Szczegółowy opis przedmiotu zamówienia

1. Informacje ogólne

1. Niniejsza specyfikacja określa wymagania funkcjonalne i techniczne w zakresie dostawy urządzeń informatycznych dla Starostwa Powiatowego w Gliwicach.
2. Przedmiotem zamówienia dostawa urządzeń UTM z aktualizacjami, aktualizacje dla urządzeń sieciowych oraz szkolenie.

2. Wykaz dostaw, instalacji i konfiguracji

Mając na uwadze charakter przetargu Zamawiający w tabelach od nr 4.1 do nr 4.6 przyporządkował cechy urządzeń, aktualizacji i szkolenia będących przedmiotem niniejszego postępowania, które szczegółowo opisane zostały w dalszej części niniejszego załącznika do SWZ. Dodatkowo w poniższej tabeli nr 1 zawarto informację na temat liczby urządzeń jakie Wykonawca będzie zobligowany dostarczyć po podpisaniu z Zamawiającym umowy, której wzór jest integralną częścią SWZ.

Plan wdrożenia:

1. Wykonawca przygotuje i omówi koncepcję konfiguracji z administratorem sieci Zamawiającego.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogram dostawy i montażu.
3. Wdrożenia nowych urządzeń UTM musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu przełączniki, Active Directory) będących w posiadaniu Zamawiającego. Dodatkowo każda zmiana w koncepcji musi być każdorazowo uzgadniana z administratorem sieci.
4. Wykonawca zamontuje urządzenia w szafie rack Zamawiającego uwzględniając wszelkie aspekty związanie z montażem tego typu urządzeń przewidzianych przez producenta dostarczanych rozwiązań.
5. Wdrożenie klastra HA firewalli na styku z siecią Internet w zakresie minimum:
    a. rejestracja i aktualizacja do najnowszej stabilnej wersji OS (o ile wymagane jest to przez producenta),
    b. podłączenie i konfiguracja redundantnego łącza WAN,
    c. konfiguracja routingu,

d. konfiguracja polityk bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu) zgodnie z wytycznymi ze strony Zamawiającego,
e. konfiguracja filtracji stron WWW na podstawie kategorii oraz treści,
f. integracja firewall`a z systemem autoryzacji Microsoft Active Directory w trybie transparentnym lub przy użyciu dedykowanych agentów, tak aby możliwa była identyfikacja użytkowników,
g. konfiguracja, dostępu zdalnego SSL VPN (VPN Client, portal WebVPN) dla 10 kont,
h. integracja systemu firewall z istniejącym systemem do gromadzenia logów SysLog oraz SIEM,
i. integracja systemu firewall z dostarczanymi przełącznikami,
j. integracja systemu firewall z posiadanymi przełącznikami Zamawiającego.

6. Wykonawca dodatkowo skonfiguruje dla dwóch administratorów logowanie do systemu z wykorzystaniem MFA. Zamawiający dopuszcza wykorzystanie ścieżki: Email, sms, token.
7. Wykonawca omówi z Zamawiającym stan końcowy konfiguracji, przedstawi zmiany naniesione na urządzeniu i w porozumieniu z Zamawiającym dopracuje szczegółowość konfiguracji.
8. Przeprowadzenie szkolenia trwające 2 dni dla 4 administratorów min. 12 godzin łącznie zakończone certyfikatem lub zaświadczeniem wystawionym przez Wykonawcę w zakresie:
    a. Firewall konfiguracja:
        i. Polityki firewall
        ii. Polityki ochrony DOS
        iii. Zarządzanie pasmem
    b. Profile utm konfiguracja:
        i. Antivirus
        ii. Web filter
        iii. Dns filter
        iv. Application control
        v. Interusion prevention
    c. VPN konfiguracja:
        i. SSL-VPN
        ii. IPSEC dialup
        iii. IPSEC SITE-TO-SITE
    d. Logowanie / alertowanie / debugowanie
9. Przekazanie dokumentacji powdrożeniowej.

<u>Wymagania ogólne dla wszystkich urządzeń informatycznych:</u>

- wszystkie oferowane urządzenia muszą być fabrycznie nowe i wyprodukowane nie wcześniej

niż w III kwartale 2023 roku,

- urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych,
- do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w formie papierowej lub elektronicznej,
- urządzenia muszą posiadać serwis gwarancyjny zgodny z opisem dla poszczególnych urządzeń,
- wszystkie urządzenia zostaną dostarczone z niezbędnym okablowaniem zasilającym i transmisyjnym,
- wszystkie dostarczone w ramach niniejszego postępowania urządzenia muszą zostać zarejestrowane przez Wykonawcę.

Tabela 1. Przyporządkowanie cech technicznych

Lp	Urządzenie/Usługa	Liczba sztuk	Cecha
1	2	3	4
1	Fortinet FortiGate 400F lub równoważne	2	A
2	Fortinet FortiSwitch 1024E lub równoważne	1	B
3	Fortinet FortiSwitch 148F lub równoważne	4	C
4	Fortinet FortiAP 431F lub równoważne	2	D
5	Aktualizacje dla posiadanych urządzeń FortiSwitch i punktów dostępowych FortiAP	1	E
6	Szkolenie	1	F

3. Wymagania co do gwarancji i obsługi serwisowej

Szczegółowy zakres gwarancji został ujęty w pkt. 4 Szczegółowego Opisu Przedmiotu Zamówienia i w Umowie.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy. Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji. Parametry równoważności zostały zaprezentowane niżej, w stosunku do każdego urządzenia.

4. Minimalne wymagania stawiane dla poszczególnych urządzeń i oprogramowania

4.1 Urządzenie typu UTM - Cecha A

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Ogólne	System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia. System realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych fizycznych instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Wszystkie funkcje i parametry wydajnościowe systemu muszą mieć możliwość weryfikacji w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
2	Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewniać funkcję synchronizacji sesji. System musi posiadać funkcję monitoringu w zakresie minimum: - wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, - stan realizowanych połączeń VPN. System musi również umożliwiać statyczną agregację linków oraz w oparciu o protokół LACP. Dodatkowo musi istnieć możliwość tworzenia interfejsów redundantnych.

3	Interfejsy, Dysk, Zasilanie	System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: • 18 portami Gigabit Ethernet RJ-45. • 6 gniazdami SFP 1 Gbps. • 6 gniazdami SFP+ 10 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G 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 musi być wyposażony w zasilanie AC.
4	Wydajność	W zakresie Firewall'a obsługa nie mniej niż 7.3 mln jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall nie mniej niż 77 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji nie mniej niż 26 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 51 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 11 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 8,9 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http minimum 7.2 Gbps.

5	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 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. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie 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).

6	Polityki, Firewall	1. Polityka Firewall musi uwzględniać co najmniej: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi umożliwiać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. System musi zapewniać możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Musi istnieć możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

7	VPN	Musi istnieć możliwość konfiguracji połączeń typu IPSec VPN. W tym zakresie musi być zapewniona funkcjonalność: • Wsparcie dla IKE v1 oraz v2. • Obsługa 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. Dodatkowo musi istnieć możliwość konfigurowania połączeń typu SSL VPN. W zakresie tej funkcji musi być zapewniona funkcjonalność: • Praca w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Praca 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.
8	Routing i obsługa łączy	W zakresie routingu rozwiązanie musi zapewniać obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9	SD-WAN	1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

10	Zarządzanie pasmem	1. System Firewall musi zapewniać możliwość zarządzania pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Dodatkowo system musi mieć możliwość: - określania pasma dla poszczególnych aplikacji. - zdefiniowania pasma dla wybranych użytkowników niezależnie od ich adresu IP. - zarządzania pasmem dla wybranych kategorii URL.
11	Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. 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. 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 typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System musi zapewniać możliwość usuwania aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Musi istnieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Musi istnieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

12	Ochrona przed atakami	1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 16 000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. System musi posiadać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. System musi posiadać możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. System musi zapewniać wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. System musi umożliwiać uruchomienie ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
13	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 5000 sygnatur podzielonych na minimum 20 kategorii i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur oraz blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 6. System musi posiadać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

14	Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 60 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 kategorie 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 mieć możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. System musi oferować funkcję Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google 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.
15	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą minimum: • 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 mieć 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. Musi istnieć możliwość uwierzytelniania w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

16	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System musi posiadać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Musi istnieć możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM) oraz możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17	Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze jak i w postaci komercyjnego systemu logowania i raportowania 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 musi zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Musi istnieć możliwość włączenia logowania dla wybranej reguły w polityce firewall. 5. System musi mieć możliwość logowania do serwera SYSLOG oraz zewnętrznych systemów z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

18	Gwarancja, serwis techniczny, licencje	1. Urządzenie musi być objęty licencją do korzystania z aktualnych baz funkcji ochronnych producenta systemu i serwisów w zakresie: 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, DLP, skanowanie inline w trybie proxy na okres 24 miesięcy. 2. Licencją muszą być objęte wszystkie instancje fizyczne systemu. 3. Urządzenie 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. 4. Dostarczone urządzenie musi być objęty wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego partnera na okres wymaganej gwarancji. 5. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: 5.1. obsługa procesu RMA u producenta, 5.2. zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, 5.3. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 5.4. doradztwo w zakresie konfiguracji. 5.5. zdalne wsparcie techniczne. 5.6. pomoc w zakładaniu zgłoszeń serwisowych u producenta. 5.7. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). 6. Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (należy podać adres oraz numery telefonów).

4.2 Urządzenie typu switch 1 – Cecha B

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Ogólne	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa.
2	Parametry fizyczne platformy	Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. - Zasilanie AC 230V. - Wymagany - z możliwością wymiany w czasie pracy - redundantny zasilacz. - Maksymalny pobór mocy: 180 W. - Minimalny zakres temperatury pracy: 0-40°C.
3	Interfejsy sieciowe	Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: - 24 porty 10 GE SFP+ - 2 porty 100 GE QSFP28
4	Zarządzanie	- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. - Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. - Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). - Wsparcie dla SNMP w wersjach 1-3. - Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. - Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. - Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. - Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). - Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. - Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. - Automatycznie wykonywane rewizje konfiguracji.
5	Wydajność	- Przepustowość urządzenia - min. 880 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1300 Mpps. - Tablica adresów MAC o pojemności co najmniej 64 k wpisów. - Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

6	Funkcje	- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. - Obsługa Jumbo Frames. - Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). - Agregacja portów zgodna ze standardem 802.3ad. - Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. - Obsługa routingu statycznego. - Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. - Port-mirroring. - Uwierzytelnianie 802.1x na poziomie portu. - Uwierzytelnianie 802.1x w oparciu o adres MAC. - W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN). - W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. - W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. - Obsługa protokołu sFlow.
7	Dodatkowe funkcje urządzenia przy integracji z systemem nadrzędnego zarządzania	Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: - Centralne zarządzanie konfiguracją urządzenia. - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania. - Centralne zarządzanie sieciami VLAN. - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u. - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. - Automatyczna detekcja i rekomendacje konfiguracji. - Przesyłanie logów na zewnętrzny serwer syslog. - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. - Obsługa białych i czarnych list adresów MAC. - Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

8	Gwarancja, serwis techniczny	1. Urządzenie 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. 2. Dostarczone urządzanie musi być objęty wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego partnera na okres wymaganej gwarancji. 3. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: 3.1. obsługa procesu RMA u producenta, 3.2. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 3.3. doradztwo w zakresie konfiguracji. 3.4. zdalne wsparcie techniczne. 3.5. pomoc w zakładaniu zgłoszeń serwisowych u producenta. 3.6. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). 4. Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (należy podać adres oraz numery telefonów).

4.3 Urządzenie typu switch 2 - Cecha C

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Ogólne	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
2	Parametry fizyczne platformy	1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: a. Temperatura 0–45°C, b. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: a. 2.4 GHz 802.11b/g/n, b. 5 GHz 802.11a/n/ac/ax, c. Skaner 2.4GHz i 5GHz 4. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
3	Interfejsy sieciowe	Urządzenie musi być wyposażone w min dwa interfejsy Ethernet a. 10/100/1000 Base-TX, b. 10/100/1000/2500 Base-TX
4	Funkcje	Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: a. Tunnel, b. Bridge, c. Mesh. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). Interfejs radiowy urządzenia powinien wspierać następujące funkcje: a. MIMO – 4x4, b. Maksymalna przepustowość dla poszczególnych modułów radiowych: - 1147 Mbps; - 2402 Mbps; c. Wymagana moc nadawania: - min. 24 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; - min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; d. Wsparcie dla 802.11n 20/40Mhz HT, e. Wsparcie dla kanałów 80 i 160 MHz, f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz. g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, h. Maksymalna deklarowana liczba klientów per moduł radiowy: 512

5	Funkcje dodatkowe	a. OFDMA UL i DL b. Spatial Reuse (BSS Coloring) c. HE-MU-MIMO d. UL-MU-MIMO 802.11ax e. DL-MU-MIMO f. Enhanced Target Wake Time (TWT)
6	Gwarancja, serwis techniczny	1. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte 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. 2. Dostarczone urządzenie musi być objęty wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego partnera na okres wymaganej gwarancji. 3. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: 3.1. obsługa procesu RMA u producenta, 3.2. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 3.3. doradztwo w zakresie konfiguracji. 3.4. zdalne wsparcie techniczne. 3.5. pomoc w zakładaniu zgłoszeń serwisowych u producenta. 3.6. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). 4. Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (należy podać adres oraz numery telefonów).

4.4 Urządzenie typu access point - Cecha D

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Ogólne	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
2	Parametry fizyczne platformy	1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: a. Temperatura 0–45°C, b. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: a. 2.4 GHz 802.11b/g/n, b. 5 GHz 802.11a/n/ac/ax, c. Skaner 2.4GHz i 5GHz 4. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
3	Interfejsy sieciowe	Urządzenie musi być wyposażone w min dwa interfejsy Ethernet a. 10/100/1000 Base-TX, b. 10/100/1000/2500 Base-TX
4	Funkcje	Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: a. Tunnel, b. Bridge, c. Mesh. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). Interfejs radiowy urządzenia powinien wspierać następujące funkcje: a. MIMO – 4x4, b. Maksymalna przepustowość dla poszczególnych modułów radiowych: - 1147 Mbps; - 2402 Mbps; c. Wymagana moc nadawania: - min. 24 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; - min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; d. Wsparcie dla 802.11n 20/40Mhz HT, e. Wsparcie dla kanałów 80 i 160 MHz, f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz. g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, h. Maksymalna deklarowana liczba klientów per moduł radiowy: 512

5	Funkcje dodatkowe	a. OFDMA UL i DL b. Spatial Reuse (BSS Coloring) c. HE-MU-MIMO d. UL-MU-MIMO 802.11ax e. DL-MU-MIMO f. Enhanced Target Wake Time (TWT)
6	Gwarancja, serwis techniczny	1. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte 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. 2. Dostarczone urządzenie musi być objęty wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego partnera na okres wymaganej gwarancji. 3. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: 3.1. obsługa procesu RMA u producenta, 3.2. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 3.3. doradztwo w zakresie konfiguracji. 3.4. zdalne wsparcie techniczne. 3.5. pomoc w zakładaniu zgłoszeń serwisowych u producenta. 3.6. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). 4. Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (należy podać adres oraz numery telefonów).

4.5 Aktualizacje dla posiadanych FortiSwitch i punktów dostępowych FortiAP – Cecha E

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Posiadane urządzenia	1. FortiSwitch o numerach seryjnych: 1.1. S448ENTF20000974, 1.2. S448ENTF20000971, 1.3. S148EN5919000381, 1.4. S148EP5920000348, 1.5. S148EP5919001780, 1.6. S148EN5919002068, 1.7. S148EN5919002660, 1.8. S148EN5919000419, 1.9. S148EN5919002925, 2. FortiAP o numerach seryjnych: 2.1. FP221ETF18094183 2.2. FP421ETF18013261, 2.3. FP421ETF18013270
2	Aktualizacja, gwarancja, serwis techniczny	1. Urządzenia muszą być objęte serwisem gwarancyjnym producenta przez okres 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. 2. Urządzenia muszą być objęte wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego partnera na okres wymaganej gwarancji. 3. Dla urządzeń Wykonawca zapewni usługi wsparcia technicznego w języku polskim w zakresie: 3.1. obsługa procesu RMA u producenta, 3.2. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 3.3. doradztwo w zakresie konfiguracji. 3.4. zdalne wsparcie techniczne. 3.5. pomoc w zakładaniu zgłoszeń serwisowych u producenta. 3.6. pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). 4. Dostęp do usługi powinien być świadczony przez dedykowane numery telefonu oraz przez dedykowany moduł internetowy (należy podać adres oraz numery telefonów).

4.6 Szkolenie – Cecha F

L.P.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
1	2	3
1	Ogólne	3. 2-dniowe szkolenia (12 godzin lekcyjnych) 4. Szkolenie ma zostać przeprowadzone dla 4 osób 5. Szkolenie uwzględniające informacje z zakresu wdrożonych urządzeń wraz z tematami i umiejętności jakie zdobędzie uczestnik: 5.1. firewall konfiguracja 5.1.1. polityki firewalla, 5.1.2. polityki ochrony DOS, 5.1.3. zarządzanie pasmem, 5.2. Profile UTM konfiguracja: 5.2.1.Antivirus, 5.2.2. Web filter, 5.2.3. DNS filter, 5.2.4.Application control, 5.2.5. Intrusion prevention, 5.3. VPN konfiguracja: 5.3.1. SSL-VPN, 5.3.2. IPSEC DIALUP, 5.3.3. IPSEC SITE-TO-SITE, 5.4. Logowanie / alertowanie / debugowanie 6. Szkolenie musi być przeprowadzone w języku polskim. 7. Szkolenie może być realizowane online wraz z wygenerowanym certyfikatem lub zaświadczeniem ukończenia dla każdego uczestnika szkolenia.

Opracował:

Łukasz Szyszko

_____

(imię i nazwisko)