjne,
- pamięć,
- roaming danych,
- roaming połączeń,
- nieznane źródła,
- tryb debugowania,
- komunikacja NFC,
- szyfrowanie pamięci masowej,
- urządzenie zrootowane. Kontrola aplikacji:

19. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.

20. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.

21. Blokowanie aplikacji musi być możliwe w oparciu o:

- nazwę aplikacji,
- nazwę pakietu,
- kategorię sklepu Google Play,
- uprawnienia aplikacji,
- pochodzenie aplikacji z nieznanego źródła. Zabezpieczenia urządzenia:

22. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:

- minimalny poziom zabezpieczeń i złożoność blokady ekranu,
- maksymalną dopuszczaną liczbę błędnych prób odblokowania,
- odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
- czas, po którym automatycznie nastąpi blokada ekranu,

- ograniczenie dostępu do kamery wbudowanej w urządzenie. Aktualizacje modułów:

23. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.

24. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.

25. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. Konfiguracja i zdalne zarządzanie:

26. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.

27. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.

28. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.

29. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.

30. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:

- za pomocą kodu QR,
- za pomocą unikatowego łącza,
- za pomocą wiadomości e-mail, W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).

**Administracja zdalna**

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019,2022 oraz systemach Linux.

2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.

5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.

9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.

10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.

11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.

12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.

14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.

16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

17. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".

18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.

19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.

20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.

23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.

24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.

25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.

26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.

27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.

28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.

31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.

32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.

33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.

35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.

37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.

38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.

39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.

41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.

42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.

43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.

47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.

48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.

51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.

53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

55. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.

57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.

58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.

59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.

61. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.

62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.

63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.

64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.

65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.

66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.

67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.

68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.

69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.

70. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.

71. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.

72. Powiadomienia mailowe mają być wysyłane w formacie HTML.

73. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.

74. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.

75. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.

76. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.

77. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.

78. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.

79. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.

80. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.

81. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.

82. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

83. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.

84. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.

85. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.

86. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

87. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.

88. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.

89. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

90. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.

91. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).

92. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.

93. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).

94. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

**Ochrona serwera – Linux Architektura rozwiązania**

1. Rozwiązanie musi posiadać skaner antywirusowy i antyspyware.

2. Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących.

3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

4. Rozwiązanie musi posiadać wbudowany mechanizm typu ,,watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.

5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikroserwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.

6. Rozwiązanie musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.

7. Rozwiązanie musi posiadać wsparcie dla SecureBoot-a.

8. Rozwiązanie musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.

9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.

10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.

11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.

12. Rozwiązanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".

13. Rozwiązanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7, Centos 8.

14. Wszystkie mechanizmy bezpieczeństwa rozwiązania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.

15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.

16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

17. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.

18. Rozwiązanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.

19. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".

20. Rozwiązanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.

21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

**Interfejs graficzny**

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.

3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.

5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.

6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.

7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników, w lokalnej konsoli administracyjnej.

8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.

9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.

10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

**Skanowanie sieciowych systemów plików**

1. Rozwiązanie musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.

2. Rozwiązanie nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.

3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.

4. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

**Instalacja**

1. Rozwiązanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.

2. Rozwiązanie musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.

3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

4. Rozwiązanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL) 7, CentOS 7, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.

**Licencjonowanie**

1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

2. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji rozwiązania w trybie offline

**2. Rozbudowa Istniejącej Infrastruktury Serwerowej – Serwerowe Systemy Operacyjne - Windows Server 2022 Datacenter (3 sztuki) + Windows Server 2022 Standard (10 sztuk) + Windows Server Calc (400 sztuk)**

Przedmiotem zamówienia jest sprzedaż i dostarczenie niewyłącznych, nieograniczonych czasowo licencji serwerowego systemu operacyjnego, wyszczególnionych w poniższej :

- Windows Server Datacenter 16 Core 2022 Sngl Licenses ESD w ilości 3 szt
- Windows Server Datacenter 16 Core 2022 Sngl Licenses ESD w ilości 10 szt
- Licencje dostępowe CAL , w licencji na urządzenia dla systemu operacyjnego Windos 2022 w ilości 400 szt.

W związku z używaniem w środowisku Zamawiającego serwerów opartych o system operacyjny Microsoft Windows Serwer nie istnieją licencje równoważne do przedstawionych powyżej. Licencje wieczyste muszą pozwalać na swobodne przenoszenie pomiędzy serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu). Wymagane jest zapewnienie instalacji oprogramowania na wielu urządzeniach przy wykorzystaniu jednego standardowego obrazu, z prawem do:

a. wielokrotnego użycia jednego obrazu dysku w procesie instalacji,
b. tworzenia kopii zapasowych
c. aktywacji oprogramowania przy użyciu pojedynczego klucza aktywacyjnego dla danego typu programowania

**3. Rozbudowa Istniejącej Infrastruktury Sieciowej – firewall typu FortiGate (3 sztuki)+ Konfiguracja klastra + Wkładki dla firewall typu FortiGate (4 sztuki) + licencja 1 rok + oprogramowanie do Zarządzania.**

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe

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

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z

funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

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

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

- 5 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 xxx interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 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 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http –minimum 300Mbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą

one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach 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 Polityki, Firewall

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi

zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach 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.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków –

białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On

przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów:

RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach 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.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące

certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

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 12 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: 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.

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu,

Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co

najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna

istnieć możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

- 16 portami Gigabit Ethernet RJ-45.
- 8 gniazdami SFP 1 Gbps.
- 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 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 2.5 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application

Control, Antywirus - minimum 1 Gbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą

one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach 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. Analiza ruchu szyfrowanego protokołem SSH.

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

14. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

15. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np.

DMZ, LAN, WAN.

17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

**Funkcje SD-WAN**

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach 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.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach 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.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące

certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

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 12 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: 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.

**Oprogramowanie do Zarządzania:**

**Wymagania Ogólne**
W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

**Interfejsy, Dysk:**

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

**Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

**Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

**Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

**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. Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

**Opisy do wymagań ogólnych**

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

**4. Rozbudowa Istniejącej Infrastruktury Sieciowej Administracja/Izba Przyjęć – przełącznik sieciowy typu Aruba 6100 (3 sztuki 48 porty i 2 sztuki 24 porty) + Wkładka światłowodowa (20 sztuk) + Multimode OM3 Duplex (1 metr - 20 sztuk, 2 metry – 10 sztuk, 3 metry – 10 sztuk)**

**Wymagania dla urządzenia 24 porty (2 sztuki)**

1. Minimum 24 porty 100/1000BastT umieszczonych z przodu obudowy ze wsparciem dla standardu 802.3at (PoE+)

2. Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy.

3. Przepustowość: minimum 127 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)

4. Wydajność: minimum 95 Mp/s

5. Bufor pakietów: minimum 12 MB

6. Minimum 4GB pamięci operacyjnej

7. Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).

8. Dedykowany port konsoli USB-C

9. Port USB 2.0 (niezależny od portu konsoli USB)

10. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)

11. Tablica adresów MAC o wielkości minimum 8000 pozycji

12. Obsługa Jumbo Frames

13. Obsługa sFlow lub Netflow

14. Obsługa skryptów w języku Python

15. Obsługa REST API

16. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.

17. Obsługa RMON (minimum grupy 1,2,3 i 9)

18. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN

19. Obsługa standardu 802.1v

20. Obsługa protokołu MVRP

21. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3,

dedykowaną aplikację na urządzenia mobilne

22. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)

23. Obsługa Secure FTP lub SCP

24. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)

25. Obsługa SNTPv4 lub NTP

26. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)

27. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)

28. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting

29. Obsługa uwierzytelniania użytkowników zgodna z 802.1x

30. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS

31. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW

32. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie

33. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+

34. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+

35. Wbudowany serwer DHCP

36. Obsługa funkcji User Datagram Protocol (UDP) helper

37. Obsługa blokowania nieautoryzowanych serwerów DHCP

38. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego

39. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)

40. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP

41. Zakres pracy od 0 do 45°C

42. Zasilacz zapewniający budżet mocy PoE na poziomie nie niższym niż 370W

43. Przełącznik w obudowie 19". Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 30 cm.

44. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania

45. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

46. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem

sprzętu.

**Dodatkowy zapis do przełącznika :**
Do każdego oferowanego urządzenia należy dostarczyć :
- 4 szt oryginalnych wkładek optycznych tego samego producenta co urządzenia o następujących parametrach - 10G SFP+ LC LR 10km SMF Transceiver . W przypadku dostarczenia wkładek innego producenta niż oferowany przełącznik należy dostarczyć oświadczenie producenta przełącznika dotyczące kompatybilności oferowanych urządzeń.
- 10 szt - patchcordy światłowodowe długości 1 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi.
- 5 szt - patchcordy światłowodowe długości 2 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi.
- 5 szt - patchcordy światłowodowe długości 3 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi.

**Wymagania dla urządzenia 48 portów (3 sztuki)**

1. Minimum 48 porty 100/1000BastT umieszczonych z przodu obudowy ze wsparciem dla standardu 802.3at (PoE+)

2. Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy.

3. Przepustowość: minimum 175 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)

4. Wydajność: minimum 98 Mp/s

5. Bufor pakietów: minimum 12 MB

6. Minimum 4GB pamięci operacyjnej

7. Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).

8. Dedykowany port konsoli USB-C

9. Port USB 2.0 (niezależny od portu konsoli USB)

10. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)

11. Tablica adresów MAC o wielkości minimum 8000 pozycji

12. Obsługa Jumbo Frames

13. Obsługa sFlow lub Netflow

14. Obsługa skryptów w języku Python

15. Obsługa REST API

16. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.

17. Obsługa RMON (minimum grupy 1,2,3 i 9)

18. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN

19. Obsługa standardu 802.1v

20. Obsługa protokołu MVRP

21. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne

22. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)

23. Obsługa Secure FTP lub SCP

24. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)

25. Obsługa SNTPv4 lub NTP

26. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)

27. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)

28. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting

29. Obsługa uwierzytelniania użytkowników zgodna z 802.1x

30. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS

31. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW

32. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie

33. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+

34. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+

35. Wbudowany serwer DHCP

36. Obsługa funkcji User Datagram Protocol (UDP) helper

37. Obsługa blokowania nieautoryzowanych serwerów DHCP

38. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego

39. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)

40. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z

uwzględnieniem adresów, MAC, IP i portów TCP/UDP

41. Zakres pracy od 0 do 45°C

42. Zasilacz zapewniający budżet mocy PoE na poziomie nie niższym niż 370W

43. Przełącznik w obudowie 19". Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 33 cm.

44. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania

45. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

46. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

**Dodatkowy zapis do przełącznika :**
Do każdego oferowanego urządzenia należy dostarczyć :
- 4 szt oryginalnych wkładek optycznych tego samego producenta co urządzenia o następujących parametrach - 10G SFP+ LC LR 10km SMF Transceiver . W przypadku dostarczenia wkładek innego producenta niż oferowany przełącznik należy dostarczyć oświadczenie producenta przełącznika dotyczące kompatybilności oferowanych urządzeń.
- 10 szt - patchcordy światłowodowe długości 1 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi.
- 5 szt - patchcordy światłowodowe długości 2 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi.
- 5 szt - patchcordy światłowodowe długości 3 m każdy , kompatybilne z dostarczonymi wkładkami optycznymi..