**Załącznik nr 2.1 do SWZ**

|  |
| --- |
| **MINIMALNE WYMAGANIA** |
| **Urządzenie sieciowe wraz z usługą wdrożenia i konfiguracji (5 sztuk)** | **Potwierdzenie spełniania przez oferowane dostawy wymagań Zamawiającego z kol. nr 1 i 2** |
| **Wymagania** |  |
| **1.** | **2.** | **3.** |
| Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje: | • Ilość portów 48 porty 1GBaseT, 4 x SFP oraz 2 x 10GBaseT niezależne• Chłodzenie od przodu do tyłu obudowy• Możliwość instalacji redundantnego zasilacza• Tablica MAC min. 16K• Tablica ARP/NDP min. 888• Bufor 16Mb• MTBF min. 578472 godzin• Wydajność min. 130,9 Mp/s• Przepustowość min. 176 Gb/s• Port USB• Port miniUSB• Port zarządzania Out-of-band;• Web GUI • HTTPs• CLI• Telnet • SSH• SNMP• MIB RSPAN• Radius• TACACS+• DiffServ• Możliwość łączenia w stos za pomocą interfejsów 10Gb/s• Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh• Non-stop forwarding (NSF)• Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram• IPv4/IPv6 Multicast filtering• IGMPv3 MLDv2 Snooping• ASM & SSM• IGMPv1,v2 Querier• Auto-VoIP• Auto-iSCSI• Policy-based routing (PBR)• LLDP-MED• Spanning Tree • Green Ethernet• STP• MTP• RSTP• PV(R)STP• BPDU/STRG Root Guard• EEE (802.3az)• GVRP/GMRP• Q in Q,• Private VLAN• DOT1X • MAB• Captive Portal• DHCP Snooping• Dynamic ARP • Inspection• IP Source Guard• CPU min 800 Mhz• Min 1GB RAM• Min 256MB Flash• Min ilość obsługiwanych VLAN 4K• OSPFv3 min. sąsiadów na interfejs 100• UDLD• LLPF• DHCPv6 Snooping• wysyłanie alertów na email• MMRP• Ilość ACL min. 100• Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu• Zasilacz z certyfikatem 80+• CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,• Class A, EN 61000-3-3:2013, EN 55024:2010• VCCI : VCCI-CISPR 32:2016, Class A• RCM: AS/NZS CISPR 32:2013 Class A• FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014• ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014• BSMI: CNS 13438 Class A | Tak\* Nie\* |
| Gwarancja | Wymaga się aby urządzenie było objęte gwarancją producenta **minimum 36 miesięcy** realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że urządzenia zostały wyprodukowane zgodnie z normami ISO9001, ISO14001 oraz posiadają znak CE – na potwierdzenie, że spełniają wszystkie stosowne wymagania prawne obowiązujące w UE, tj. wymagania dotyczące bezpieczeństwa, ochrony zdrowia czy środowiska naturalnego. | Tak\* Nie\* |
| **System kopii bezpieczeństwa wraz z usługą wdrożenia i konfiguracji (1 sztuka)** | **Potwierdzenie spełniania przez oferowane dostawy wymagań Zamawiającego z kol. nr 1 i 2** |
| **Wymagania** |
| **1.** | **2.** | **3.** |
|  | Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. | Tak\* Nie\* |
|  | Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 32TB netto. | Tak\* Nie\* |
|  | Oferowane urządzenie musi posiadać minimum * 2 porty Eth 10 Gb/s SFP+
* 1 port do zarządzania

wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle; | Tak\* Nie\* |
|  | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:* CIFS, NFS, deduplikacja na źródle – alternatywnie BOOST/OST/CATALYST
 | Tak\* Nie\* |
| 1.
 | **Wymagane jest dostarczenie licencji,** pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, BOOST/OST/CATALYST (alternatywnie) dla maksymalnej pojemności urządzenia (określonej w wymaganiach dot. skalowalności). | Tak\* Nie\* |
|  | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 4 TB/h (dane podawane przez producenta) oraz co najmniej 5 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta). | Tak\* Nie\* |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym * 50 dedykowanych do zapisu
* 50 dedykowanych do odczytu
* 40 dedykowanych do replikacji

wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. | Tak\* Nie\* |
|  | Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. | Tak\* Nie\* |
|  | Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. | Tak\* Nie\* |
|  | De-duplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości | Tak\* Nie\* |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, BOOST/OST/CATALYST) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. | Tak\* Nie\* |
|  | Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma (i więcej) udziałami NFS/CIFS w obrębie tego samego urządzenia. Blok danych otrzymany i zapisany na udziale A, nie może zostać ponownie zapisany jeśli trafi do udziału B w obrębie tego samego urządzenia. | Tak\* Nie\* |
|  | Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych. | Tak\* Nie\* |
|  | Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. | Tak\* Nie\* |
|  | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) | Tak\* Nie\* |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane jedną z metod do wyboru: gz, lz. | Tak\* Nie\* |
|  | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: oferowana aplikacja, Micro Focus Data Protector, VERITAS NetBackup, EMC NetWorker, EMC Avamar, Oracle RMAN, Microsoft SQL Server Management Studio, Veeam. | Tak\* Nie\* |
|  | W przypadku współpracy z każdą z poniższych aplikacji:* oferowana aplikacja backupowa
* RMAN (dla ORACLE)
* Microsoft SQL Server Management Studio (dla Microsoft SQL)
* VERITAS NetBackup
* Micro Focus Data Protector
* EMC NetWorker
* EMC Avamar
* Veeam

urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. De-duplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup’a / klienta Avamar / serwera RMAN / serwera SQL / klienta systemu NetWorker nie posiadającego licencji Storage Node.De-duplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. | Tak\* Nie\* |
|  | W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. | Tak\* Nie\* |
|  | Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane co najmniej z poziomu aplikacji VERITAS NetBackup, EMC NetWorker | Tak\* Nie\* |
|  | Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. | Tak\* Nie\* |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: \* jeden do jednego  \* wiele do jednego \* jeden do wielu \* kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.  | Tak\* Nie\* |
|  | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. | Tak\* Nie\* |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. | Tak\* Nie\* |
|  | W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: oferowana aplikacja backupowa/VERITAS NetBackup / Micro Focus Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:* replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
* replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu
* replikacja zarządzana jest z poziomu aplikacji backupowej
* aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
 | Tak\* Nie\* |
|  | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. | Tak\* Nie\* |
|  | Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%. | Tak\* Nie\* |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. | Tak\* Nie\* |
|  | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6. | Tak\* Nie\* |
|  | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). | Tak\* Nie\* |
|  | Urządzenie musi pozwalać na przechowywanie **minimum 300 Snapshotów** jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. | Tak\* Nie\* |
|  | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia). | Tak\* Nie\* |
|  | Urządzenie musi mieć możliwość podziału na minimum 4 logiczne części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 4 logicznych części pracujących równolegle z pełną wydajnością urządzenia. | Tak\* Nie\* |
|  | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. | Tak\* Nie\* |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:* CIFS
* NFS
* BOOST/OST/CATALYST
 | Tak\* Nie\* |
|  | Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. | Tak\* Nie\* |
|  | Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie:* systemu plików

oraz* grup RAID

Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu. | Tak\* Nie\* |
|  | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. | Tak\* Nie\* |
|  | Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy w locie.Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się „w locie” – musi być elementem procesu zapisu danych przez urządzenie. | Tak\* Nie\* |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.  | Tak\* Nie\* |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).  | Tak\* Nie\* |
|  | Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). | Tak\* Nie\* |
|  | Musi istnieć możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). | Tak\* Nie\* |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). | Tak\* Nie\* |
|  | Urządzenie musi mieć możliwość zarządzania poprzez* Interfejs graficzny dostępny z przeglądarki internetowej
* Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
 | Tak\* Nie\* |
|  | Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu de-duplikacyjnym.  | Tak\* Nie\* |
|  | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. | Tak\* Nie\* |
|  | Oferowane urządzenie powinno być objęte wsparciem producenta w okresie minimum 36 miesięcy, realizowanym w trybie 5x9 NBD. Urządzenie wyprodukowane, zgodnie z normą ISO 9001 oraz ISO 50001 – certyfikaty załączyć do oferty. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. | Tak\* Nie\* |
| **Urządzenie typu firewall UTM - Typ 2 wraz z usługą wdrożenia i konfiguracji (3 sztuki)** | **Potwierdzenie spełniania przez oferowane dostawy wymagań Zamawiającego z kol. nr 1 i 2** |
| **Wymagania:** |  |
| **1.** | **2.** | **3.** |
| Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System musi wspierać IPv4 oraz IPv6 w zakresie:• Firewall.• Ochrony w warstwie aplikacji.• Protokołów routingu dynamicznego. | Tak\* Nie\* |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.3. Monitoring stanu realizowanych połączeń VPN. | Tak\* Nie\* |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall musi dysponować minimum: 5 portami Gigabit Ethernet RJ-45.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.4. System musi być wyposażony w zasilanie AC. | Tak\* Nie\* |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. | Tak\* Nie\* |
| Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system | Tak\* Nie\* |
| Polityki, Firewall | 13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:• Translację jeden do jeden oraz jeden do wielu.• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.• Amazon Web Services (AWS).• Microsoft Azure • Google Cloud Platform (GCP).• OpenStack.• VMware NSX. | Tak\* Nie\* |
| Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:• Wsparcie dla IKE v1 oraz v2.• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).• Obsługa protokołu Diffie-Hellman grup 19 i 20.• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.• Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | Tak\* Nie\* |
| Routing i obsługa łączy WAN | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:• Routingu statycznego. • Policy Based Routingu.• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | Tak\* Nie\* |
| Funkcje SD-WAN | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | Tak\* Nie\* |
| Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | Tak\* Nie\* |
| Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | Tak\* Nie\* |
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | Tak\* Nie\* |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | Tak\* Nie\* |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | Tak\* Nie\* |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | Tak\* Nie\* |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | Tak\* Nie\* |
| Logowanie | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.4. Musi istnieć możliwość logowania do serwera SYSLOG. | Tak\* Nie\* |
| Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:• ICSA lub EAL4 dla funkcji Firewall. | Tak\* Nie\* |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy. | Tak\* Nie\* |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | Tak\* Nie\* |
| **Urządzenie typu firewall UTM - Typ 1 wraz z usługą wdrożenia i konfiguracji (1 sztuka)** | **Potwierdzenie spełniania przez oferowane dostawy wymagań Zamawiającego z kol. nr 1 i 2** |
| **Wymagania:** |  |
| **1.** | **2.** | **3.** |
| Wymagania Ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa Urządzenie typu firewall UTM - Typ 1 wraz z usługą wdrożenia i konfiguracji niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System wspiera protokoły IPv4 oraz IPv6 w zakresie:• Firewall.• Ochrony w warstwie aplikacji.• Protokołów routingu dynamicznego. | Tak\* Nie\* |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.3. Monitoring stanu realizowanych połączeń VPN.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. | Tak\* Nie\* |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 16 portami Gigabit Ethernet RJ-45.• 8 gniazdami SFP 1 Gbps.• 2 gniazdami SFP+ 10 Gbps.2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.4. System jest wyposażony w zasilanie AC. | Tak\* Nie\* |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | Tak\* Nie\* |
| Funkcje Systemu Bezpieczeństwa | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | Tak\* Nie\* |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:• Translację jeden do jeden oraz jeden do wielu.• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.• Amazon Web Services (AWS).• Microsoft Azure.• Cisco ACI.• Google Cloud Platform (GCP).• OpenStack.• VMware NSX.• Kubernetes. | Tak\* Nie\* |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:• Wsparcie dla IKE v1 oraz v2.• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).• Obsługa protokołu Diffie-Hellman grup 19, 20.• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.• Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. | Tak\* Nie\* |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:1. Routingu statycznego.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.6. BFD (Bidirectional Forwarding Detection).7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | Tak\* Nie\* |
| Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). | Tak\* Nie\* |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. System daje możliwość określania pasma dla poszczególnych aplikacji.3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. | Tak\* Nie\* |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | Tak\* Nie\* |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | Tak\* Nie\* |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). | Tak\* Nie\* |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. | Tak\* Nie\* |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | Tak\* Nie\* |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. | Tak\* Nie\* |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.4. Możliwość włączenia logowania per reguła w polityce firewall.5. System zapewnia możliwość logowania do serwera SYSLOG.6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. | Tak\* Nie\* |
| Certyfikaty | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:• ICSA lub EAL4 dla funkcji Firewall. | Tak\* Nie\* |
| Testy wydajnościowe oraz funkcjonalne | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. | Tak\* Nie\* |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy. | Tak\* Nie\* |
| Gwarancja oraz wsparcie | 1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | Tak\* Nie\* |

\* niepotrzebne skreślić