

SPECYFIKACJA TECHNICZNA – OPIS PRZEDMIOTU ZAMÓWIENIA

ZADANIE 1 - Dostawa, instalacja i konfiguracja urządzeń sieciowych oraz osprzętu sieciowego dla jednostek podległych Zamawiającego

Przełącznik sieciowy 48-portowy **w konfiguracji minimalnej** jak podano w pkt **I** – 1 sztuka;

Przełącznik sieciowy 24-portowy **w konfiguracji minimalnej** jak podano w pkt **II** – 3 sztuki;

Przełącznik sieciowy 8-portowy **w konfiguracji minimalnej** jak podano w pkt **III** – 2 sztuki;

Kontroler zarządzania siecią **w konfiguracji minimalnej** jak podano w pkt **IV** – 2 sztuki;

Acces Point PoE typ A **w konfiguracji minimalnej** jak podano w pkt **V** – 4 sztuk;

Acces Point PoE typ B **w konfiguracji minimalnej** jak podano w pkt **VI** – 6 sztuk;

Wzmacniacz sygnału sieci WiFi **w konfiguracji minimalnej** jak podano w pkt **VII** – 6 sztuk;

Router UTM **w konfiguracji minimalnej** jak podano w pkt **VIII** - 1 sztuka;

I – Przełącznik sieciowy 48-portowy

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Typ obudowy	- Obudowa rack, przeznaczona do montażu w szafie 19", wraz z akcesoriami niezbędnymi do montażu
B	Porty	- min. 48 portów RJ-45 10/100/1000 z automatycznym wykrywaniem szybkości (10BASE-T typu IEEE 802.3, 100BASE-TX typu IEEE 802.3u, 1000BASE-T typu IEEE 802.3ab) - min. 2 porty SFP+ 10GBE - min. 1 port konsoli RJ-45
C	Wydajność przełącznika	- pojemność pamięci wewnętrznej – min. 512 MB - wielkość pamięci flash – min. 256 MB - przepustowość rutowania/przełączania – min. 176 Gbps - prędkość przekazywania – min. 130 Mpps - pojemność tabeli MAC – min. 16000 adresów - obsługa Jumbo Frames - pamięci bufora pakietów – min. 3 MB
D	Zarządzanie	- SNMP ver. 1- 3 - RMON - Telnet - HTTP - HTTPS - SSH - CLI

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

E	Standardy komunikacyjne	<ul style="list-style-type: none"> - IEEE 802.3 10BASE-T Ethernet - IEEE 802.3u 100BASE-TX Fast Ethernet - IEEE 802.3ab 1000BASE-T Gigabit Ethernet - IEEE 802.3bz 2.5GBase-T and 5GBase-T - IEEE 802.3ad Link Aggregation Control Protocol - IEEE 802.3z Gigabit Ethernet - IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN - IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable - IEEE 802.3x Flow Control - IEEE 802.1D (STP, GARP and GVRP) - IEEE 802.1Q/p VLAN - IEEE 802.1w Rapid STP - IEEE 802.1s Multiple STP - IEEE 802.1X Port Access Authentication - IEEE 802.3af - IEEE 802.3at - IEEE 802.1AB Link Layer Discovery Protocol - IEEE 802.3az Energy Efficient Ethernet,
F	Dodatkowe wyposażenie	<p>2 szt. listwy zasilającej do montażu w szafie RACK 19" o następujących parametrach:</p> <ul style="list-style-type: none"> - złącza wyjściowe z uziemieniem kołkowym min. 6 sztuk – możliwe zastosowanie adapterów - możliwość wyłączania i włączania pojedynczych gniazd - minimalne gwarantowane obciążenie 10A - zarządzanie listwą poprzez interfejs www, - port sieciowy LAN (port RJ45) - elementy niezbędne do montażu w szafie RACK
G	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu. - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.

II – Przełącznik sieciowy 24-portowy

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Typ obudowy	- Obudowa rack, przeznaczona do montażu w szafie 19", wraz z akcesoriami niezbędnymi do montażu
B	Porty	- min. 24 porty RJ-45 10/100/1000 - min. 2 porty SFP
C	Specyfikacja, pamięć	- Algorytm przełączania – Store-and-forward - Przepustowość – min. 52 Gbps - Bufor pakietów – min. 2Mb
D	Standardy i protokoły	- IEEE 802.3 Ethernet - IEEE 802.3i 10BASE-T - IEEE 802.3u 100BASE-T - IEEE 802.3ab 1000BASE-T - IEEE 802.1Q VLAN Tagging - IEEE 802.3x Full-Duplex Flow Control - IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX - IEEE 802.3ae 10-Gigabit Ethernet - IEEE 802.3ad Trunking (LACP) - IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED) - IEEE 802.1p Class of Service - IEEE 802.1D Spanning Tree (STP) - IEEE 802.1s Multiple Spanning Tree (MSTP) - IEEE 802.1w Rapid Spanning Tree (RSTP) - IEEE 802.1x Radius network access control
E	Zarządzanie	- SNMP ver. 1- 3 - RMON - HTTPS - SSL - Zarządzanie pasmem - Wsparcie dla IPv6 - Port Mirroring - Syslog
F	Dodatkowe cechy przełącznika dla warstwy 2 i 3	- Statyczny routing - DHCP Snooping

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> - DHCP Client - LAGs - Broadcast Storm Control - IGM Snooping (1/2/3) - Blokowanie nieznanymi transmisji multicast - LACP
H	Okablowanie	<ul style="list-style-type: none"> - kabel zasilający - patchcord RJ-45 kat.6 3m – 5szt. (szary lub biały) - patchcord RJ-45 kat.6 0,5m – 26szt. (szary lub biały)
I	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu. - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.

III – Przełącznik sieciowy 8-portowy

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Typ przełącznika	- zarządzalny
B	Porty	<ul style="list-style-type: none"> - liczba portów Ethernet RJ-45 (10/100/1000) – min. 8szt. - liczba portów PoE – min. 4szt. - obciążenie realizowane przez 4 porty PoE min. 50W - obciążalność zasilania jednego portu PoE min.30W, przy podłączonym jednym urządzeniu PoE,
C	Standardy komunikacyjne	- IEEE 802.3at
D	Przepustowość przełączania	- min. 8 Gbit/s

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

E	Kompatybilność	- 100% kompatybilność z kontrolerem z pkt IV nin. specyfikacji
F	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu. - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.

IV – Kontroler zarządzania siecią

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Typ urządzenia	- urządzenie typu kontroler sieciowy
B	Pamięć i wydajność	<ul style="list-style-type: none"> - min. 3 GB RAM - min. 32 GB Pamięci FLASH - min. 1 TB pamięci masowej (SATA) - procesor min. 8 rdzeni
C	Standardy komunikacyjne	- IEEE 802.3af
D	Rodzaje wejść/wyjść:	- min. 1 port RJ-45 1GBE (LAN)
E	Dodatkowe informacje	- Zasilanie USB, PoE
F	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu.</p> <ul style="list-style-type: none"> - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.
--	--	--

V – Access Point PoE typ A

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Tryb pracy	- Access point
B	Typ obudowy	<ul style="list-style-type: none"> - Możliwość montażu na ścianie lub suficie - Zastosowanie: wewnątrz pomieszczenia - wbudowane anteny
C	Standard	<ul style="list-style-type: none"> - Standard WiFi - 802.11 a/b/g - Standard szyfrowania - WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)
D	Porty	- min. 1 port LAN 1GbE
E	Funkcje i parametry pracy	<ul style="list-style-type: none"> - częstotliwość pracy: 2.4 GHz, 5 GHz - standard - 802.1Q - moc anteny – min. 2 dBi
F	Zasilanie	- PoE
G	Kompatybilność	- 100% kompatybilność z kontrolerem z pkt IV nin. specyfikacji
H	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.
--	--	--

VI – Access Point PoE typ B

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Tryb pracy	- Access point
B	Typ obudowy	<ul style="list-style-type: none"> - możliwość montażu na ścianie lub suficie - zastosowanie: wewnątrz pomieszczenia
C	Porty	- LAN 10/100/1000 – min. 2szt.
D	Funkcje i parametry pracy	<ul style="list-style-type: none"> - częstotliwość pracy: 2.4 GHz, 5 GHz - standard WiFi - 802.11b/g/n, 802.11a/n/ac - obsługa szyfrowanej transmisji - antena – wbudowana - moc anteny – min. 2 dBi
E	Zasilanie	- PoE
F	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu. - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.

VII – Wzmacniacz sygnału sieci WiFi

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia Wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Typ urządzenia	<ul style="list-style-type: none"> - wzmacniacz sygnału sieci bezprzewodowej do instalacji w gnieździe elektrycznym 230V, - wzmacniacz musi udostępniać gniazdo elektryczne, - podłączony wzmacniacz nie może zmniejszać dostępnych gniazd elektrycznych w miejscu instalacji
B	Standardy i protokoły	- IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
C	Porty	- 1 x 10/100Mbps Ethernet Port (RJ45)
D	Przyciski	- Przycisk do automatycznej konfiguracji urządzenia – poprzez WPS, Przycisk Reset
E	Antena	- Zewnętrzne anteny – 2szt.
F	Prędkość transmisji	<ul style="list-style-type: none"> - dla 11n: min. 250 Mb/s (dynamicznie) - dla 11g: min. 50 Mb/s (dynamicznie) - dla 11b: min. 10 Mb/s (dynamicznie)
G	Bezpieczeństwo transmisji bezprzewodowej	- 64/128/152-bitowe szyfrowanie WEP, WPA-PSK / WPA2-PSK
H	Zasilanie wejściowe	- 230V 50/60Hz
I	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> - Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. - Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonego sprzętu. - Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. - Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób jednostki podległej Zamawiającego.

VIII – Zintegrowana platforma bezpieczeństwa – UTM

Lp.	Nazwa składnika/parametru technicznego sprzętu	Główne elementy przedmiotu zamówienia, wymagania jakościowe w zakresie składników i parametrów technicznych sprzętu, tj. co najmniej:
A	Wymagania Ogólne	<ul style="list-style-type: none"> System UTM musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizując funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: routera NAT, transparentnej bramy oraz pracy w trybie monitorowania na porcie SPAN. System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. System musi wspierać protokoły IPv4 oraz IPv6 w zakresie: funkcjonalności Firewall, funkcjonalności ochrony w warstwie aplikacji, funkcjonalności protokołów routingu dynamicznego.
B	Redundancja, monitoring i wykrywanie awarii	<ul style="list-style-type: none"> Dla możliwości przyszłej rozbudowy urządzenie musi umożliwiać dla funkcjonalności: Firewall, IPSec, Kontrola Aplikacji oraz IPS – łączenie z innym (takim samym urządzeniem) w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewniać funkcję synchronizacji sesji. Zaproponowane rozwiązanie musi realizować funkcje: <ul style="list-style-type: none"> monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych, monitoringu stanu realizowanych połączeń VPN, agregacji linków: statyczną oraz w oparciu o protokół LACP, tworzenia interfejsów redundantnych.
C	Interfejsy, Dysk, Zasilanie	<ul style="list-style-type: none"> Ilość dostępnych interfejsów: 10 Gigabit Ethernet RJ-45, co najmniej jeden wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G lub instalacji oprogramowania z klucza USB. Minimalna ilość interfejsów wirtualnych: 200, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
D	Parametry wydajnościowe	<ul style="list-style-type: none"> Obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz co najmniej 35 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6.5 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu - minimum 1.4 Gbps. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus – co najmniej 700 Mbps. Minimalna wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – co najmniej 630 Mbps.
E	Funkcje Systemu Bezpieczeństwa	<p>W celu realizacji funkcji bezpieczeństwa, oferowany system musi udostępniać wszystkie poniższe funkcjonalności:</p> <ul style="list-style-type: none"> kontrola dostępu - zaporę ogniową klasy Stateful Inspection, kontrola Aplikacji,

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> – 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. W ramach realizacji tego zadania, Wykonawca dostarczy co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane w celu realizacji dwu-składnikowego uwierzytelnienia dla 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, – funkcjonalność realizująca procesy automatyzacji zadań, polegające na wykonaniu określonej sekwencji akcji (takich jak np. zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
F	Polityki systemu Firewall	<ul style="list-style-type: none"> – Polityki Firewall'a muszą realizować co najmniej takie właściwości jak: adresy IP, użytkowników i grupy użytkowników, protokoły, usługi sieciowe, aplikacje i zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. – Translacja adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu, dedykowany ALG (Application Level Gateway) dla protokołu SIP. – System musi umożliwiać: <ul style="list-style-type: none"> • tworzenie wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN, • wykorzystywanie w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, • tworzenie polityk firewall umożliwiających filtrowanie ruchu w zależności od kraju, z którego pochodzi ruch lub do którego ruchu jest kierowany, • ustalenia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. • Firewallowi integracje z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
G	Połączenia VPN	<ul style="list-style-type: none"> – System musi realizować konfigurację połączeń typu IPSec VPN w zakresie co najmniej: <ul style="list-style-type: none"> • wsparcia dla IKE v1 oraz v2, • obsługi szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), • obsługi protokołu Diffie-Hellman grup 19, 20, • wsparcia dla pracy w topologii Hub and Spoke oraz Mesh, • tworzenia połączeń typu Site-to-Site oraz Client-to-Site, • monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności, • wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, • wsparcia dla uwierzytelniania: pre-shared key, certyfikat,

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> • ustalenia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, • monitorowania wybranego tunelu IPSec site-to-site - a w przypadku jego niedostępności - automatycznego aktywowania zapasowego tunelu, • obsługi mechanizmów: IPSec NAT Traversal, DPD, Xauth, • mechanizmu „Split tunneling” dla połączeń Client-to-Site. <p>– System musi realizować konfigurację połączeń typu SSL VPN w zakresie co najmniej:</p> <ul style="list-style-type: none"> • realizacji dostępu w trybie „portal” - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki, w celu obsługi tego trybu system musi zapewniać realizację takiego portalu ‘www’ w oparciu o HTML 5.0, • realizacji dostępu w trybie „tunnel” z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta VPN, <p>– Producent dostarczonego rozwiązania musi posiadać wspierane i aktualizowane oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN i SSL VPN. W procesie realizacji niniejszego zamówienia nie jest wymagane dostarczenie oprogramowania klienckiego VPN.</p>
H	Routing i obsługa łącz WAN	<p>– W zakresie routingu zaproponowane rozwiązanie musi zapewnić obsługę:</p> <ul style="list-style-type: none"> • routingu statycznego, • Policy Based routingu, w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP, • protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM, • filtrowania tras rozgłaszanych w protokołach dynamicznego routingu, • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu, • wykorzystania protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.
I	Zarządzanie pasmem	<p>– System musi zapewnić zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu, a także określania pasma dla poszczególnych aplikacji, urządzeń oraz użytkowników.</p>
J	Ochrona przed malware	<p>– Rozwiązanie musi być wyposażone w silnik antywirusowy umożliwiający skanowanie ruchu w obu kierunkach komunikacji dla protokołów HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS; skanowanie musi uwzględniać także komunikację na tych protokołach na innych niż standardowe porty.</p> <p>– System musi pozwalać na:</p> <ul style="list-style-type: none"> • skanowanie archiwów, w tym co najmniej: Zip, RAR; w przypadku archiwów zagnieżdżonych, musi istnieć parametr do określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości, • blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. <p>– Baza sygnatur antywirusowych i bezpieczeństwa musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora urządzenia.</p>

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> – System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. – System musi posiadać funkcjonalność zapewniającą usuwanie aktywnej zawartości w plikach pdf oraz plikach doc, docx, xls, xlsx bez konieczności blokowania transferu całych plików. – System musi umożliwiać wykorzystanie silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta dostarczanego rozwiązania. – System musi pozwalać na uruchomienie ochrony przed malware dla wybranego zakresu ruchu. – System musi dysponować sygnaturami do ochrony urządzeń mobilnych, co najmniej dla systemu operacyjnego typu Android.
K	Ochrona przed atakami	<ul style="list-style-type: none"> – System musi być wyposażony w funkcjonalność ochrony IPS opartej co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych także dla aplikacji i protokołów pracujących na niestandardowych portach. – Producent urządzenia zapewnia stale aktualizowaną bazę sygnatur ataków, która musi zawierać minimum 5000 wpisów, a jej aktualizacja na urządzeniu musi przebiegać automatycznie, zgodnie z harmonogramem definiowanym przez administratora urządzenia. – Dostarczony system musi zapewnić administratorowi urządzenia możliwość definiowania własnych wyjątków oraz własnych sygnatur stosowanych na tym urządzeniu. – Dostarczony system zapewni wykrywanie anomalii protokołów i ruchu sieciowego i umożliwi ochronę przed atakami typu DoS oraz DDoS. – System musi dostarczać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym na poziomie co najmniej ochrony przed: CSS, SQL Injecton, Trojany, Exploity, Roboty. – System musi umożliwiać: <ul style="list-style-type: none"> • parametryzację w zakresie kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http, • wykrywanie i blokowanie komunikacji C&C do sieci botnet, – System musi pozwolić na uruchomienie ochrony przed atakami dla wybranych zakresów komunikacji sieciowej, mechanizmy ochrony IPS nie mogą działać globalnie.
L	Kontrola aplikacji	<ul style="list-style-type: none"> – System musi być wyposażony w funkcję kontroli aplikacji, która umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. – Baza sygnatur aplikacji dla systemu kontroli aplikacji musi zawierać minimum 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora urządzenia, dostępna baza sygnatur musi zawierać kategorie aplikacji szczególnie ważne ze względu na bezpieczeństwo np.: aplikacje służące do realizacji p2p lub proxy. – Aplikacje chmurowe - co najmniej: Facebook, Google Docs, Dropbox – muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. – Administrator urządzenia musi mieć możliwość definiowania wyjątków oraz tworzenia własnych sygnatur stosowanych na urządzeniu.
M	Kontrola WWW	<ul style="list-style-type: none"> – System musi być wyposażony w funkcję filtra ruchu WWW, który korzysta z bazy sygnatur zawierającej co najmniej 40 milionów adresów URL pogrupowanych na kategorie tematyczne odpowiadające treściom skatalogowanym.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> – Dla realizacji zawartości bazy sygnatur filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, co najmniej: malware (kategoria URL będących źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. – Filtr WWW musi dostarczać również kategorie stron zabronionych prawem oraz powszechnie nieakceptowane, tj. co najmniej: hazard, handel bronią, pornografia, handel narkotykami, hacking. – System musi umożliwiać administratorowi urządzenia na nadpisywanie kategorii oraz tworzenie wyjątków a także statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym definiowanie reguł w oparciu o mechanizm wyrażeń regularnych (Regex). – Konfiguracja reguł filtra WWW musi umożliwiać ustalenie dla kategorii wykonania akcji typu „ostrzeżenie” dla użytkownika wchodzącego na zasoby przyporządkowane do tej kategorii wymagające od niego potwierdzenia informacji ostrzegawczej przed otwarciem żądanej strony. – System musi umożliwić administratorowi urządzenia definiowania komunikatów zwracanych użytkownikom w oparciu o akcje podejmowanych przez moduł filtrowania WWW. – System musi pozwalać na określenie, dla których kategorii URL lub dla jakich wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
N	Uwierzytelnianie użytkowników w ramach sesji	<ul style="list-style-type: none"> – System musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej: <ul style="list-style-type: none"> • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia, • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. – System musi pozwalać na konfigurację mechanizmu uwierzytelniania dwuskładnikowego. – System musi realizować architekturę uwierzytelniania typu Single Sign On co najmniej do technologii Active Directory. – Dostarczony system musi posiadać wsparcie dla realizacji uwierzytelniania w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
O	Zarządzanie systemem	<ul style="list-style-type: none"> – Dostarczone w rozwiązaniu elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, oraz muszą mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. – Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. – System musi posiadać możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. – System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach co najmniej: 2c, 3 oraz powinien umożliwić przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. – Dostarczony system musi udostępniać możliwość zarządzania nim przez systemy firm trzecich za pomocą dostarczanego API, do którego producent urządzenia udostępnia dokumentację.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none"> – Element systemu pełniący funkcję firewall'a musi posiadać: <ul style="list-style-type: none"> • wbudowane narzędzia diagnostyczne, co najmniej: ping, traceroute, narzędzia do podglądu pakietów, narzędzia do monitorowania procesowania sesji oraz stanu sesji firewall'a, • konfiguracji systemu przez administratora za pomocą CLI oraz GUI. – System musi posiadać wbudowany system uprawnień pozwalający nadawać i przypisywać różnym administratorom urządzenia prawa do zarządzania określonymi częściami systemu (RBM) oraz możliwość ograniczenia zarządzania systemem tylko ze wskazanych adresów źródłowych IP.
P	Logowanie	<ul style="list-style-type: none"> – System musi posiadać funkcjonalność realizującą logowanie pracy systemu i działania wszystkich jego modułów w tym ruchu sieciowego i stosowanych polityk zabezpieczeń. Logowanie może się odbywać do aplikacji lokalnej lub do udostępnianej w chmurze, a także przekierowania logów do innej platformy wspierającej SYSLOG lub do wielu serwerów logowania. – Proces logowania zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowaniu ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Logowanie musi obejmować także: <ul style="list-style-type: none"> • zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa funkcjonujących na urządzeniu, • logowanie per reguła w polityce firewall. • przesyłanie SYSLOG do zewnętrznych systemów musi mieć możliwość transmisji w formie zaszyfrowanej, uniemożliwiającej jej podsłuchanie.
R	Instalacja, konfiguracja, testy	<ul style="list-style-type: none"> – Całość sprzętu zostanie dostarczona, zainstalowana, uruchomiona, skonfigurowana i przetestowana przez Oferenta w systemie teleinformatycznym jednostki podległej Zamawiającego. – Oferent zapewni odpowiednio wykwalifikowany personel niezbędny do poprawnego i pełnego wdrożenia, konfiguracji, uruchomienia i przetestowania poprawności działania dostarczonej platformy. – Oferent zobowiązuje się zainstalować, skonfigurować i uruchomić dostarczony sprzęt w sposób umożliwiający jego pełne wykorzystanie w infrastrukturze jednostki podległej Zamawiającego oraz jednocześnie w sposób nie wpływający negatywnie na System Teleinformatyczny jednostki podległej Zamawiającego. – Wszelkie prace konfiguracyjne i przyłączeniowe nowych komponentów będą się odbywać pod nadzorem, w konsultacji i po akceptacji osób wskazanych do nadzoru nad wdrożeniem z jednostki podległej Zamawiającego.
S	Gwarancja oraz wsparcie	<ul style="list-style-type: none"> – System musi być objęty serwisem gwarancyjnym producenta urządzenia przez okres co najmniej 12 miesięcy. Serwis i wsparcie producenta musi realizować naprawy lub wymianę urządzenia w przypadku problemów z poprawnym działaniem sprzętu. W ramach tego serwisu producent musi zapewnić dostęp do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Informacje dodatkowe dot. specyfikacji sprzętu:

Do urządzeń muszą być dołączone wszystkie niezbędne dokumenty takie jak instrukcja obsługi, gwarancja, deklaracja zgodności oraz wszystkie nośniki z oprogramowaniem, sterownikami dodawanymi do sprzętu.

Każde urządzenie powinno mieć nadany przez dostawcę unikalny numer, który pozwoli na jednoznaczne zidentyfikowanie takiego urządzenia w razie np.: awarii lub serwisu, numer powinien zostać przyklejony lub nadrukowany na urządzeniu.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

W zamówieniu oferowany może być jedynie sprzęt i oprogramowanie fabrycznie nowe, nigdzie nieużywane poza oczywistą sytuacją związaną z jego testowaniem.

W zamówieniu musi być oferowany sprzęt dopuszczony do sprzedaży w Polsce i na terenie UE, posiadający ważną deklarację CE. W przypadkach odniesienia do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych zamawiający dopuszcza rozwiązania równoważne z opisywanym.