

Zestawienie tabelaryczne sprzętu informatycznego i oprogramowania dla części 1 - załącznik nr 8a

Gmina Rawicz
ul. Marszałka Józefa Piłsudskiego 21
63-900 Rawicz
Tel. 65 616 49 80
e-mail: umg@rawicz.eu

Opis Przedmiotu Zamówienia

**Dostawa sprzętu informatycznego i oprogramowania
w ramach projektu „Cyberbezpieczny Samorząd”
na potrzeby Gminy Rawicz
Część 1 – Dostawa Firewalli sieciowych**



SPIS TREŚCI

1.	FIREWALL SIECIOWY TYP 1 DLA URZĘDU GMINY W RAWICZU – WYMAGANIA MINIMALNE.....	3
2.	FIREWALL SIECIOWY TYP 2 DLA JEDNOSTKI PODLEGŁEJ (CENTRUM USŁUG SPOŁECZNYCH W RAWICZU) – WYMAGANIA MINIMALNE	9
3.	FIREWALL SIECIOWY TYP 3 DLA JEDNOSTEK PODLEGŁYCH (OŚRODEK SPORTU I REKREACJI W RAWICZU I ZAKŁAD USŁUG KOMUNALNYCH W RAWICZU) – WYMAGANIA MINIMALNE.....	15
4.	FIREWALL SIECIOWY TYP 4 DLA JEDNOSTEK PODLEGŁYCH (ZESPÓŁ SZKOLNO-PRZEDSZKOLNY W ZIELONEJ WSI I ZESPÓŁ SZKOLNO-PRZEDSZKOLNY W SŁUPI KAPITULNEJ) – WYMAGANIA MINIMALNE	21
5.	FIREWALL SIECIOWY TYP 5 DLA JEDNOSTEK PODLEGŁYCH (PRZEDSZKOLE NR 6 IM. PRZYJACIÓŁ KUBUSIA PUCHATKA W RAWICZU, PRZEDSZKOLE NR 5 „POD GRZYBKIEM” W RAWICZU I PRZEDSZKOLE NR 3 IM. KRASNALA HAŁABAŁY W RAWICZU) – WYMAGANIA MINIMALNE	27



1. Firewall sieciowy typ 1 dla Urzędu Gminy w Rawiczu – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	Firewall sieciowy typ 1 dla Urzędu Gminy w Rawiczu
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 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.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> 1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> • 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G/5G oraz instalacji oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie 2xAC.
Parametry wydajnościowe	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12.6 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 12 Gbps.

	<ol style="list-style-type: none"> 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 4.8 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 Gbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie musi posiadać 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).
Polityki, Firewall	<ol style="list-style-type: none"> 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: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 7. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
Połączenia VPN	<ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę 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.

	<ul style="list-style-type: none"> • 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. <p>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • 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 5.2. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi posiadać 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.
Routing i obsługa łącz WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ol style="list-style-type: none"> 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 RIPv2), 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.
Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR, .tar, .gz, .gzip, .7z. W przypadku archiwów zagnieżdżonych istnieje możliwość

	<p>określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</p> <ol style="list-style-type: none"> System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System musi współpracować 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. System musi zapewniać usuwanie aktywnej zawartości plików PDF, Libre Office, Open Office oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21). System musi mieć możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW	<ol style="list-style-type: none"> 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą 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 np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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, Bing oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • 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 musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać 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.
Zarządzanie	<ol style="list-style-type: none"> 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 dwuskładnikowego 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.

	<ol style="list-style-type: none"> 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
Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować 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 musi zapewniać 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: 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 24 miesiące.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesiące, 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.
Wdrożenie	<p>Wdrożenie musi obejmować minimum:</p> <ul style="list-style-type: none"> • Montaż w/w rozwiązania w sposób zgodny z zaleceniami producenta • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP

	<ul style="list-style-type: none"> • Konfiguracja klastra wysokiej dostępności <p>Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego rozwiązania.</p>
Ilość	1 szt.

2. Firewall sieciowy typ 2 dla Jednostki Podległej (Centrum Usług Społecznych w Rawiczu) – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	Firewall sieciowy typ 2 dla Centrum Usług Społecznych w Rawiczu
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastrer 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.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> 1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> • 10 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G/5G oraz instalacji oprogramowania z klucza USB. Z 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

	<ol style="list-style-type: none"> Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 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 1.3 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. Ochrona przed malware. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping). Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Rozwiązanie musi posiadać 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).
Polityki, Firewall	<ol style="list-style-type: none"> Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 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. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
Połączenia VPN	<ol style="list-style-type: none"> System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> Wsparcie dla IKE v1 oraz v2.

	<ul style="list-style-type: none"> • 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. •
Routing i obsługa łącz WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ol style="list-style-type: none"> 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 RIPv2), 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.
Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR, .tar, .gz, .gzip, .7z. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

	<ol style="list-style-type: none"> System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System musi współpracować 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. System musi zapewniać usuwanie aktywnej zawartości plików PDF, Libre Office, Open Office oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21). System musi mieć możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW	<ol style="list-style-type: none"> 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą 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 np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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, Bing oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • 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 musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać 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.
Zarządzanie	<ol style="list-style-type: none"> 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 dwuskładnikowego 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.

	<ol style="list-style-type: none"> 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
Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować 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 musi zapewniać 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: 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 24 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 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.
Wdrożenie	<p>Wdrożenie musi obejmować minimum:</p> <ul style="list-style-type: none"> • Montaż w/w rozwiązania w sposób zgodny z zaleceniami producenta • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Konfiguracja klastra wysokiej dostępności

Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego rozwiązania.

Ilość

1 szt.

3. Firewall sieciowy typ 3 dla Jednostek Podległych (Ośrodek Sportu i Rekreacji w Rawiczu i Zakład Usług Komunalnych w Rawiczu) – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	<p>Firewall sieciowy typ 3 dla:</p> <ul style="list-style-type: none"> Ośrodek Sportu i Rekreacji w Rawiczu Zakład Usług Komunalnych w Rawiczu
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> 5 portami Gigabit Ethernet RJ-45. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G/5G oraz instalacji oprogramowania z klucza USB. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none"> W zakresie Firewall'a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

	<ol style="list-style-type: none"> 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 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 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie musi posiadać 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).
Polityki, Firewall	<ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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.
Połączenia VPN	<ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

	<ul style="list-style-type: none"> • 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.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ol style="list-style-type: none"> 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 RIPv3), 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.
Funkcje SD-WAN	<p>System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR, .tar, .gz, .gzip, .7z. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

	<ol style="list-style-type: none"> System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System musi współpracować 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. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). System musi mieć możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	<ol style="list-style-type: none"> Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

	<ol style="list-style-type: none"> 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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, Bing oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • 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 musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać 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.
Zarządzanie	<ol style="list-style-type: none"> 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 dwuskładnikowego 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

Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować 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 musi zapewniać 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: 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 24 miesiące.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesiące, 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.
Wdrożenie	<p>Wdrożenie musi obejmować minimum:</p> <ul style="list-style-type: none"> • Montaż w/w rozwiązania w sposób zgodny z zaleceniami producenta • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Konfiguracja klastra wysokiej dostępności <p>Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego rozwiązania.</p>
Ilość	2 szt.

4. Firewall sieciowy typ 4 dla Jednostek Podległych (Zespół Szkolno-Przedszkolny w Zielonej Wsi i Zespół Szkolno-Przedszkolny w Słupi Kapitulnej) – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	<p>Firewall sieciowy typ 4 dla:</p> <ul style="list-style-type: none"> Zespół Szkolno-Przedszkolny w Zielonej Wsi Zespół Szkolno-Przedszkolny w Słupi Kapitulnej
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G/5G oraz instalacji oprogramowania z klucza USB. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none"> W zakresie Firewall'a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 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.

	<ol style="list-style-type: none"> 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zaporę ogniową klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie musi posiadać 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).
Polityki, Firewall	<ol style="list-style-type: none"> 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: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 7. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
Połączenia VPN	<ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę 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.

	<ul style="list-style-type: none"> • 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.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ol style="list-style-type: none"> 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.
Funkcje SD-WAN	<p>System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR, .tar, .gz, .gzip, .7z. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy

	<p>typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <ol style="list-style-type: none"> System musi zapewniać usuwanie aktywnej zawartości plików PDF, Libre Office, Open Office oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). System musi mieć możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	<ol style="list-style-type: none"> Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

	<ol style="list-style-type: none"> 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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, Bing oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 6. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	<ol style="list-style-type: none"> 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 dwuskładnikowego 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
Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci

	<p>odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <ol style="list-style-type: none"> 2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>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 24 miesięcy.</p>
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 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.
Wdrożenie	<p>Wdrożenie musi obejmować minimum:</p> <ul style="list-style-type: none"> • Montaż w/w rozwiązania w sposób zgodny z zaleceniami producenta • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Konfiguracja klastra wysokiej dostępności <p>Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego rozwiązania.</p>
Ilość	2 szt.

5. Firewall sieciowy typ 5 dla Jednostek Podległych (Przedszkole nr 6 im. Przyjaciół Kubusia Puchatka w Rawiczu, Przedszkole nr 5 „Pod Grzybkiem” w Rawiczu i Przedszkole nr 3 im. Krasnala Hałabały w Rawiczu) – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
Typ	<p>Firewall sieciowy typ 5 dla:</p> <ul style="list-style-type: none"> Przedszkole nr 6 im. Przyjaciół Kubusia Puchatka w Rawiczu Przedszkole nr 5 „Pod Grzybkiem” w Rawiczu Przedszkole nr 3 im. Krasnala Hałabały w Rawiczu
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa muszą 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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> 5 portami Gigabit Ethernet RJ-45. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G/5G oraz instalacji oprogramowania z klucza USB. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none"> W zakresie Firewall’a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.

	<ol style="list-style-type: none"> 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 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie musi posiadać 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).
Polityki, Firewall	<ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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.
Połączenia VPN	<ol style="list-style-type: none"> 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

	<ul style="list-style-type: none"> • 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. •
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ol style="list-style-type: none"> 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.
Funkcje SD-WAN	<p>System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR, .tar, .gz, .gzip, .7z. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy

	<p>typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <ol style="list-style-type: none"> System musi zapewniać usuwanie aktywnej zawartości plików PDF, Libre Office, Open Office oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). System musi mieć możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	<ol style="list-style-type: none"> Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

	<ol style="list-style-type: none"> 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać 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, Bing oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • 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 musi dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System musi umożliwiać 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.
Zarządzanie	<ol style="list-style-type: none"> 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 dwuskładnikowego 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
Logowanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci

	<p>odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <ol style="list-style-type: none"> 2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: 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 24 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 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.
Wdrożenie	<p>Wdrożenie musi obejmować minimum:</p> <ul style="list-style-type: none"> • Montaż w/w rozwiązania w sposób zgodny z zaleceniami producenta • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Konfiguracja klastra wysokiej dostępności <p>Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis skonfigurowanych opcji wdrożonego rozwiązania.</p>
Ilość	3 szt.