

Radom, dnia 06.11.2025 r.

ZAPROSZENIE DO ZŁOŻENIA OFERTY

Zamawiający – Samodzielny Wojewódzki Publiczny Zespół Zakładów Psychiatrycznej Opieki Zdrowotnej im. dr B. Borzym, ul. Krychnowicka 1, 26-607 Radom, zaprasza do złożenia oferty na: **„Odnowienie licencji oprogramowania antywirusowego, odnowienie licencji UTM typ - 1 i UTM - typ - 2”**

Informacje niezbędne do przygotowania i złożenia oferty:

1.Opis przedmiotu zamówienia:

Przedmiotem zamówienia jest przedłużenie ważności licencji, dotyczących n/w produktów:

- Oprogramowanie antywirusowe - licencje dla 260 stanowisk
- Odnowienie licencji pakietu UTM – typ 1
- Odnowienie licencji pakietu UTM – typ 2

Szczegółowy opis przedmiotu zamówienia znajduje się w Załączniku Nr 1.

2.Termin wykonania zamówienia: 3 dni od otrzymania zlecenia drogą pisemną lub pocztą elektroniczną.

3.Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków:

- 1) Na podstawie w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tj. Dz.U. 2024 poz. 507) Zamawiający wykluczy Wykonawcę w stosunku do którego zachodzi którakolwiek z przesłanek określonych w niniejszej ustawie.

4. Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu:

- 1) Oświadczenie wykonawcy (zgodnie z formularzem oferty).

5. Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami:

- 1) Adres strony internetowej, na której udostępniane będą dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

https://szpitalpsychiatryczny.radom.pl/kategorie_zamowien/zamowienia-o-wartosci-powyzej-10-000-zlotych-do-130-000-zlotych/

- 2) Korespondencję związaną z Zaproszeniem do złożenia oferty (dalej zaproszenie) należy przekazywać na adres poczty elektronicznej iwona.nowak@szpitalpsychiatryczny.radom.pl
- 3) Osoby uprawnione do udzielania informacji po stronie Zamawiającego:
Iwona Nowak – sprawy formalne - tel. (48) 332-46-02
Piotr Gierczak – sprawy merytoryczne - tel. (48) 332-45-11;
- 4) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zaproszenia.
- 5) Zamawiający informuje, iż udzieli odpowiedzi na pytania wniesione co najmniej na 2 dni przed upływem terminu składania ofert. Jeżeli pytania wpłyną po tym terminie lub dotyczą udzielonych już wyjaśnień, lub nie dotyczą treści niniejszego zaproszenia Zamawiający może udzielić wyjaśnień lub pozostawić pytania bez odpowiedzi.
- 6) Wyjaśnienia będą stanowić integralną część zaproszenia.
- 7) Zamawiający zastrzega możliwość zmiany treści zaproszenia.
- 8) Wykonawca zobowiązany jest śledzić zaproszenie upublicznione na stronie internetowej zamawiającego w zakresie pytań i udzielonych odpowiedzi oraz wprowadzonych ewentualnych zmian.

6. Termin związania ofertą: Termin związania ofertą wynosi **30 dni** od upływu składania ofert.

7. Opis sposobu przygotowywania ofert: Opis sposobu przygotowywania ofert:

- 1) Ofertę należy sporządzić w języku polskim.
- 2) Oferta musi być zgodna z niniejszym zaproszeniem. Zaleca się wykorzystanie wzorów formularzy stanowiących załączniki do niniejszego zaproszenia.
- 3) Oferta oraz załączniki wymagają podpisu osób uprawnionych do reprezentowania Wykonawcy. Jeżeli Wykonawca składa ofertę poprzez ustanowionego pełnomocnika, Zamawiający wymaga załączenia do oferty stosownego pełnomocnictwa rodzajowego.
- 4) Ofertę należy złożyć w **formie pisemnej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym. Oferta nie podpisana lub nie opatrzona kwalifikowalnym podpisem elektronicznym lub podpisem zaufanym przez osobę uprawnioną zostanie odrzucona.**
- 5) Oferta i dokumenty stanowiące załączniki do oferty nie podlegają zwrotowi przez Zamawiającego.
- 6) Wykonawca może wycofać ofertę przed terminem składania ofert.
- 7) Zamawiający nie dopuszcza możliwości złożenia ofert częściowych.
- 8) Wykonawca może złożyć jedną ofertę. Złożenie więcej niż jednej oferty spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
- 9) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
- 10) Zamawiający poprawi w ofercie oczywiste omyłki rachunkowe i pisarskie.
- 11) **Oferta powinna zawierać:**
 - a) Ofertę wykonawcy – zgodnie z załączonym wzorem - Formularz oferty – Załącznik Nr 2;
 - b) W przypadku, gdy Wykonawcę reprezentuje pełnomocnik - pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy;

- c) Zamawiający przewiduje jednokrotne uzupełnienie dokumentów potwierdzających spełnianie warunków udziału w postępowaniu lub pełnomocnictwa.

8. Miejsce oraz termin składania ofert:

- 1) Ofertę należy złożyć do dnia **14.11.2025 roku do godz. 11:00**
- 2) Miejsce składania ofert:
 - a) W formie pisemnej: Samodzielny Wojewódzki Publiczny Zespół Zakładów Psychiatrycznej Opieki Zdrowotnej im. dr Barbary Borzym; 26-607 Radom ul. Krychnowicka 1 pok. 101 (Zamówienia publiczne)
 - Ofertę należy umieścić w kopercie, która będzie zaadresowana na adres Zamawiającego:
SAMODZIELNY WOJEWÓDZKI PUBLICZNY ZESPÓŁ ZAKŁADÓW PSYCHIATRYCZNEJ OPIEKI ZDROWOTNEJ im. dr Barbary Borzym; 26-607 Radom, ul. KRYCHNOWICKA 1
 - będzie posiadać oznaczenie: **Oferta - „Odnowienie licencji oprogramowania antywirusowego, odnowienie licencji UTM typ - 1 i UTM - typ - 2” – 23/REG/25**
 - b) w postaci elektronicznej na adres email:
iwona.nowak@szpitalpsychiatryczny.radom.pl
 - zaleca się by tytuł wiadomości zawierał oznaczenie: **Oferta - „Odnowienie licencji oprogramowania antywirusowego, odnowienie licencji UTM typ - 1 i UTM - typ - 2” - 23/REG/25**
 - sugerowane jest zaszyfrowanie pliku z ofertą i przesłanie hasła do otwarcia w kolejnym mailu w ciągu godziny po terminie składania ofert.
 - c) po otwarciu ofert Zamawiający udostępni na stronie internetowej informacje o nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte oraz cenach zawartych w ofertach.

9. Opis sposobu obliczenia ceny:

- 1) Podana w ofercie cena musi zawierać wszelkie koszty jakie poniesie Wykonawca z tytułu należytej, zgodnej z załączonym opisem przedmiotu zamówienia oraz zgodnej z obowiązującymi przepisami realizacji zamówienia.
- 2) Wykonawca zobowiązany jest pod rygorem odrzucenia oferty do wyszczególnienia wszystkich elementów ceny, tj. ceny jednostkowej netto PLN, wartości netto i brutto za wykonanie przedmiotu zamówienia PLN.
- 3) Kwoty wykazane w ofercie zaokrągla się do pełnych groszy (dwóch miejsc po przecinku), przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się do 1 grosza.
- 4) Cena oferty musi być podana liczbą.

10. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert:

Zamawiający dokona wyboru najkorzystniejszej oferty z najniższą ceną.

11. Istotne dla stron warunki zamówienia albo wzór umowy

- 1) Niniejsze zamówienie zostanie zrealizowane na podstawie pisemnego zlecenia w oparciu o opis przedmiotu zamówienia stanowiący Załącznik Nr 1.
- 2) Termin płatności - 30 dni od wystawienia faktury.

12. Wadium, o ile przewidziano: Zamawiający nie wymaga wniesienia wadium.

13. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego:

Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zamieszcza informację na swojej stronie internetowej.

14. Zamawiający zastrzega sobie prawo unieważnienia postępowania na każdym jego etapie bez podania przyczyny i Wykonawcy nie przysługują z tego tytułu żadne roszczenia.

15. Informacja dotycząca przetwarzania danych osobowych

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Samodzielny Wojewódzki Publiczny Zespół Zakładów Psychiatrycznej Opieki Zdrowotnej im. dr Barbary Borzym 26-607 Radom ul. Krychnowicka 1.
- 2) Kontakt z Inspektorem Ochrony Danych – Pan Ryszard Bryś tel.: 48 33 24 562, e-mail: ochronadanych@szpitalpsychiatryczny.radom.pl
- 3) Pani/Pana dane osobowe przetwarzane będą w celu realizacji ustawowych zadań urzędu – na podstawie art. 6 ust. 1 lit. C ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. oraz na podstawie art. 9 ust. 1 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r.
- 4) Odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
- 5) Pani/Pana dane osobowe przechowywane będą w czasie określonym przepisami prawa, zgodnie z instrukcją kancelaryjną.
- 6) Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania.
- 7) Ma Pani/Pan prawo do wniesienia skargi do organu nadzorczego.
- 8) Podanie danych osobowych w zakresie wymaganym ustawodawstwem (zgodnie z instrukcją kancelaryjną oraz Rozporządzeniem Prezesa Rady Ministrów z dnia 27 czerwca 2017r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych (Dz. U. z 2017 roku, poz. 1320) jest obligatoryjne.

FORMULARZ OFERTY_____
/nazwa wykonawcy/_____
/dokładny adres_____
/telefon/_____
/adres e-mail/

REGON _____

NIP _____

Zamawiający:
Samodzielny Wojewódzki
Publiczny Zespół Zakładów Psychiatrycznej Opieki
Zdrowotnej im. dr B. Borzym
ul. Krychnowicka 1, 26-607 Radom

Nawiązując do zaproszenia do złożenia oferty na: „**Odnowienie licencji oprogramowania antywirusowego, odnowienie licencji UTM typ 1 i UTM – typ 2**” - 23/REG/2025 przedkładamy niniejszą ofertę.

1. Deklarujemy wykonanie przedmiotu zamówienia za cenę:

Lp.	Przedmiot zamówienia (zgodnie z opisem przedmiotu zamówienia – zał. Nr 1 do n/n Zaproszenia)	Ilość	Cena jednostkowa netto w PLN	Wartość netto w PLN (cena jedn. x ilość)	Wartość brutto (z VAT) w PLN (wartość netto + VAT)
1	Oprogramowanie antywirusowe - licencje dla 260 stanowisk	260 szt.			
2	Odnowienie licencji pakietu UTM – typ 1	1 szt.			
3	Odnowienie licencji pakietu UTM – typ 2	1 szt.			
Razem					

2. Oświadczam, że zapoznaliśmy się z warunkami zamówienia określonymi w zaproszeniu wraz z załącznikami i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia

umowy zgodnej z niniejszą ofertą, na warunkach określonych w Zaproszeniu w miejscu i terminie wyznaczonym przez Zamawiającego

3. Oświadczam, że związani jesteśmy niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.
4. **Oświadczam, że nie podlegam wykluczeniu** z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

_____ dnia _____ r.

*(w formie pisemnej – podpis Wykonawcy;
w postaci elektronicznej - kwalifikowany podpis
elektroniczny lub podpis zaufany)*

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Oprogramowanie antywirusowe

Nazwa	Wymagania minimalne
Informacje ogólne	<p>Zamawiający posiada aktualnie pakiet ESET PROTECT Enterprise ON-PREM obowiązujący na 293 stanowiska z datą ważności licencji do dnia 18.11.2025 roku. W ramach wykonania zadania, Zamawiający wymaga zmniejszenia liczby wykorzystywanych stanowisk do 260 oraz przedłużenie ważności licencji na okres minimum do dnia 18.11.2026 roku lub dostarczenia licencji spełniającej wymagania równoważności na okres 1 roku.</p> <p>W przypadku dostarczenia licencji równoważnej, Zamawiający wymaga wdrożenia konsoli zarządzania antywirusa wraz z konfiguracją ustawień analogicznych do bieżących i instalacją agentów na komputerach użytkowników.</p>
Administracja zdalna	<ol style="list-style-type: none"> 1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS). 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej: <ol style="list-style-type: none"> a. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania, b. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta, c. Buforowanie ruchu HTTPS. 6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej. 8. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:

	<ul style="list-style-type: none"> a. Google Authenticator, b. Microsoft Authenticator, c. Authy, d. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania. <p>9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</p> <p>10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</p> <p>11. 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:</p> <ul style="list-style-type: none"> a. adresy sieciowe IP, b. aktywne zagrożenia, c. stan funkcjonowania oraz ochrony, d. wersja systemu operacyjnego, e. podzespoły komputera. <p>12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem</p> <ul style="list-style-type: none"> a. wyrażenie CRON, b. codziennie, c. cotygodniowo, d. co miesiąc, e. co rok, f. po wystąpieniu nowego zdarzenia, g. po automatycznym umieszczeniu hosta w grupie dynamicznej. <p>13. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim</p> <p>14. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania</p> <p>15. Rozwiązanie musi mieć możliwość tagowania obiektów.</p> <p>16. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.</p> <p>17. Eksport danych musi być możliwy w co najmniej następujących formatach:</p> <ul style="list-style-type: none"> a. JSON, b. LEEF, c. CEF.
<p>Ochrona stacji roboczych - Windows</p>	<ul style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

	<ol style="list-style-type: none">3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:<ol style="list-style-type: none">3.1. wirus,3.2. trojan,3.3. robak,3.4. adware,3.5. spyware,3.6. dialer,3.7. phishing,3.8. backdoor.4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.<ol style="list-style-type: none">7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:<ol style="list-style-type: none">10.1. całego dysku,10.2. wybranych katalogów,10.3. pojedynczych plików,
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none">10.4. plików spakowanych oraz skompresowanych,10.5. dysków sieciowych,10.6. dysków przenośnych. <p>11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:</p> <ul style="list-style-type: none">11.1. wybranych plików,11.2. wybranych procesów,11.3. wybranych lokalizacji,11.4. wybranych rozszerzeń,11.5. nazwy wykrycia,11.6. sumy kontrolnej (SHA1). <p>12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.</p> <p>13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:</p> <ul style="list-style-type: none">13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. <p>14. Rozwiązanie musi zapewniać 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).</p> <p>15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.</p> <p>16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

- 17.1.1. pamięci masowe,
- 17.1.2. optyczne pamięci masowe,
- 17.1.3. pamięci masowe Firewire,
- 17.1.4. urządzenia do tworzenia obrazów,
- 17.1.5. drukarki USB,
- 17.1.6. urządzenia Bluetooth,
- 17.1.7. czytniki kart inteligentnych,
- 17.1.8. modemy,
- 17.1.9. porty LPT/COM,
- 17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

- 17.2.1. numer seryjny,
- 17.2.2. producent,
- 17.2.3. model.

17.3. typ dostępu:

- 17.3.1. brak możliwości zapisu,
- 17.3.2. pełen dostęp,
- 17.3.3. ostrzeżenie użytkownika,
- 17.3.4. brak dostępu.

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

18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

18.4. 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

	<p>program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,</p> <p>18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</p> <p>19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.</p> <p>19.1. 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.</p> <p>19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.</p> <p>19.3. Raport musi posiadać co najmniej:</p> <ul style="list-style-type: none">19.3.1. Listę zainstalowanych aplikacji,19.3.2. Listę usług systemowych,19.3.3. Informacje o systemie operacyjnym i sprzęcie,19.3.4. Listę aktywnych procesów i połączeń sieciowych,19.3.5. Harmonogram systemu operacyjnego,19.3.6. Szczegóły pliku hosts,19.3.7. Informacje o sterownikach. <p>20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu</p> <ul style="list-style-type: none">20.1. antywirus,20.2. zapora osobista20.3. sandbox,20.4. antyspyware,20.5. metody heurystyczne. <p>21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
- 22.2. Ochrona musi być realizowana w oparciu o co najmniej:
- 22.1.1. globalna czarna lista RBL,
 - 22.1.2. czarna lista użytkownika,
 - 22.1.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 23.1.1. Skanowanie portów TCP oraz UDP,
 - 23.1.2. Wykrywanie duplikacji adresu IP,
 - 23.1.3. Atak zatruwania ARP,
 - 23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - 23.2.1. RDP,
 - 23.2.2. SMB,
 - 23.2.3. My SQL,
 - 23.2.4. MS SQL.
 - 23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
- 24.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
 - 24.2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 24.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 24.2.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

	<p>24.2.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,</p> <p>24.2.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.</p> <p>24.2.5. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.</p> <p>25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.</p> <p>25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.</p> <p>25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.</p> <p>26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.</p> <p>26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.</p> <p>26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:</p> <p>26.2.1. Treść komunikatu,</p> <p>26.2.2. Obraz.</p>
<p>Ochrona stacji roboczych – MacOS</p>	<p>1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.</p> <p>2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:</p> <p>3.1. wirus,</p> <p>3.2. trojan,</p> <p>3.3. robak,</p>

	<ul style="list-style-type: none">3.4. adware,3.5. spyware,3.6. dialer,3.7. phishing,3.8. backdoor. <p>4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.</p> <p>6. Rozwiązanie musi chronić pliki co najmniej za pomocą:</p> <ul style="list-style-type: none">6.1. Sygnatur wirusów.6.2. Reputacji chmurowej. <p>7. 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).</p> <p>8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:</p> <ul style="list-style-type: none">8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysłane do analizy. <p>9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:</p> <ul style="list-style-type: none">9.1. całego dysku,9.2. wybranych katalogów,9.3. pojedynczych plików,9.4. plików spakowanych oraz skompresowanych,
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>9.5. Dysków sieciowych, 9.6. dysków przenośnych.</p> <p>10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:</p> <p>10.1. wybranych plików, 10.2. wybranych procesów, 10.3. wybranych lokalizacji, 10.4. wybranych rozszerzeń, 10.5. nazwy wykrycia, 10.6. sumy kontrolnej (SHA1).</p> <p>11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.</p> <p>11.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.</p> <p>11.2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:</p> <p>11.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, 11.2.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,</p>
<p>Ochrona stacji roboczych – Linux</p>	<p>1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:</p> <p>1.1. Ubuntu Desktop, 1.2. Red Hat Enterprise Linux 1.3. Linux Mint.</p> <p>2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:</p> <p>2.1. Cinnamon, 2.2. GNOME, 2.3. KDE, 2.4. MATE, 2.5. XFCE.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:</p> <p>3.1. wirus, 3.2. trojan, 3.3. robak,</p>

	<ul style="list-style-type: none">3.4. adware,3.5. spyware,3.6. dialer,3.7. phishing,3.8. backdoor. <p>4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.</p> <p>6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwi co najmniej:</p> <ul style="list-style-type: none">6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. <p>7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:</p> <ul style="list-style-type: none">7.1. całego dysku,7.2. wybranych katalogów,7.3. pojedynczych plików,7.4. plików spakowanych oraz skompresowanych,7.5. dysków sieciowych,7.6. dysków przenośnych. <p>8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:</p> <ul style="list-style-type: none">8.1. wybranych plików,8.2. wybranych procesów,8.3. wybranych lokalizacji,8.4. wybranych rozszerzeń,
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:</p> <ul style="list-style-type: none"> 9.1. typ urządzenia: <ul style="list-style-type: none"> 9.1.1. pamięci masowe, 9.1.2. optyczne pamięci masowe, 9.2. parametry urządzenia: <ul style="list-style-type: none"> 9.2.1. numer seryjny, 9.2.2. producent, 9.2.3. model. 9.3. typ dostępu: <ul style="list-style-type: none"> 9.3.1. brak możliwości zapisu, 9.3.2. pełen dostęp, 9.3.3. brak dostępu.
<p>Ochrona serwera – Windows Server</p>	<ul style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy w tym co najmniej: <ul style="list-style-type: none"> 1.1. Microsoft Windows Server 2012 R2, 1.2. Microsoft Windows Server 2016, 1.3. Microsoft Windows Server 2019, 1.4. Microsoft Windows Server 2022, 1.5. Microsoft Windows Server 2025. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: <ul style="list-style-type: none"> 3.1. wirus, 3.2. trojan, 3.3. robak, 3.4. adware, 3.5. spyware, 3.6. dialer, 3.7. phishing, 3.8. backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość

wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwi co najmniej:

8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

9.1. całego dysku,

9.2. wybranych katalogów,

9.3. pojedynczych plików,

9.4. plików spakowanych oraz skompresowanych,

9.5. dysków sieciowych,

9.6. dysków przenośnych.

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

10.1. wybranych plików,

10.2. wybranych procesów,

10.3. wybranych lokalizacji,

10.4. wybranych rozszerzeń,

10.5. nazwy wykrycia,

10.6. sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

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

12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły

	<p>wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,</p> <p>12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,</p> <p>12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,</p> <p>12.4. 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,</p> <p>12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</p> <p>13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.</p> <p>13.1. 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.</p> <p>13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.</p> <p>13.3. Raport musi posiadać co najmniej:</p> <ul style="list-style-type: none">13.3.1. Listę zainstalowanych aplikacji,13.3.2. Listę usług systemowych,13.3.3. informacje o systemie operacyjnym i sprzęcie,13.3.4. Listę aktywnych procesów i połączeń sieciowych,13.3.5. harmonogram systemu operacyjnego,13.3.6. Szczegóły pliku hosts,13.3.7. Informacje o sterownikach.
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

- 14.1. antywirus,
- 14.2. zaporę osobistą
- 14.3. sandbox,
- 14.4. antyspyware,
- 14.5. metody heurystyczne.

15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

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

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

- 17.1.1. pamięci masowe,
- 17.1.2. optyczne pamięci masowe,
- 17.1.3. pamięci masowe Firewire,
- 17.1.4. urządzenia do tworzenia obrazów,
- 17.1.5. drukarki USB,
- 17.1.6. urządzenia Bluetooth,
- 17.1.7. czytniki kart inteligentnych,
- 17.1.8. modemy,
- 17.1.9. porty LPT/COM,
- 17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

- 17.2.1. numer seryjny,
- 17.2.2. producent,
- 17.2.3. model.

17.3. typ dostępu:

- 17.3.1. brak możliwości zapisu,
- 17.3.2. pełen dostęp,
- 17.3.3. ostrzeżenie użytkownika, 17.3.4. brak dostępu.

18. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:

	<ul style="list-style-type: none">18.1. MS SQL,18.2. Active Directory,18.3. IIS,18.4. Sysvol,18.5. DNS,18.6. DHCP,18.7. Hyper-V,18.8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego. <p>19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:</p> <ul style="list-style-type: none">19.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:<ul style="list-style-type: none">19.1.1. Skanowanie portów TCP oraz UDP,19.1.2. Wykrywanie duplikacji adresu IP,19.1.3. Atak zatruwania ARP,19.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.19.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:<ul style="list-style-type: none">19.2.1. RDP,19.2.2. SMB,19.2.3. My SQL,19.2.4. MS SQL.19.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. <p>20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.</p> <p>21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.</p> <ul style="list-style-type: none">21.1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:<ul style="list-style-type: none">21.1.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,21.1.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>21.1.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,</p> <p>21.1.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.</p> <p>21.1.5. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.</p>
<p>Ochrona serwera – Linux</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy w tym co najmniej: <ol style="list-style-type: none"> 1.1. RedHat Enterprise Linux (RHEL), 1.2. Rocky Linux, 1.3. Ubuntu, 1.4. Debian, 1.5. SUSE Linux Enterprise Server (SLES), 1.6. Oracle Linux, 1.7. Amazon Linux. 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: <ol style="list-style-type: none"> 2.1. wirus, 2.2. trojan, 2.3. robak, 2.4. adware, 2.5. spyware, 2.6. dialer, 2.7. phishing, 2.8. backdoor. 3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

6. Rozwiązanie musi posiadać możliwość wykluczenia ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwi co najmniej:
 - 7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 8.1. całego dysku,
 - 8.2. wybranych katalogów,
 - 8.3. pojedynczych plików,
 - 8.4. plików spakowanych oraz skompresowanych,
 - 8.5. dysków sieciowych,
 - 8.6. dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 9.1. wybranych plików,
 - 9.2. wybranych procesów,
 - 9.3. wybranych lokalizacji,
 - 9.4. wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
 - 10.1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. 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

	<p>przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.</p> <p>13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:</p> <ul style="list-style-type: none"> 13.1. proces budowania obrazu kontenera, 13.2. wdrażanie obrazu kontenera.
<p style="text-align: center;">Zarządzenie urządzeniami mobilnymi</p>	<ul style="list-style-type: none"> 1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania. <ul style="list-style-type: none"> 2.1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: <ul style="list-style-type: none"> 2.1.1. Android, 2.1.2. iOS, 2.1.3. iPadOS. 2.2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami: <ul style="list-style-type: none"> 2.2.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników), 2.2.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), 2.2.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), 2.2.4. Apple Business Manager (ABM), 2.2.5. Android Enterprise (co najmniej w zakresie Device Owner). 3. MDM musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: <ul style="list-style-type: none"> 3.1. usunięcie zawartości urządzenia, 3.2. przywrócenie urządzenia do ustawień fabrycznych, 3.3. zablokowanie urządzenia, 3.4. uruchomienie sygnału dźwiękowego,

	<ul style="list-style-type: none"> 3.5. lokalizację GPS, 3.6. Resetowanie hasła blokady ekranu. 4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 5. MDM musi umożliwiać co najmniej: <ul style="list-style-type: none"> 5.1. Dla systemów iOS oraz iPadOS <ul style="list-style-type: none"> 5.1.1. konfigurację kont e-mail, 5.1.2. konfigurację połączeń VPN, 5.1.3. Konfigurację połączeń Wi-Fi, 5.1.4. Konfigurację listy certyfikatów, 5.1.5. możliwość uruchomienia trybu jednej aplikacji. 5.2. Dla systemu Android: <ul style="list-style-type: none"> 5.2.1. blokadę wykonywania połączeń, 5.2.2. blokadę konfiguracji sieci Wi-Fi, 5.2.3. blokadę konfiguracji tuneli VPN, 5.2.4. zarządzanie aktualizacjami systemu operacyjnego, 5.2.5. blokadę zmiany tapety urządzenia.
<p>Mobile Threat Defense (MTD) dla systemu Android</p>	<ul style="list-style-type: none"> 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: <ul style="list-style-type: none"> 2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD. 2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej: <ul style="list-style-type: none"> 4.1. Złożoność kodu blokady ekranu: <ul style="list-style-type: none"> 4.1.1. Wzór, 4.1.2. PIN, 4.1.3. Hasło, 4.2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

	<ol style="list-style-type: none"> 4.3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu. 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: <ol style="list-style-type: none"> 5.1. nazwę aplikacji, 5.2. nazwę pakietu, 5.3. kategorię sklepu Google Play, 5.4. uprawnienia aplikacji, 5.5. pochodzenie aplikacji z nieznanego źródła. 6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.
<p style="text-align: center;">Sandbox w chmurze</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń. 2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. 3. Rozwiązanie musi wspierać systemy w tym co najmniej: <ol style="list-style-type: none"> 3.1. Microsoft Windows 10 oraz 11, 3.2. Microsoft Windows Server, 3.3. macOS 11 (Big Sur) oraz nowszych 3.4. RedHat Enterprise Linux (RHEL), 3.5. Rocky Linux, 3.6. Ubuntu, 3.7. Debian, 3.8. SUSE Linux Enterprise Server (SLES), 3.9. Oracle Linux, 3.10. Amazon Linux. 4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego. 6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej: <ol style="list-style-type: none"> 6.1. archiwa, 6.2. skrypty, 6.3. pliki wykonywalne, 6.4. pliki rejestru systemowego (.reg),

	<ul style="list-style-type: none">6.5. możliwy spam,6.6. dokumenty.7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:<ul style="list-style-type: none">7.1. natychmiast po ich przeanalizowaniu,7.2. po upływie 30 dni,7.3. nigdy.8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.12. Rozwiązanie pozwala na wystanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.<ul style="list-style-type: none">12.1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:<ul style="list-style-type: none">13.1. czysty,13.2. podejrzany,13.3. bardzo podejrzany,13.4. szkodliwy.14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:<ul style="list-style-type: none">14.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:<ul style="list-style-type: none">14.1.1. przeglądarki internetowe,14.1.2. programy poczty e-mail,
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>14.1.3. nośniki wymienne, 14.1.4. pliki wyodrębnione z archiwum.</p> <p>15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.</p>
<p>Szyfrowanie</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. 2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker. 3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego. 5. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. <ol style="list-style-type: none"> 5.1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia. 5.2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania. 6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania. <ol style="list-style-type: none"> 6.1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane. 6.2. Hasło odzyskiwania nie może być krótsze niż 8 znaków. 6.3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków. 7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. 8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania

	<p>(SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.</p> <p>9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.</p> <p>10. Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.</p> <p>11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.</p>
<p>Endpoint Detection and Response / eXtended Detection and Response</p>	<p>1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.</p> <p>2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.</p> <p>3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:</p> <ul style="list-style-type: none"> 3.1. tworzenie procesów, 3.2. uruchamianie, zatrzymanie i modyfikacja usług, 3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym, 3.4. usuwanie oraz zmiana nazw plików, 3.5. tworzenie i usuwanie kluczy rejestru systemowego, 3.6. ładowanie bibliotek DLL, 3.7. zalogowanie użytkowników, 3.8. elementy sieciowe, w tym co najmniej <ul style="list-style-type: none"> 3.8.1. pobranie plików wykonywalnych, 3.8.2. zestawienie połączeń TCP/IP, 3.8.3. zapytania HTTP, 3.8.4. zapytania DNS. <p>4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.</p> <p>4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:</p> <ul style="list-style-type: none"> 4.1.1. blokowanie pliku wykonywalnego, 4.1.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,

	<ul style="list-style-type: none">4.1.3. blokowanie podejrzanej biblioteki DLL,4.1.4. zakończenie procesu,4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,4.1.6. wyłączenie komputera,4.1.7. izolacja sieciowa hosta,4.1.8. wylogowanie użytkownika. <p>4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.</p> <p>5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.</p> <p>5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.</p> <p>5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:</p> <ul style="list-style-type: none">5.2.1. proces,5.2.2. proces nadrzędny (proces rodzica),5.2.3. nazwę procesu,5.2.4. ścieżkę procesu,5.2.5. wiersz polecenia,5.2.6. wydawcę,5.2.7. typ podpisu,5.2.8. SHA-1,5.2.9. SHA-2,5.2.10. użytkownika. <p>5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.</p> <p>6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.</p> <p>6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.</p> <p>6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):</p> <ul style="list-style-type: none">6.2.1. SHA-1,6.2.2. SHA-256. <p>7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

podglądu szczegółów wybranego pliku w tym przynajmniej:

- 7.1. hash pliku SHA-1,
 - 7.2. hash pliku SHA-256,
 - 7.3. hash pliku MD5,
 - 7.4. typ sygnatury podpisu cyfrowego,
 - 7.5. wydawcę certyfikatu,
 - 7.6. wersję pliku,
 - 7.7. oryginalną nazwę pliku,
 - 7.8. rozmiar pliku,
 - 7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,
 - 7.10. pierwsze uruchomienie pliku w środowisku,
 - 7.11. ostatnie uruchomienie pliku w środowisku,
8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
- 8.1. oznaczania ich jako bezpieczne lub niebezpieczne,
 - 8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 8.3. zablokowania wykonywania i wykorzystania pliku,
 - 8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
- 9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 - 9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
 - 9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

	<p>10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.</p> <p>10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.</p> <p>11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.</p> <p>12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Odnowienie licencji pakietu UTM typ 1

Nazwa	Wymagania minimalne
Wymagania ogólne	Zamawiający posiada aktualnie urządzenie UTM Stormshield SN720 z licencją UTM Security Pack + NBD ważną do dnia 6.12.2025 roku. W ramach wykonania zadania Zamawiający wymaga wykupienia licencji Essential Security Pack Oraz serwisu Next Business Day (wymiana urządzenia) na okres jednego roku lub dostarczenia urządzenia równoważnego wraz z licencjami i serwisem na jeden rok. W przypadku dostarczenia urządzenia równoważnego, Zamawiający wymaga wdrożenia UTM-a wraz z konfiguracją na nowym urządzeniu polityk bezpieczeństwa i innych ustawień znajdujących się na obecnie używanym urządzeniu. Opis równoważności znajduje się poniżej.
Obsługa sieci	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz

	<p>hybrydowo (częściowo jako router, a częściowo jako bridge).</p> <ol style="list-style-type: none"> 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
<p>Intrusion prevention system (ips)</p>	<ol style="list-style-type: none"> 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

	<ol style="list-style-type: none"> 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
<p style="text-align: center;">Kształtowanie pasma (traffic shapping)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
<p style="text-align: center;">Ochrona antywirusowa</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).

	<ol style="list-style-type: none"> 2. Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. 3. Skaner antywirusowy ma pochodzić od europejskiego producenta. 4. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 5. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: <ol style="list-style-type: none"> a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (vpn)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ol style="list-style-type: none"> a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

	<ol style="list-style-type: none"> 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPsec Policy Based oraz Route Based.
<p style="text-align: center;">Filtr dostępu do stron www</p>	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ol style="list-style-type: none"> a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
<p style="text-align: center;">Uwierzytelnianie</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ol style="list-style-type: none"> a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

	<ol style="list-style-type: none"> 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ol style="list-style-type: none"> a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. 10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
<p>Administracja łączami do internetu (isp)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ol style="list-style-type: none"> a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.

	<ol style="list-style-type: none"> 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przetączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przetączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.
Administracja urządzeniem	<ol style="list-style-type: none"> 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

6. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH).
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki hasła stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
 - a. manualnego eksportu do pliku w dowolnym momencie czasu,
 - b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

	<p>19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.</p> <p>20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.</p> <p>21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.</p>
<p>Raportowanie</p>	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
<p>Pozostałe usługi i funkcje</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

	<ol style="list-style-type: none"> 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć zaimplementowane Open API. 10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. 11. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
<p>Gwarancja i serwis</p>	<ol style="list-style-type: none"> 1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencją dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.
<p>Parametry sprzętowe</p>	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.

3. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.
4. Liczba portów światłowodowych 10Gbps – min. 2 z możliwością rozszerzenia do 6.
5. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
 - a. Moduł z 8 interfejsami miedzianymi 1Gbps.
 - b. Moduł z 4 interfejsami miedzianymi 10Gbps.
 - c. Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass).
 - d. Moduł z 8 interfejsami miedzianymi 2,5Gbps.
 - e. Moduł z 8 interfejsami światłowodowymi 1Gbps.
 - f. Moduł z 4 interfejsami światłowodowymi 10Gbps.
 - g. Moduł z 2 interfejsami światłowodowymi 25Gbps.
6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
7. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
8. Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps.
9. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps.
10. Przepustowość filtrowania Antywirusowego – minimum 3Gbps.
11. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps.
12. Liczba tuneli VPN IPSec – minimum 1 000.
13. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.
14. Obsługa interfejsów 802.11q (VLAN) – minimum 1336.
15. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
16. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive.
17. Urządzenie musi być wyposażone w moduł TPM
18. Urządzenie nie ma limitu na liczbę użytkowników.
19. Liczba reguł filtrowania – minimum 32 768.
20. Liczba tras statycznego routingu – minimum 5 120.
21. Liczba tras dynamicznego routingu – minimum 10 000.

	22. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.
--	---------------------------------------------------------------------

Odnowienie licencji pakietu UTM typ 2

Nazwa	Wymagania minimalne
Wymagania ogólne	Zamawiający posiada aktualnie urządzenie UTM Stormshield SN310 z licencją UTM Security Pack + NBD ważną do dnia 6.12.2025 roku. W ramach wykonania zadania Zamawiający wymaga wykupienia licencji Essential Security Pack oraz serwisu Next Business Day (wymiana urządzenia) na okres jednego roku lub dostarczenia urządzenia równoważnego wraz z licencjami i serwisem na jeden rok. W przypadku dostarczenia urządzenia równoważnego, Zamawiający wymaga wdrożenia UTM-a wraz z konfiguracją na nowym urządzeniu polityk bezpieczeństwa i innych ustawień znajdujących się na obecnie używanym urządzeniu. Opis równoważności znajduje się poniżej.
Obsługa sieci	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web

	<p>services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.</p> <ol style="list-style-type: none"> 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
<p style="text-align: center;">Intrusion prevention system (ips)</p>	<ol style="list-style-type: none"> 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall

	<p>dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.</p> <ol style="list-style-type: none"> 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
<p>Kształtowanie pasma (traffic shapping)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
<p>Ochrona antywirusowa</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania). 2. Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. 3. Skaner antywirusowy ma pochodzić od europejskiego producenta. 4. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 5. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

<p>Ochrona antyspam</p>	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: <ol style="list-style-type: none"> a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
<p>Wirtualne sieci prywatne (vpn)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ol style="list-style-type: none"> a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przetączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
<p>Filtr dostępu do stron www</p>	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ol style="list-style-type: none"> a. blokowanie dostępu do adresu URL,

	<ul style="list-style-type: none"> b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. <ol style="list-style-type: none"> 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
<p>Uwierzytelnianie</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ul style="list-style-type: none"> a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ul style="list-style-type: none"> a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co

	<p>najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).</p> <ol style="list-style-type: none"> 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. 10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
<p>Administracja łączy do internetu (isp)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ol style="list-style-type: none"> a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przetączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.
<p>Routing (trasowanie)</p>	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przetączenia na łączy zapasowe w przypadku awarii łączy podstawowego.

	<ol style="list-style-type: none"> 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.
<p style="text-align: center;">Administracja urządzeniem</p>	<ol style="list-style-type: none"> 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezasyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

	<p>12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).</p> <p>13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).</p> <p>14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.</p> <p>15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).</p> <p>16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.</p> <p>17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:</p> <ul style="list-style-type: none"> a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu <p>18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.</p> <p>19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.</p> <p>20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.</p>
<p>Raportowanie</p>	<p>1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</p> <p>2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.</p> <p>3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.</p> <p>4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.</p>

	<ol style="list-style-type: none"> 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
<p>Pozostałe usługi i funkcje</p>	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 7. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 8. Urządzenie musi mieć zaimplementowane Open API 9. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. 10. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
<p>Gwarancja i serwis</p>	<ol style="list-style-type: none"> 1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

	<ol style="list-style-type: none"> 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.
<p style="text-align: center;">Parametry sprzętowe</p>	<ol style="list-style-type: none"> 1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 3. Liczba portów Ethernet 2,5Gbps – min. 8. 4. Liczba portów światłowodowych 1Gbps – min. 1. 5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 6. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. 7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. 8. Przepustowość filtrowania Antywirusowego – minimum 1Gbps. 9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. 10. Liczba tuneli VPN IPSec – minimum 100. 11. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. 12. Obsługa interfejsów 802.11q (VLAN) – minimum 128 13. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. 14. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive. 15. Urządzenie nie ma limitu na liczbę użytkowników. 16. Liczba reguł filtrowania – minimum 8 192. 17. Liczba tras statycznego routingu – minimum 512.

	<p>18. Liczba tras dynamicznego routingu – minimum 10 000.</p> <p>19. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.</p> <p>20. Urządzenie musi być wyposażone w moduł TPM.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------