Załącznik Nr 1 do SWZ

Specyfikacja techniczna
„Cyfryzacja Urzędu Gminy w Rogowie”

Część 1. Dostawa sprzętu komputerowego	
1. Serwer danych	
	parametry minimalne
Obudowa	Rack 2U do 3U, 16 dysków 2,5" (ramki, TPM 2.0 V3)
Procesor	1 lub 2 procesory (41000 pkt Passmark)
Pamięć	32GB pamięci RAM 3200MT/s
Kontroler RAID	Kontroler o szybkości 12Gb/s per port z 4GB nieulotnej pamięci podręcznej, Obsługa RAID 0,1,5,10. Obsługa dysków samodzielnych, możliwość utworzenia macierzy RAID + 1 lub 2 dyski samodzielne
Dyski SSD	5 x 480 SSD SATA do intensywnego odczytu 6Gb/s, Hot-plug, 1 DWPD
Dyski SAS	5 x 1,2TB HDD SAS 12Gb/s, 10 tys. obr./min, Hot-plug
Porty	4x USB w tym co najmniej 2x USB 3.2 gen.1
Sieć	2 x Rj45 10Gbit/s, 1x SFP 10Gbit/s (dostarczenie patchcordu SFP kompatybilnego ze Switchem z poz 2., umożliwiający uzyskanie 10Gbit/s 2 szt.)
Zasilanie	Redundantne zasilacze (1+1) 800W
Mocowanie	Szyny wysuwane
Gwarancja	Pozostawienie dysków w razie awarii
System operacyjny	Microsoft Windows Server 2022 Essentials
Klawiatura i mysz	bezprzewodowe, mysz laserowa (zestaw z jednym obiornikiem USB)
2. Switch	
Obudowa	Rack 1U lub 2U
Interfejsy	48 x 10/100/1000Mbps Ethernet, RJ-45 6 x 1000Mbps/10Gbps SFP+ slot 1 (Port/PoE LED)(P2540x) 1 x Factory Reset
PoE	PoE Capable Ports - 48 PoE+ (802.3af/802.3at), Type mode A Moc 400 W Power Cycle on Port - Manual, Ping Watchdog
Zdolność	Buffer Size 6 Switching Capacity 216 Gbps Forwarding Rate 160.7 Mpps (64 bytes) MAC Address Table 32k Jumbo Frame Up to 12KB

Zarządzanie	Web Interface HTTP, HTTPS Command Line Interface Telnet, SSH OpenVPN Client - Certificate-based authentication Mail Alert Port Status, Port Speed, System Restart, IP Conflict Możliwość zarządzania switchem poprzez funkcję Central Switch Management wbudowaną w posiadany przez gminę router Draytek
Akcesoria	3 moduły SFP 10Gbps
3. AP (7 szt.)	
Obudowa	Montaż ścienny lub sufitowy
Anteny	4 x Internal PiFA Single-Band (2.4G) 4 x Internal PiFA Single-Band (5G) 1 x Internal PCB DB (for scanning radio)
Interfejsy	1 x 2.5G/1G/100M/10M Ethernet, RJ-45
PoE	PoE-PD Support
Zdolność	2.4GHz Peak Speed 1200 Mbps 5GHz Peak Speed 2400 Mbps Max. Number of 256 Concurrent Active Clients 256 (128 per radio band) Operating Mode: AP, Mesh Root, Mesh Node, Range Extender
Zarządzanie	Local Service: HTTP, HTTPS, Telnet Konfiguracja: Stand Alone, TR-069 (VigorACS), Vigor Router APM, VigorAP Mesh Root Możliwosc zarządzania switchem poprzez funkcję Central Switch Management wbudowaną w posiadany przez gminę router Draytek
Akcesoria	Dołączone zasilacze
4. AP outdoor (1 szt.)	
Obudowa	Montaż ścienny lub sufitowy, wodoszczelna IP67
Anteny	2x Dual-Band dipole External (Gain: 6 dBi for 5GHz, 3.5 dBi for 2.4GHz)
Interfejsy	1x 10/100/1000Base-T Ethernet, RJ-45
PoE	802.3at (in) (R model) 802.3at (in), 802.3at **(out)**
Zdolność	2.4GHz Link Rate Up to 400 Mbps 5GHz Link Rate Up to 867 Mbps Max. Number of Concurrent Active Clients 256 (128 per radio band) 2.4GHz Standard IEEE 802.11b/g/n 2x2 MIMO 5GHz Standard IEEE 802.11a/n/ac Wave 2 2x2 MU-MIMO Tryby pracy AP, Mesh Root, Mesh Node, Range Extender
Zarządzanie	Local Service: HTTP, HTTPS, Telnet Konfiguracja: Stand Alone, TR-069 (VigorACS), Vigor Router APM, VigorAP Mesh Root Możliwosc zarządzania switchem poprzez funkcję Central Switch Management wbudowaną w posiadany przez gminę router Draytek
5. Stacje robocze 5 szt.	
Obudowa	All-In-One
Przekątna ekranu	23.8"
Rozdzielczość	1920 x 1080 (FHD 1080)

Ekran dotykowy	TAK
Powierzchnia matrycy	Matowa
Procesor	4,2 GHz (10000 pkt. Passmark)
Zainstalowana pamięć RAM	8 GB
Rodzaj pamięci	DDR4
Częstotliwość szyny pamięci	2666 MHz
Typ dysku	SSD
Pojemność SSD	512 GB
Format szerokości SSD	M.2
Interfejs dysku SSD	PCI-Express
Karta graficzna	wydajność 2500 pkt. Passmark
Wielkość pamięci VRAM	2 GB
Porty wideo	2 x HDMI
Interfejs sieciowy	1 x 10/100/1000 Mbit/s Wi-Fi 802.11a/b/g/n/ac/ax Bluetooth
Czytnik kart pamięci	Tak
Porty USB	1 x USB 2.0 Type-A 3 x USB 3.0 Type-A
Pozostałe porty we/wy	1 x Audio (Słuchawki / Line-out) 1 x RJ-45
Kamera internetowa	Tak
Kolor	Srebrny
Typ podstawy	Frame Stand
System operacyjny	Windows 11 w wersji PRO
Akcesoria w zestawie	Bezprzewodowa klawiatura i mysz (kolor biały)
6a. Komputer przenośny (1. szt)	
Procesor	8 rdzeni (16 tys. pkt Passmark)
Pamięć RAM	24 GB (DDR4, 3200MHz)
Dysk SSD M.2 PCIe	512 GB
Opcje dołożenia dysków	Możliwość montażu dysku M.2 PCIe (elementy montażowe w zestawie)
Typ ekranu	Matowy, LED, IPS
Przekątna ekranu	15,6"
Rozdzielczość ekranu	1920 x 1080 (Full HD)
Jasność matrycy	300 cd/m²
Dźwięk	Wbudowane głośniki stereo. Wbudowane dwa mikrofony
Kamera internetowa	Kamera na podczerwień. 1.0 Mpix
Łączność	LAN 1 Gb/s Wi-Fi 6 Moduł Bluetooth 5.2

Złącza	USB 2.0 - 1 szt. USB 3.2 Gen. 1 - 1 szt. USB Typu-C (z DisplayPort i Power Delivery) - 1 szt. HDMI 1.4b - 1 szt. RJ-45 (LAN) - 1 szt. Wyjście słuchawkowe/wejście mikrofonowe
Typ baterii	Litowo-jonowa
Pojemność baterii	3-komorowa, 4900 mAh
Czytnik linii papilarnych	Tak (w przycisku POWER)
Podświetlana klawiatura	Tak
Zabezpieczenia	Możliwość zabezpieczenia linką (port Kensington Lock) Szyfrowanie TPM Kamera z wbudowaną zaślepką
Obudowa	Aluminiowa pokrywa matrycy
System operacyjny	Microsoft Windows 11 Pro
Zasilacz	Wtyk: USB-C
Dodatkowe wymagania	Wydzielona klawiatura numeryczna Wielodotykowy, intuicyjny touchpad, Trackpoint w klawiaturze Kolor obudowy: czarny
6b. Komputer przenośny (1szt.)	
Procesor	6 rdzeni, 12200 pkt Passmark
Pamięć RAM	16 GB (DDR4, 2666MHz) (mozliwość rozbudowy do 64GB)
Dysk SSD M.2 PCIe	512 GB
Dotykowy ekran	TAK
Typ ekranu	Błyszczący, LED, IPS
Przekątna ekranu	15,6"
Rozdzielczość ekranu	1920 x 1080 (Full HD)
Karta graficzna	min 10000 pkt. Passmark, 6 GB GDDR6
Dźwięk	Wbudowane głośniki stereo Wbudowane dwa mikrofony
Kamera internetowa	30fps@720p
Łączność	LAN 1 Gb/s Wi-Fi 6 Moduł Bluetooth
Złącza	USB 3.2 Gen. 1 - 1 szt. USB Typu-C - 1 szt. USB Typu-C (z Thunderbolt™ 3) - 1 szt. HDMI - 1 szt. Czytnik kart pamięci SD - 1 szt. RJ-45 (LAN) - 1 szt. Wyjście słuchawkowe/wejście mikrofonowe - 1 szt. DC-in (wejście zasilania) - 1 szt.
Typ baterii	Litowo-polimerowa
Podświetlana klawiatura	TAK
Zabezpieczenia	Szyfrowanie TPM

Obudowa	Aluminiowa pokrywa matrycy Aluminiowe wnętrze laptopa Aluminiowa obudowa
System operacyjny	Microsoft Windows 11 PRO
Zasilacz	180W
Dodatkowe wymagania	Wejścia HDMI IN 2 szt. (dopuszczamy dodatkowy moduł USB)
6c. Komputer przenośny (2szt.)	
Procesor	6 rdzeni, 16100 pkt. passmark
Pamięć RAM	16 GB (DDR4, 3200MHz)
Dysk SSD M.2 PCIe	256 GB
Dotykowy ekran	TAK
Typ ekranu	Matowy, LED, WVA
Przekątna ekranu	15,6"
Rozdzielczość ekranu	1920 x 1080 (Full HD)
Karta graficzna	Dedykowana 3700 pkt. passmark (2 GB GDDR6)
Dźwięk	Wbudowane głośniki stereo Wbudowane dwa mikrofony
Kamera internetowa	1.0 Mpix
Łączność	LAN 1 Gb/s Wi-Fi 6 Moduł Bluetooth 5.1
Złącza	USB 3.2 Gen. 1 - 1 szt. USB 3.2 Gen. 1 (z PowerShare) - 1 szt. USB Typu-C (z Thunderbolt™ 4) - 2 szt. HDMI 2.0 - 1 szt. Czytnik kart pamięci microSD - 1 szt. RJ-45 (LAN) - 1 szt. Wyjście słuchawkowe/wejście mikrofonowe - 1 szt. Czytnik Smart Card - 1 szt.
Typ baterii	Litowo-polimerowa, 4-komorowa, 4200 mAh
Podświetlana klawiatura	TAK
Zabezpieczenia	Możliwość zabezpieczenia linką (port Noble Wedge) Szyfrowanie TPM Kamera z wbudowaną zaślepką
Obudowa	Standard militarny MIL-STD-810H
System operacyjny	Microsoft Windows 10 Pro PL
Dodatkowe wymagania	Wydzielona klawiatura numeryczna Wielodotykowy, intuicyjny touchpad
7. System zabezpieczania danych - backup	
Rodzaj urządzenia	Napęd kaset RDX - zewnętrzny
Interfejs	SuperSpeed USB 3.0
Wyposażenie	6 kaset o pojemności 2 TB każda

Oprogramowanie	Możliwość backupu 25 komputerów, 3 serwerów, 2 hostów wirtualizacji Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) Automatyczny backup przy wyłączaniu komputera Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ? Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) Backup baz danych i plików poczty w trybie online i offline Kopie rotacyjne (wersjonowanie) Zapis archiwów w otwartym formacie (ZIP 64-bit) Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO Kompresja po stronie stacji roboczej Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) Centralne sterowanie całym Systemem z jednego miejsca Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN Wysyłanie Alertów administracyjnych na e-mail Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki Automatyczna aktualizacja oprogramowania na komputerach zdalnych Bezterminowa licencja - licencja nie może być ograniczona czasowo Interfejs, instrukcja i pomoc techniczna w języku polskim

Część 2. Dostawa urzadzenia UTM

1. UTM (Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)
Termin realizacji 3 miesiące

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.

ZAPORA KORPORACYJNA (Firewall)

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, 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.
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).
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, FTPS, 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).

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.
OCHRONA ANTYWIRUSOWA
Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
OCHRONA ANTYSPAM
Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
Ochrona antyspam ma działać w oparciu o: - białe/czarne listy, - DNS RBL, - Skaner heurystyczny.
W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)
Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
Urządzenie ma wspierać co najmniej następujące typy sieci VPN: - PPTP VPN, - IPSec VPN, - SSL VPN.
SSL VPN ma działać co najmniej w trybach tunelu i portalu.
Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW
Urządzenie ma posiadać wbudowany filtr URL.

Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
Administrator ma mieć możliwość dodawania własnych kategorii URL.
Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: - blokowanie dostępu do adresu URL, - zezwolenie na dostęp do adresu URL, - blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
Filtr URL musi uwzględniać komunikację po protokole HTTPS.
Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
UWIERZYTELNIANIE
Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: - lokalną bazę użytkowników (wewnętrzny LDAP), - zewnętrzną bazę użytkowników (zewnętrzny LDAP), - usługę katalogową Microsoft Active Directory.
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.
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: - równoważenie względem adresu źródłowego, - 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.

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.
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 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.
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: - manualnego eksportu do pliku w dowolnym momencie czasu, - automatycznego eksportu do chmury 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 bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
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 posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
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 1, 2 i 3.
Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

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 w zakresie określenia bramy, serwerów DNS, nazwy domeny.
Urządzenie ma posiadać usługę DNS Proxy.
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.
GWARANCJA I SERWIS
Urządzenie ma być objęte 24-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 lub telefonicznie.
PARAMETRY SPRZĘTOWE
Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
Liczba portów Ethernet 10/100/1000Mbps – min.8.
Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
Maksymalna liczba tuneli VPN IPSec – minimum 100.
Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
Obsługa interfejsów 802.11q (VLAN) – minimum 128
Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 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 8 192.
Liczba tras statycznego routingu – minimum 512.
Liczba tras dynamicznego routingu – minimum 10 000.
WDROŻENIE
Wymagane jest wdrożenie polegające na pełnej konfiguracji zdalnej urządzenia według ustaleń administratora sieci.

Część 3. Edukacja cyfrowa i diagnoza cyberbezpieczeństwa	
1. Szkolenie specjalistyczne administratora urządzeń UTM	
Ilość osób	1
Rodzaj szkolenia	Stacjonarne, minimum 24 godziny lekcyjne wraz z pakietem materiałów szkoleniowych, w tym dostęp do maszyn wirtualnych
Wymagana tematyka:	1. Zaawansowana konfiguracja IPS. · Technologia ASQ i fazy analizy pakietu w szczegółach, · Wykorzystanie profili IPS, · Zmiana domyślnych profili dla ruchu wchodzącego i wychodzącego z sieci, · Zapisywanie i analiza pakietów dzięki sygnaturom kontekstowym, · Łączenie profili IPS z regułami filteringu.
	2. Zaawansowana konfiguracja sieci. · Interfejsy typu Dialup, · Interfejsy typu VLAN.
	3. Zaawansowana konfiguracja routingu. · Routing by interface, · Policy routing, · Load balancing.
	4. Zaawansowana translacja adresów.
	5. Zaawansowana konfiguracja firewalla.
	6. Kształtowanie pasma (QoS). · Omówienie mechanizmu Quality of Service (QoS), · Konfiguracja kolejek QoS z wykorzystaniem algorytmu PRIQ, · Konfiguracja kolejek QoS z wykorzystaniem algorytmu CBQ, · Monitorowanie ruchu z wykorzystaniem kolejek QoS typu MONITOR, · Integracja kolejek QoS z firewallem.
	7. Infrastruktura Klucza Publicznego. · Wprowadzenie to tematyki Public Key Infrastructure (PKI). · Tworzenie wewnętrznego urzędu certyfikacji, · Integracja PKI z innymi usługami w urządzeniu, · Integracja urządzenia z zewnętrznym urzędem certyfikacji.
	8. Technologia VPN. · IPSec VPN. · Kanały VPN typu site-to-site z wykorzystaniem protokołu IPSec (PKI), · Kanały VPN typu client-to-site z wykorzystaniem protokołu IPSec (PKI), · Translacja adresów w tunelach IPSec, · Zaawansowane opcje IPSec VPN. · SSL VPN. · Konfiguracja SSL VPN w trybie Portal, · Konfiguracja SSL VPN w trybie Tunel.
	9. Zaawansowane opcje Proxy - SSL Proxy. · Wprowadzenie do SSL Proxy, · Konfiguracja certyfikatów dla SSL Prox
	10. Zarządzanie urządzeniem z wykorzystaniem CLI.
	11. Diagnostyka pracy urządzenia.
	· Rozwiązywanie problemów konfiguracyjnych,
	· Tworzenie i analiza technical report
Dodatkowe wymagania	Szkolenie powinno zostać zakończone egzaminem i powinień zostać wystawiony certyfikat. W przypadku organizacji szkolenia w odległości większej niż 50 km od siedziby zamawiającego wymagane jest zapewnienie zakwaterowania i wyżywienia.

2. Szkolenie cyberbezpieczeństwa	
Miejsce	Sala konferencyjna w siedzibie zamawiającego
Ilość osób	24 w podziale na dwie grupy,
Rodzaj szkolenia	Stacjonarne, minimum 24 godziny lekcyjne wraz z pakietem materiałów szkoleniowych, w tym dostęp do maszyn wirtualnych
Termin	1-31 Października 2022
Wymagana tematyka:	1. Podstawowe zagrożenia związane z korzystaniem z internetu: phishing, ransomware, poczta e-mail, strony www, serwisy społecznościowe. 2. Reguły tworzenia i zmiany haseł do systemów informatycznych i aplikacji. 3. Bezpieczeństwo urządzeń mobilnych. 4. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne. 5. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia. 6. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych. 7. Prawidłowe korzystanie z oprogramowania antywirusowego. 8. Zasady aktualizacji programów i aplikacji. 9. Monitorowanie przez pracodawcę stanu bezpieczeństwa systemów informatycznych oraz działań podejmowanych przez użytkowników. 10. Szyfrowanie dokumentów w ramach dostępnych funkcji w pakiecie Microsoft Office (word, excel, power point). 11. Szyfrowanie dowolnego pliku programem zewnętrznym (na przykładzie aplikacji 7- zip, izarc, rar). 12. Prezentacja prawidłowych ustawień przeglądarki internetowej (na przykładzie google chrome oraz opera). 13. Przedstawienie alternatywnych rozwiązań zapewniających anonimowość i ochronę prywatności użytkowników (przeglądarka brave oraz wyszukiwarka duckduckgo). 14. Zasady bezpiecznego korzystania z poczty e-mail (pokaz praktyczny). 15. Ataki z wykorzystaniem stron WWW, w tym mediów społecznościowych 16. Ataki na pracowników - jak i kiedy sam pracownik ułatwia zadanie atakującym.
Dodatkowe wymagania	Zapewnienie 12 laptopów na czas szkolenia

3. Diagnoza cyberbezpieczeństwa
1) Przedmiotem zamówienia jest wykonanie Diagnozy Cyberbezpieczeństwa w ramach realizacji projektu zgłoszonego do Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia w Urzędzie Gminy w Rogowie. 2) Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. 3) Diagnoza musi być przeprowadzona w zakresie określonym w Regulaminie Konkursu Grantowego Cyfrowa Gmina, opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina, w szczególności w zakresie określonym w załączniku nr 8 do przedmiotowego Regulaminu „Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa”. 4) Termin wykonania zamówienia: Między 15 sierpnia 2022 a 15 września 2022