Załącznik nr 1 - Opis przedmiotu zamówienia

Zamówienie obejmuje dostawę sprzętu oraz konfigurację i wdrożenie urządzeń typu utm i firewall dla systemów bezpieczeństwa IT/OT wraz ze świadczeniem usług towarzyszących w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Zakład Komunalny w Pobiedziskach Spółka z o.o.

W sytuacjach gdy w OPZ użyte zostały nazwy własne, znaki towarowe, nazwy producentów, produktów, technologii lub wskazano rozwiązania referencyjne, to takie wskazanie należy rozumieć jako określenie funkcjonalności lub poziomu technicznego oczekiwanego rozwiązania. Zamawiający dopuszcza rozwiązania równoważne, spełniające wymagania funkcjonalne i techniczne oraz zapewniające kompatybilność i bezpieczeństwo z zachowaniem wydajności określone w OPZ. Wykonawca oferujący rozwiązanie równoważne musi wykazać jego równoważność na podstawie dokumentacji producenta lub innych wiarygodnych danych.

W związku z planowanym wdrożeniem rozwiązań w obszarze cyberbezpieczeństwa, Zamawiający wymaga, aby wszystkie wdrażane systemy, usługi oraz procesy były zgodne z dobrymi praktykami zarządzania usługami IT opartymi na metodyce ITIL.

Zastosowanie standardów ITIL wiąże się z:
- zachowaniem powtarzalnego modelu zarządzania usługami IT,
- zapewnieniem cyklu życia wdrażanych rozwiązań,
- zapewnieniem wysokiej jakości świadczenia usług oraz ich zgodności z wymaganiami organizacyjnymi i prawnymi (ustawa o KSC, zgodność z NIS2),
- zagwarantowaniem poprawnej integracji wdrażanych rozwiązań z istniejącą infrastrukturą i procesami Zamawiającego.

Wdrożenie systemów cyberbezpieczeństwa wymaga stosowania ustandaryzowanego podejścia do zarządzania usługami IT. Brak takiego działania może prowadzić do rozwiązań

niespójnych i wykazujących podatność na błędy co finalnie wpływa na poziom bezpieczeństwa oraz ciągłość działania organizacji.

Zakres zamówienia w zakresie IT

LP.	NAZWA	SPECYFIKACJA
1	Urządzenie UTM	Zadanie 1
2	Macierz dyskowa z dyskami	Zadanie 2
3	Serwer NAS (network attached storage) z dyskami	Zadanie 3
4	Zasilacz awaryjny	Zadanie 4
5	Wdrożenie urządzenia UTM	Zadanie 5
6	Przełącznik zarządzalny	Zadanie 6
7	Opłata za subskrypcje ochronne do urządzenia UTM	Zadanie 7
8	Access point Wi-Fi	Zadanie 8
9	Firewall sieciowy	Zadanie 9

Zadanie 1: Urządzenie UTM

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia UTM.
2	Opis	Zapewniona funkcjonalność SD-WAN zapewniająca optymalizację połączeń, łącząc bezpieczeństwo sieci i zarządzanie ruchem, co zwiększa wydajność. Wymagana technologia firewall nowej generacji (NGFW) oferująca zaawansowaną ochronę przed zagrożeniami, blokująca nieautoryzowany dostęp i zapewniając głęboką inspekcję ruchu SSL. Funkcja IPS (Intrusion Prevention System), identyfikująca i blokująca zagrożenia w czasie rzeczywistym. Wbudowane kontrole aplikacji, pozwalające administratorom na monitorowanie i zarządzanie użyciem aplikacji w sieci. Wsparcie połączenia VPN, umożliwiając bezpieczny zdalny dostęp do zasobów organizacyjnych. zagrożeń. Wsparcie dla Zero Trust, co pozwala na zwiększone bezpieczeństwo w złożonych środowiskach IT.

		Możliwość centralnego zarządzania politykami i konfiguracjami.Urządzenie typu next-generation firewall (NGFW) i SD-WAN.
3	Wymagania Ogólne	System bezpieczeństwa realizuje 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. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
4	Redundancja, monitoring i wykrywanie awarii	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.
5	Interfejsy, Dysk, Zasilanie:	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.

		System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
6	Parametry wydajnościowe:	W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 90 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 3.4 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.3 Gbps. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.2 Gbps.
7	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa 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. 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. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
8	Polityki, Firewall	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: adresy 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. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

9	Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
10	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: Routingu statycznego. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. Możliwość 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.
11	Funkcje SD-WAN	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
12	Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
13	Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.

		System zapewnia 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.
14	Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 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.
15	Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

		System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
16	Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
17	Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

		Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
18	Zarządzanie	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. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
19	Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

		Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
20	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
21	IPS Throughput	2,5Gbps
22	NGFW Throughput	Co najmniej 1,5Gbps
23	Threat Protection Throughput	Co najmniej 1,3Gbps
24	Sesje równoległe (TCP)	1 400 000
25	Przepustowość IPsec VPN (512 bajtów)	7.1 Gb/s
26	Firewall Policies	5 000
27	Porty	RJ45 (WAN1, WAN2, LAN1, LAN2, LAN3, LAN4, LAN5, LAN6)
28	Gwarancja i serwis	Gwarancja producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 2: Macierz dyskowa z dyskami

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowej macierzy dyskowej z nowymi dyskami
2	Obudowa	Rack 2U o wymiarach nie większych niż: 90(Wys.) x 434(Szer.) x 300 (Gł.) mm, Szyny do montażu w szafie RACK wraz z urządzeniem
3	Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B lub równoważny procesor czterordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4500 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html
4	Architektura procesora	64-bitowy x86
5	Pamięć RAM	4GB SODIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB
6	Pamięć flash	Co najmniej 5GB
7	Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6Gb/s 2 dyski SSD M.2 NVMe 2280
8	Ilość zainstalowanych dysków	6 dysków o pojemności 8TB każdy, minimum256MB cache, 7200 RPM, 1 mil godzin MTBF, będących na liście zgodności producenta macierzy; Dyski hot swap
9	Interfejsy sieciowe	2 x 2,5GbE (RJ45)
10	Gniazdo PCIe	1 x PCIe Gen3 x8
11	Porty USB	2 x USB Typu-C 3.2 Gen 2 (10Gb/s) 2 x USB Typu-A 3.2 Gen 2 (10Gb/s)
12	Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60
13	Szyfrowanie	Możliwośc szyfrowania folderów i wolumenów kluczem AES 256-bit
14	Funkcja Hot Spare	RAID Hot Spare and Global Hot Spare
15	Protokoły	CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
16	Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS

		Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog
17	System plików	Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
18	Wentylatory	Min. 3 x 60 mm
19	Zasilanie	Redundantne (2x 300W)
20	Gwarancja i serwis	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie oraz dyski

Zadanie 3: Serwer NAS (network attached storage) z dyskami.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera NAS z nowymi dyskami
2	Obudowa	Tower o wymiarach nie większych niż: 185(Wys.) x 333(Szer.) x 285(Gł.) mm
3	Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B lub równoważny procesor czterordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4500 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html
4	Architektura procesora	64-bitowy x86
5	Pamięć RAM	8GB SODIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB
6	Pamięć flash	Co najmniej 5GB
7	Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6Gb/s 2 dyski SSD M.2 NVMe 2280
8	Ilość zainstalowanych dysków	6 dysków o pojemności 8TB każdy, minimum256MB cache, 7200 RPM, 1 mil godzin MTBF, będących na liście zgodności producenta macierzy; 2 dyski SSD w formacie M.2 NVMe o pojemności 1,92TB każdy; Dyski hot swap
9	Interfejsy sieciowe	2 x 2,5GbE (RJ45)
10	Gniazdo PCIe	1 x PCIe Gen3 x8
11	Porty USB	2 x USB Typu-C 3.2 Gen 2 (10Gb/s) 2 x USB Typu-A 3.2 Gen 2 (10Gb/s)
12	Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60
13	Szyfrowanie	Możliwosc szyfrowania folderów i wolumenów kluczem AES 256-bit
14	Funkcja Hot Spare	RAID Hot Spare and Global Hot Spare
15	Protokoły	CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
16	Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS

		Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog
17	System plików	Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
18	Wentylatory	Min. 3 x 60 mm
19	Zasilanie	Redundantne (2x 300W)
20	Gwarancja i serwis	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie oraz dyski

Zadanie 4: Zasilacz awaryjny.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia UPS. Działającego w technologii Line Interactive
2	Moc urządzenia:	Minimalna pozorna moc urządzenia 2200VA, Moc rzeczywista urządzenia minimum 1980W.
3	Parametry wejściowe	Nominalne napięcie wejściowe 230V Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie). Typ gniazda wejściowego: IEC-320 C20
4	Parametry wyjściowe	Napięcie wyjściowe 220, 230, 240V Częstotliwość na wyjściu przy pracy bateryjnej 50/60Hz ±3Hz Typ przebiegu sinusoida Złącza/gniazda wyjściowe - co najmniej 6 IEC 320 C13
5	Komunikacja i zarządzanie	Porty komunikacyjne: RJ-45 Serial, USB, Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD

		Alarm dźwiękowy: Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
6	Akumulatory i czas podtrzymania	Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu Czas autonomii: 8 minut 42 sekund dla pełnego obciążenia 24 minuty 57 sekundy dla połowy obciążenia Oczekiwana żywotność akumulatora (lata) 3 – 5 Baterie wymieniane na gorąco. Akumulatory muszą być fabrycznie nowe
7	Certyfikaty, zgodności oraz gwarancja	CE, EN62040-1, EN62040-2, VDE, RoHS, REACh 3 lata gwarancji producenta door to door na naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator
8	Oprogramowanie	Oprogramowanie do zarządzania zgodne Windows® Server 2019, 2016, 2012;

Zadanie 5: Wdrożenie urządzenia UTM.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest przeprowadzenie wdrożenia urządzenia utm.
2	Zakres prac	Dla urządzeń zabezpieczających sieć IT wykonanie wdrożenia ww. obejmujące: kontrolę ruchu sieciowego, ustawienie wymaganych zabezpieczeń. Stworzenie dokumentacji obejmującej wdrożone polityki bezpieczeństwa. Przeszkolenie pracownika Zakładu.
3	Miejsce prac	Realizacja wdrożenia ww. urządzenia i szkolenia ma być przeprowadzona na miejscu w wskazanej lokalizacji Zakładu

Zadanie 6: Przełącznik zarządzalny.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego przełącznika zarządzalnego
2	Obudowa	Rack 1U
3	Funkcjonalność	Przełącznik z obsługą 802.1AE i 802.1x VLANY Zarządzany L2+ Zarządzanie przez stronę www
4	Porty	48 portów PoE+ RJ45 10/100/1000 Mb/s • 4 sloty SFP+ 10G • 1 port konsolowy RJ45 • 1 port konsolowy micro-USB
5	Bufor pakietów	12 Mbit
6	Ramki jumbo	9 KB
7	Tablica adresów MAC	16 K
8	Cechy przełącznika L3	128 interfejsów IPv4/IPv6 • Statyczny routing - 48 statyczne trasy • Statyczny ARP - 128 Statycznych wpisów • Proxy ARP • Gratuitous ARP • DHCP Serwer • Przekaźnik DHCP - DHCP Przekaźnik interfejsu - DHCP Przekaźnik VLAN • DHCP L2 Przekaźnik
9	Funkcje L2 i L2+	Link Aggregation - statyczna agregacja linków - 802.3ad LACP - Do 8 grup agregacji, zawierających 8 portów na grupę • Spanning Tree Protocol - 802.1d STP - 802.1w RSTP - 802.1s MSTP - STP Security: TC Protect, BPDU Filter, Root Protect • Wykrywanie Pętli - Bazujące na Porcie - Bazujące na VLAN • Flow Control - 802.3x Flow Control - HOL Blocking Prevention • Mirroring - Port Mirroring

		- CPU Mirroring One-to-One - Many-to-One - Tx/Rx/Both
10	Bezpieczeństwo transmisji	Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4: 100 wpisów • Wiązanie adresów IPv6, MAC i portów - 512 wpisów - DHCPv6 Snooping - Wykrywanie ND - Ochrona źródłowego adresu IPv6: 100 wpisów • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC - Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • AAA (w tym TACACS+) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 • Kontrola dostępu w oparciu o IP/port/MAC
11	Architektura	Co najmniej1Gb
12	Przepustowość	Powyżej 150Gb/s
13	Warunki serwisu	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 7: Opłata za subskrypcje ochronne do urządzenia UTM.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest opłata za subskrypcje ochronne w zakresie stałych aktualizacji bazy sygnatur i chmury producenta.

Zadanie 8: Access point Wi-Fi

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego access pointa
2	Funkcjonalność	Obsługa standardu 802.1x, oraz WPA3 - Enterprise
3	Złącza ethernet	RJ-45 10/100/1000 (LAN) - 1 szt.
4	Przepustowość	Minimalna 2500Mb/s
5	Moc wyjściowa anten	Minimalnie 20dB
6	Zasilacz do urządzenia	Dołączony
7	Warunki serwisu	Gwarancji producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 9: Firewall sieciowy

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego firewalla sieciowego
2	Obudowa	rack
3	Interfejs LAN	RJ-45 10/100/1000 - 8 szt. SFP+ - 1 szt.
4	Maksymalna liczba równoczesnych połączeń	2000 połączeń
5	Pamięć RAM	8 GB
6	Pamięć flash	128 GB
7	Warunki serwisu	Gwarancji producenta lub autoryzowanego partnera producenta na urządzenie

Zakres zamówienia w zakresie OT

LP.	NAZWA	SPECYFIKACJA
1	Firewall sieciowy	Zadanie 1
2	Urządzenie UTM	Zadanie 2
3	Macierz dyskowa z dyskami	Zadanie 3
4	Zasilacz awaryjny	Zadanie 4
5	Wdrożenie urządzenia UTM i Firewall	Zadanie 5
6	Opłata za subskrypcje ochronne do urządzenia UTM	Zadanie 6
7	Przełącznik zarządzalny	Zadanie 7
8	Access point Wi-Fi	Zadanie 8
9	Opłata za subskrypcje ochronne do urządzenia Firewall	Zadanie 9

Zadanie 1: Fierwall sieciowy.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia firewall
2	Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
3	Funkcjonalność ZAPORA KORPORACYJNA	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania

		kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe
4	INTRUSION PREVENTION SYSTEM (IPS)	System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP PROFINET, SOFBUS/LACBUS, IEC

		60870-5-104, IEC 61850 (MMS, Goose & SV). Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych .
5	KSZTAŁTOWANIE PASMA (Traffic Shapping)	Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
6	WIRTUALNE SIECI PRYWATNE (VPN)	Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub siteto-site (lokalizacja-lokalizacja). Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. IPSec VPN, b. SSL VPN. SSL VPN ma działać w trybie tunelu. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal). Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). W ramach licencji dostępny jest klient SSLVPN pod systemy: Windows, Linux, macOS objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.
7	UWIERZYTELNIANIE	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. d. Microsoft Entra ID, opartej na protokole OpenID Connect. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. Urządzenie ma umożliwiać

		uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL, Radius, Kerberos. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
8	ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do internetu. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. W zakresie SD-WAN urządzenie

		ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
9	ROUTING (TRASOWANIE)	Urządzenie ma umożliwiać statyczne trasowanie pakietów. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

10	ADMINISTRACJA URZĄDZENIEM	Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH). Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie

		czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwyużytkownika. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. RAPORTOWANIE
11	RAPORTOWANIE	Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system

		zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
12	POZOSTAŁE USŁUGI I FUNKCJE	Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). Urządzenie ma posiadać usługę DNS Proxy. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. Urządzenie musi mieć możliwość wykorzystania REST API. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie
13	PARAMETRY SPRZĘTOWE	Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. Liczba portów Ethernet 2,5Gbps – min.4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. Przepustowość Firewall (1518 bajtów UDP) – minimum 8,5Gbps. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1,8Gbps. Liczba tuneli VPN IPSec – minimum 200. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum Obsługa interfejsów 802.11q (VLAN) – minimum 137. Liczba równoczesnych sesji – minimum 150 000 i nie mniej

		niż 25 000 nowych sesji/sekundę. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. Urządzenie nie ma limitu na liczbę użytkowników. Liczba reguł filtrowania – minimum 1024. Liczba tras statycznego routingu – minimum 512. Liczba tras dynamicznego routingu – minimum 10 000. Urządzenie musi posiadać pasywny system chłodzenia. Urządzenie ma być przystosowane do pracy w temperaturach od -20oC do +60oC przy wilgotności od 0% do 95% (bez kondensacji). Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 50,1 lat. Urządzenie musi być przystosowane do montażu na szynie DIN zgodnej ze standardem EN 50022. Urządzenie musi być wyposażone w moduł TPM. Urządzenie musi dawać możliwość podłączenia zasilania bezpośrednio z linii produkcyjnej prądem stałym 12-48VDC 3-0.75A. Urządzenie musi być wyposażone w zasilacz umożliwiający podłączenie do sieci 100-240V 60-50Hz 1.2A.
14	Warunki gwarancja i serwis	Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal
15	PARAMETRY SPRZĘTOWE	Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. Liczba portów Ethernet 2,5Gbps – min.4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. Przepustowość Firewall (1518 bajtów UDP) – minimum 8,5Gbps. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1,8Gbps. Liczba tuneli VPN IPSec – minimum 200. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 200. Obsługa interfejsów 802.11q (VLAN) – minimum 137. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 25 000 nowych sesji/sekundę. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

		Urządzenie nie ma limitu na liczbę użytkowników. Liczba reguł filtrowania – minimum 1024. Liczba tras statycznego routingu – minimum 512. . Liczba tras dynamicznego routingu – minimum 10 000. Urządzenie musi posiadać pasywny system chłodzenia. Urządzenie ma być przystosowane do pracy w temperaturach od -20oC do +60oC przy wilgotności od 0% do 95% (bez kondensacji).Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 50,1 lat. Urządzenie musi być przystosowane do montażu na szynie DIN zgodnej ze standardem EN 50022. Urządzenie musi być wyposażone w moduł TPM. Urządzenie musi dawać możliwość podłączenia zasilania bezpośrednio z linii produkcyjnej prądem stałym 12-48VDC 3-0.75A. Urządzenie musi być wyposażone w zasilacz umożliwiający podłączenie do sieci 100-240V 60-50Hz 1.2A.

Zadanie 2: Urządzenie UTM.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia UTM z funkcjonalnością dla ochrony sieci OT
2	Opis	Zapewniona funkcjonalność SD-WAN zapewniająca optymalizację połączeń, łącząc bezpieczeństwo sieci i zarządzanie ruchem, co zwiększa wydajność. Wymagana technologia firewall nowej generacji (NGFW) oferująca zaawansowaną ochronę przed zagrożeniami, blokująca nieautoryzowany dostęp i zapewniając głęboką inspekcję ruchu SSL. Funkcja IPS (Intrusion Prevention System), identyfikująca i blokująca zagrożenia w czasie rzeczywistym. Wbudowane kontrole aplikacji, pozwalające administratorom na monitorowanie i zarządzanie użyciem aplikacji w sieci. Wsparcie połączenia VPN, umożliwiając bezpieczny zdalny dostęp do zasobów organizacyjnych. zagrożeń. Wsparcie dla Zero Trust, co pozwala na zwiększone bezpieczeństwo w złożonych środowiskach IT. Możliwość centralnego zarządzania politykami i konfiguracjami. Urządzenie typu next-generation firewall (NGFW) i SD-WAN.
3	Wymagania Ogólne	System bezpieczeństwa realizuje 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. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

		Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
4	Redundancja, monitoring i wykrywanie awarii	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. 2Monitoring 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.
5	Interfejsy, Dysk, Zasilanie:	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
6	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 50 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 2 Gbps. 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 o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2 Gbps. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi

		funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
7	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa 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. 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. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
8	Polityki, Firewall	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: adresy 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. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
9	Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

		• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji
10	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: Routingu statycznego. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. Możliwość 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.
11	Funkcje SD-WAN	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
12	Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
13	Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

		W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. System zapewnia 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.
14	Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.

		Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 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.
15	Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
16	Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

		Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
17	Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
18	Zarządzanie	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. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

		System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
19	Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
20	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
21	IPS Throughput	Co najmniej 2Gbps
22	NGFW Throughput	Co najmniej 1Gbps

23	Threat Protection Throughput	Co najmniej 1Gbps
24	Firewall Policies	2000
25	Sesje równoległe (TCP)	720 000
26	Przepustowość IPsec VPN (512 bajtów)	1.3 Gb/s
27	Połączenia RJ45	5portów
28	Gwarancja i serwis	Gwarancja producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 3: Macierz dyskowa z dyskami.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowej macierzy dyskowej z nowymi dyskami
2	Obudowa	Rack 2U o wymiarach nie większych niż: 90(Wys.) x 434(Szer.) x 300 (Gł.) mm, Szyny do montażu w szafie RACK wraz z urządzeniem
3	Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B lub równoważny procesor czterordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4500 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html
4	Architektura procesora	64-bitowy x86
5	Pamięć RAM	4GB SODIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB
6	Pamięć flash	Co najmniej 5GB
7	Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6Gb/s 2 dyski SSD M.2 NVMe 2280
8	Ilość zainstalowanych dysków	2 dyski o pojemności 8TB każdy, minimum256MB cache, 7200 RPM, 1 mil godzin MTBF, będących na liście zgodności producenta macierzy; Dyski hot swap

9	Interfejsy sieciowe	2 x 2,5GbE (RJ45)
10	Gniazdo PCIe	1 x PCIe Gen3 x8
11	Porty USB	2 x USB Typu-C 3.2 Gen 2 (10Gb/s) 2 x USB Typu-A 3.2 Gen 2 (10Gb/s)
12	Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60
13	Szyfrowanie	Możliwośc szyfrowania folderów i wolumenów kluczem AES 256-bit
14	Funkcja Hot Spare	RAID Hot Spare and Global Hot Spare
15	Protokoły	CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
16	Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog
17	System plików	Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
18	Wentylatory	Min. 3 x 60 mm
19	Zasilanie	Redundantne (2x 300W)
20	Gwarancja i serwis	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie oraz dyski

Zadanie 4: Zasilacz awaryjny.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia UPS. Działającego w technologii Line Interactive
2	Moc urządzenia:	Minimalna pozorna moc urządzenia 2200VA, Moc rzeczywista urządzenia minimum 1980W.
3	Parametry wejściowe	Nominalne napięcie wejściowe 230V Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie). Typ gniazda wejściowego: IEC-320 C20
4	Parametry wyjściowe	Napięcie wyjściowe 220, 230, 240V Częstotliwość na wyjściu przy pracy bateryjnej 50/60Hz ±3Hz Typ przebiegu sinusoida Złącza/gniazda wyjściowe - co najmniej 6 IEC 320 C13
5	Komunikacja i zarządzanie	Porty komunikacyjne: RJ-45 Serial, USB, Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD Alarm dźwiękowy: Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
6	Akumulatory i czas podtrzymania	Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu Czas autonomii: 8 minut 42 sekund dla pełnego obciążenia 24 minuty 57 sekundy dla połowy obciążenia Oczekiwana żywotność akumulatora (lata) 3 – 5 Baterie wymieniane na gorąco. Akumulatory muszą być fabrycznie nowe
7	Certyfikaty, zgodności oraz gwarancja	CE, EN62040-1, EN62040-2, VDE, RoHS, REACh 3 lata gwarancji producenta door to door na naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator
8	Oprogramowanie	Oprogramowanie do zarządzania zgodne Windows® Server 2019, 2016, 2012;

Zadanie 5: Wdrożenie urządzenia UTM i Firewall.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest przeprowadzenie wdrożenia urządzenia utm i firewall.
2	Zakres prac	Dla urządzeń zabezpieczających sieć OT wykonanie wdrożenia ww. obejmujące: kontrolę ruchu sieciowego, ustawienie wymaganych zabezpieczeń. Stworzenie dokumentacji obejmującej wdrożone polityki bezpieczeństwa. Przeszkolenie pracownika Zakładu.
3	Miejsce prac	Realizacja wdrożenia i szkolenia ww. urządzeń ma być przeprowadzona na miejscu w wskazanej lokalizacji Zakładu.

Zadanie 6: Opłata za subskrypcje ochronne do urządzenia UTM

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest opłata za subskrypcje ochronne w zakresie stałych aktualizacji bazy sygnatur i chmury producenta.

Zadanie 7: Przełącznik zarządzalny.

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego przełącznika zarządzalnego
2	Obudowa	Rack 1U
3	Funkcjonalność	Przełącznik z obsługą 802.1AE i 802.1x VLANY Zarządzany L2+ Zarządzanie przez stronę www
4	Porty	48 portów PoE+ RJ45 10/100/1000 Mb/s • 4 sloty SFP+ 10G • 1 port konsolowy RJ45 • 1 port konsolowy micro-USB
5	Bufor pakietów	12 Mbit
6	Ramki jumbo	9 KB
7	Tablica adresów MAC	16 K
8	Cechy przełącznika L3	128 interfejsów IPv4/IPv6 • Statyczny routing - 48 statyczne trasy • Statyczny ARP - 128 Statycznych wpisów • Proxy ARP • Gratuitous ARP • DHCP Serwer • Przekaźnik DHCP - DHCP Przekaźnik interfejsu - DHCP Przekaźnik VLAN • DHCP L2 Przekaźnik
9	Funkcje L2 i L2+	Link Aggregation - statyczna agregacja linków - 802.3ad LACP - Do 8 grup agregacji, zawierających 8 portów na grupę • Spanning Tree Protocol - 802.1d STP - 802.1w RSTP - 802.1s MSTP - STP Security: TC Protect, BPDU Filter, Root Protect • Wykrywanie Pętli - Bazujące na Porcie - Bazujące na VLAN • Flow Control - 802.3x Flow Control - HOL Blocking Prevention • Mirroring - Port Mirroring

		- CPU Mirroring One-to-One - Many-to-One - Tx/Rx/Both
10	Bezpieczeństwo transmisji	Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4: 100 wpisów • Wiązanie adresów IPv6, MAC i portów - 512 wpisów - DHCPv6 Snooping - Wykrywanie ND - Ochrona źródłowego adresu IPv6: 100 wpisów • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC - Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • AAA (w tym TACACS+) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 • Kontrola dostępu w oparciu o IP/port/MAC
11	Architektura	Co najmniej1Gb
12	Przepustowość	Powyżej 150Gb/s
13	Warunki serwisu	3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 8: Access point Wi-Fi

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa fabrycznie nowego access pointa
2	Funkcjonalność	Obsługa standardu 802.1x, oraz WPA3 - Enterprise
3	Złącza ethernet	RJ-45 10/100/1000 (LAN) - 1 szt.
4	Przepustowość	Minimalna 2500Mb/s
5	Moc wyjściowa anten	Minimalnie 20dB
6	Zasilacz do urządzenia	Dołączony
7	Warunki serwisu	Gwarancji producenta lub autoryzowanego partnera producenta na urządzenie

Zadanie 9: Opłata za subskrypcje ochronne do urządzenia Firewall

LP.	NAZWA	Minimalne wymagania sprzętowe
1	Przedmiot zamówienia	Przedmiotem zamówienia jest opłata za subskrypcje ochronne w zakresie stałych aktualizacji bazy sygnatur i chmury producenta.