Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2024

Cyberbezpieczny Urząd

SZCZEGÓŁOWE WYMAGANIA TECHNICZNE

SPIS TREŚCI

1. INFORMACJE OGÓLNE

Niniejsza specyfikacja określa wymagania funkcjonalne i techniczne w zakresie dostawy i konfiguracji urządzeń bezpieczeństwa sieciowego wraz z serwerem oraz oprogramowaniem towarzyszącym stanowiącym jednolite rozwiązanie chroniące miejską sieć MAN przed atakami z cyberprzestrzeni. Projekt obejmuje fizycznie:

- 18 lokalizacji na terenie Gminy Żywiec, które korzystają z zasobów serwerowych Urzędu poprzez miejską sieć światłowodową,
- 4 lokalizacje na terenie Gminy Żywiec, które do połączenia z zasobami urzędu wykorzystują zestawiony szyfrowany tunel VPN realizowany za pośrednictwem dostępnego w danej lokalizacji operatora telekomunikacyjnego,
- lokalizację centralną znajdującą się w głównej serwerowni Urzędu Miasta Żywiec, Rynek 2.

Wykonawca podejmujący się realizacji przedmiotu zamówienia zobowiązany jest do:

- opracowania i przedstawienia Zamawiającemu do zatwierdzenia szczegółowego harmonogramu prac,
- dostawy i konfiguracji urządzeń bezpieczeństwa sieciowego do każdej z 22 lokalizacji objętych projektem,
- dostawy i konfiguracji do głównej serwerowni zlokalizowanej w Urzędzie Miasta Żywiec, Rynek 2, przełączników agregujących ruch z 22 lokalizacji wyniesionych wraz z centralnym urządzeń bezpieczeństwa sieciowego (dwa urządzenia połączone w klaster) oraz dedykowanym serwerem na którym Wykonawca zainstaluje niezbędne oprogramowanie monitorujące dostarczone w ramach niniejszego postępowania urządzenia,
- przeprowadzenie audytu bezpieczeństwa wdrożonej w ramach niniejszego postępowania infrastruktury IT.

Realizacja powyższego zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

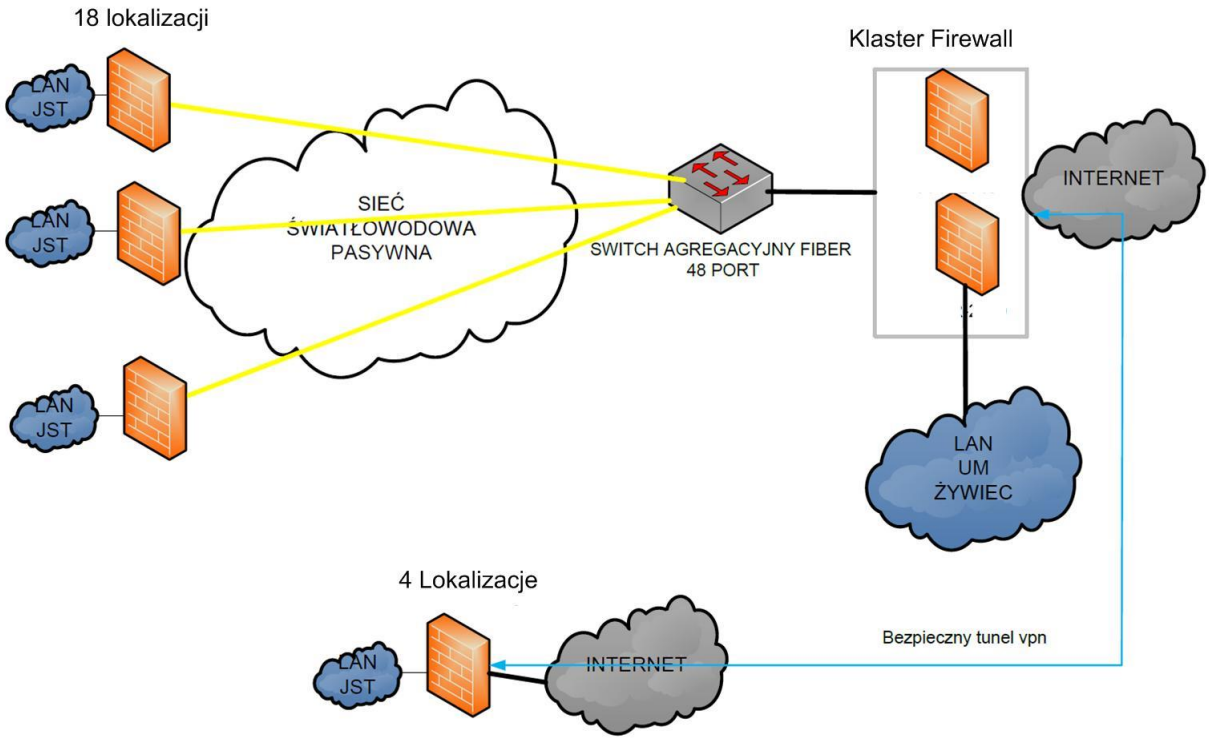
Celem budowy systemu teleinformatycznego jest zapewnienie bezpiecznego dostępu do zasobów sieciowych Urzędu Miasta Żywiec przy wykorzystaniu istniejących dedykowanych połączeń światłowodowych typu punkt (jednostka wyniesione) wielopunkt (urząd miast Żywiec) zestawionych dla 18 lokalizacji oraz 4 lokalizacji dla których połączenie realizowane będzie przy wykorzystaniu sieci internet zestawiając, wykorzystując dostarczony w niniejszym postępowaniu sprzęt i oprogramowanie, tunel VPN. Lista lokalizacji do podłączenie znajduje się w poniższej tabeli nr 1:

Lp.	Lokalizacja	Sposób połączenia do zasobów sieciowych UM
1.	Szkoła Podstawowa Nr 1 Żywiec ul. Księdza Prałata Stanisława Słonki 14	Światłowód
2.	Szkoła Podstawowa Nr 2 Żywiec ul. Zielona 1	Światłowód
3.	Szkoła Podstawowa Nr 3 Żywiec ul. M. Skłodowskiej-Curie 2	Światłowód
4.	Szkoła Podstawowa Nr 5 Żywiec ul. Powstańców Śląskich 4	Światłowód

5.	Szkoła Podstawowa Nr 9 Żywiec ul. Dworcowa 26	Światłowód
6.	Zespół Szkolno-Przedszkolny Nr 1 Żywiec ul. Moszczanicka 26	Internet/VPN
7.	Zespół Szkolno-Przedszkolny Nr 2 Żywiec ul. Niezapominajki 14	Internet/VPN
8.	Przedszkole Nr 1 Żywiec ul. Tetmajera 77	Radiolinia do SP1 / VPN
9.	Przedszkole Nr 6 Żywiec ul. Sporyska 37	Światłowód
10.	Przedszkole Nr 8 Żywiec ul. Grunwaldzka 17	Światłowód
11.	Przedszkole Nr 9 Żywiec ul. Poniatowskiego 12	Światłowód
12.	Przedszkole Nr 10 Żywiec ul. Kolonia Browar 44	Światłowód
13.	Przedszkole Nr 11 Żywiec Os. Parkowe 16	Światłowód
14.	Żłobek Miejski Nr 1 w Żywcu Ul. Jana 28 34-300 Żywiec	Internet/VPN
15.	Miejski Ośrodek Pomocy Społecznej ul. Zamkowa 10, 34-300 Żywiec	Światłowód
16.	Żywiecka Biblioteka Samorządowa ul. Kościuszki 5 34-300 Żywiec	Światłowód
17.	Miejski Ośrodek Sportu I Rekreacji ul. Zielona 7 34-300 Żywiec	Światłowód
18.	Miejskie Centrum Kultury Al. Wolności 4, 34-300 Żywiec	Światłowód
19.	Straż Miejska w Żywcu	Światłowód
20.	Urząd Stanu Cywilnego	Światłowód
21.	Pełnomocnik ds. alkoholowych	Światłowód
22.	Amfiteatr	Światłowód

(Tab.1)

Wszystkie połączenie agregowane są w serwerowni Urzędu Miasta Żywiec w lokalizacji Rynek 2. Fizyczne połączenia światłowodowe, internetowe oraz radioliniowe istnieją i nie są objęte niniejszym postępowaniem. Wykonawca w ramach postępowania zobligowany jest do uruchomiania bezpiecznych połączeń pomiędzy wyżej wymienionymi lokalizacjami a serwerownią Urzędu Miasta zgodnie z zamieszczonym poniżej schematem.



Rys.1

W każdej z 22 lokalizacji znajduje się szafka wisząca typu RACK w której należy zainstalować i skonfigurować zgodnie z wytycznymi Zamawiającego urządzenie typu firewall spełniające minimalne parametry techniczne opisane w dalszej części niniejszego opracowania. Zadaniem Wykonawcy jest dostarczenie również odpowiednich kabli, patchcordów i innych niezbędnych elementów pasywnych umożliwiających podłączenie istniejącej przełącznicy światłowodowej (złącze światłowodowe typu SC) z dostarczonym w ramach niniejszego postępowania sprzętu aktywnego tj. urządzenia bezpieczeństwa sieciowego (jednego dla danej jednostki podległej). Do głównej serwerowni zlokalizowanej w Urzędzie Miasta Żywiec należy dostarczyć dwa urządzenia bezpieczeństwa sieciowego zestawione w jeden klaster wraz z 48 portowym przełącznikiem światłowodowym oraz serwerem na którym zainstalowane będzie dedykowane przez producenta sprzętu oprogramowanie za pośrednictwem którego możliwe będzie zarządzanie, konfiguracja i monitoring dostarczonych w ramach niniejszego postępowania urządzeń typu firewall.

Niniejszy dokument zawiera tylko podstawowe i minimalne wymagania funkcjonalne i techniczne w zakresie elementów i rozwiązań przeznaczonych do realizacji projektu. Wykonawca może zaoferować sprzęt i rozwiązania dowolnego producenta, które spełniają minimalne wymagania określone w tym dokumencie. Jeśli w tym dokumencie znajdują się jakiekolwiek znaki towarowe, patent, czy pochodzenie to należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych o parametrach techniczno-użytkowych nie gorszych niż te podane w opisie przedmiotu zamówienia.
Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy, usługi lub prace spełniają wymagania określone przez Zamawiającego.

2. MINIMALNE WYMAGANIA TECHNICZNE

2.1. Serwer RACK – 1 sztuka

Dostawa, montaż i konfiguracja zgodnie z wytycznymi Zamawiającego

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	Serwer do zabudowy w szafie RACK w lokalizacji Urzędu Miasta Żywiec, Rynek 2
2	Płyta główna	Z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięci z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC, SDDC, Memory Mirroring Rank Sparing, SBEC.
3	Procesor	Wymagania minimalne: Zainstalowany co najmniej jeden procesor min. dwudziestoczterо- (24) rdzeniowy dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 292 punktów w teście SPECint_rate_base2017 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej. Zamawiający wymaga, aby powyższy wynik osiągnięty był w zgodzie co do procesora oraz rodziny zaoferowanego serwera. Pod pojęciem „rodzina” Zamawiający rozumie model o wspólnym modelu programowym i wielu odmianach implementacyjnych Wyniki testów należy złożyć wraz z ofertą.
4	Pamięć operacyjna	Minimum 128 GB pamięci RAM w modułach dwu lub czterobankowych
5	Sloty PCI Express/Porty	Wymagania minimalne: • min. 2 sloty PCIe w tym co najmniej jeden slot x16 generacji 5, • min. 3 portów USB z czego min. 1 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń), • min. 1x RS-232, • port video.
6	Wewnętrzna Pamięć masowa	Możliwość instalacji dysków twardych SATA, pamięci masowych: SSD, Flash PCI Express. Zainstalowane 3 dyski dyski 2,5 cala oparte o protokół NVMe o pojemności co najmniej 1,92 TB. Dodatkowo zainstalowane 2 dyski bootowalne o pojemności co najmniej 960GB ustawione w RAID 1 wraz z kartą kontrolera jeżeli takowa będzie konieczna do ich obsługi.
7	Kontroler Dysków	Zainstalowany sprzętowy kontroler dyskowy, możliwe konfiguracje poziomu RAID 5.

8	Grafika	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280 x 1024 pikseli.
9	Interfejsy sieciowe	Minimum dwa interfejsy sieciowe 1Gb/s oraz dodatkowo dwuportowa karta sieciowa zintegrowana z płytą bądź jako dodatkowa karta o przepływności minimum 10Gb moduł SFP+ obsługujący standard 10 Gigabit Ethernet.
10	Obudowa	Obudowa typu Rack o wysokości maksymalnie 2U z możliwością instalacji minimum 8 dysków 2.5" Hot Plug wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli.
11	Zasilacze i Wentylatory	Zainstalowane zasilacze muszą pracować w trybie redundancji Hot-Plug i charakteryzować się mocą nie większą niż 1200W każdy jednak nie mniejsze niż 1000 W. Ilość zainstalowanych wentylatorów pracujących w trybie redundancji Hot-Plug zapewniająca poprawne chłodzenie serwera nawet w przypadku jego maksymalnej rozbudowy.
12	Bezpieczeństwo i system diagnostyczny	• Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. • Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzącego z innych projektów sprzętu. • Zintegrowany z płytą główną moduł TPM. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
13	Karta zarządzająca	• Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność: komunikacja poprzez dedykowany interfejs RJ45, • podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging, • wbudowana diagnostyka oraz narzędzia do instalacji systemów operacyjnych, • dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, • lokalna oraz zdalna konfiguracja serwera, • zdalna instalacja systemów operacyjnych, • wsparcie dla IPv4 i IPv6, • zapis zrzutu ekranu z ostatniej awarii, • integracja z Active Directory,

		• wirtualna konsola z dostępem do myszy i klawiatury, • udostępnianie wirtualnej konsoli, • autentykacja poprzez publiczny klucz (dla SSH), • możliwość obsługi poprzez dwóch administratorów równocześnie, • wysyłanie do administratora powiadomienia o awarii lub zmianie konfiguracji sprzętowej, • dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć i umożliwiające automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów jak również posiadające moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
13	System operacyjny	System operacyjny w polskiej wersji językowej musi: • zawierać wszystkie potrzebne licencje w ilości zapewniającej pełną komunikację na poziomie serwera , z co najmniej 5 stacjami końcowymi. Dodatkowo wymaga się dostarczenie 5 licencji na stacje końcowe współpracujące z oferowanym systemem operacyjnym w wersji serwerowej, • być najwyższą możliwą wersją /edycją (aktualnie na dzień składania oferty) oferowaną przez producenta oprogramowania, która współpracuje z oferowanym serwerem, • pracować w roli klienta domeny Active Directory (AD), • możliwość uruchomienia roli: kontrolera domeny AD, serwera DHCP, serwera DNS, serwera NTP, usług www, pulpitów zdalnych dla klientów, serwera plików z uwierzytelnieniem i autoryzacja dostępu w domenie AD, • mieć możliwość uruchomienia serwera usługi aktualizacji systemu operacyjnego • mieć prawo do instalacji i użytkowania systemu operacyjnego na instancjach wirtualnych min. 2. • Uwaga: jeżeli wymaga tego licencja powinien zostać dostarczony z licencjami w ilości odpowiadającej wszystkim rdzeniom procesorów dla zaoferowanego w niniejszym postępowaniu serwera.
14	Certyfikaty i dokumenty	Wymagane w postępowaniu dokumenty: • Zaświadczenie dot. normy PN-EN ISO 9001 lub równoważne dla producenta oferowanego urządzenia. • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia. • Test procesora zgodnie z wymogami z punktu 3. • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 2 do 11.

15	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta, jego przedstawiciela lub Wykonawcy. Wymagane jest dołączenie nośnika ze sterownikami w formie trwałej lub linku do strony producenta / Wykonawcy umożliwiającej dostęp do najnowszych sterowników i uaktualnień.
16	Warunki gwarancji	Co najmniej **36 miesięcy gwarancji** realizowanej w miejscu instalacji sprzętu, z **czterogodzinnym czasem reakcji** od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24 x 7 x 365 poprzez ogólnopolską linię telefoniczną Wykonawcy lub producenta. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u Wykonawcy, producenta lub jego przedstawiciela. Dostępność wsparcia technicznego przez co najmniej 8 godz. co najmniej 5 dni roboczych w godz. co najmniej 8-16.

2.2. Przełącznik sieciowy 24 Porty SFP – 2 sztuki

Dostawa, montaż i konfiguracja zgodnie z wytycznymi Zamawiającego Przełącznika sieciowego 24-portowego SFP do zabudowy w szafie RACK – 2 sztuki pracujące w stosie.

Uwaga: każdy firewall zainstalowany w lokalizacji wyniesionej, która jest połączona z Urzędem Miasta Żywiec bezpośrednio światłowodem (18 lokalizacji) musi być zaterminowany dwoma linkami po jednym do jednego przełącznika 24 portowego SFP w celu zabezpieczenia połączenia na wypadek awarii jednego z połączeń lub jednego z dwóch dostarczonych w ramach niniejszego postępowania przełącznika sieciowego 24 porty SFP.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Parametry fizyczne	Przełącznik do zabudowy w szafie RACK w lokalizacji Urzędu Miasta Żywiec, Rynek 2 wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie wyższa niż 1U. Redundantne zasilanie 230V, maksymalny pobór mocy zestawu nie przekraczający 38 W. Średni czas bezawaryjnej pracy MTBF powyżej 10 lat.
2	Interfejsy sieciowe	• 24 porty GE RJ45 SFP obsadzone wkładkami min 1GE SFP+ typu long range, • 4 porty 10GE SFP+ (z obsługą wkładek 1GE) wraz z 4 wkładkami min. 10 GE SFP + typu short range.

3	Zarządzanie:	• Dedykowany interfejs do zarządzania. • Port konsoli szeregowej. • Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs przy użyciu przeglądarki internetowej. • Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników, • Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora, m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q. • Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników. • Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika. • Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika.
4	Parametry wydajnościowe	• przepustowość urządzenia – min. 128 Gbps, max. 204 Mpps, • możliwość zapamiętania co najmniej 32000 adresów MAC, • opóźnienie – poniżej 1 mikrosekundy, • bufor pakietów: min. 4 MB, • pamięć DRAM: min. 1 GB, • pamięć FLASH: min. 256 MB.
5	Wymagane funkcje	• możliwość automatycznej negocjacji prędkości i duplexu dla połączeń, • obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), • możliwość agregacji portów zgodna z 802.3ad, ilość grup min. 26, ilość portów w grupie: min. 8, • obsługa co najmniej 4000 VLANów, zgodna z 802.1Q, • możliwość wykonywania routingu statycznego, • możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2) – jeżeli funkcjonalność wymaga dodatkowej licencji, to nie jest ona wymagana do dostarczenia, • funkcje DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping, • port-mirroring, • obsługa sFlow, • obsługa list kontrolnych ACL, • wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation), • kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius, • zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, • Wsprarcie dla SNTP oraz LLDP (w trybie odbioru), • wsparcie dla SNMP w wersjach 1-3, • możliwość zarządzania przez interfejs graficzny i tekstowy, • możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI, • wsparcie dla HTTP REST API dla konfiguracji i monitoringu,

		• możliwość integracji z systemem bezpieczeństwa NGFW (Next Generation Firewall) polegającej na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie NGFW i filtracja tego ruchu z wykorzystaniem mechanizmów NGFW, np. IPS, AV, • możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników, • obsługa białych i czarnych list MAC, • stateful firewall, umożliwiający kontrolę dostępu do sieci, • routing statyczny i dynamiczny, co najmniej OSPF.
6	Gwarancja oraz wsparcie	**60 miesięcy gwarancji** producenta lub wykonawcy wraz z co najmniej **48-miesięcznym wsparciem** serwisowym. System powinien być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres **48 miesięcy**, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent lub Wykonawca nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
7	Dodatkowe wymagania	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2.3. Urządzenie bezpieczeństwa sieciowego – 2 sztuki połączone w klaster

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall,
- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	System bezpieczeństwa sieciowego typu Firewall do zabudowy w szafie RACK w lokalizacji Urzędu Miasta Żywiec, Rynek 2.
2	Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.
3	Interfejsy	System realizujący funkcję Firewall musi dysponować minimum: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps. • System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
4	Parametry wydajnościowe	• W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz min. 260 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – minimum 5 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 3 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.

5	Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być 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 oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami – Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. • Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
6	Polityki – Firewall	• Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. • Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. • Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.

7	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal – gdzie dostęp do chronionych zasobów jest realizowany za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
8	Routing i obsługa połączeń WAN oraz zarządzanie pasmem	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. • System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. • Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. • System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. • System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

9	Ochrona przed atakami i wirusami	• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. • Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10	Kontrola aplikacji i www	• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. • Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. • W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL – system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

11	Uwierzytelnianie użytkowników	System Firewall musi umożliwiać 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. • Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. • Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
12	Zarządzanie	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach co najmniej 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
13	Logowanie	• W ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG.

14	Gwarancja, serwis i licencje	• W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres co najmniej **48 miesięcy**. • System musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej **48 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. • Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
15	Certyfikaty i dokumenty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty /dokumenty • certyfikacje: ICSA lub EAL4 dla funkcji Firewall. • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia. • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 2 do 5.

2.4. Urządzenie bezpieczeństwa sieciowego – 18 sztuk

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. Wykonawca zobligowany jest dostarczyć, zainstalować, skonfigurować zgodnie z wytycznymi Zamawiającego oraz uruchomić po jednej sztuce urządzenia bezpieczeństwa sieciowego w jednej lokalizacji oznaczonej w tabeli nr 1 niniejszego opracowania jako lokalizacja połączona do zasobów sieciowych UM Światłowodem, w sumie 18 sztuk urządzeń ma zostać uruchomionych w 18 lokalizacjach połączonych już istniejący światłowodem z główną serwerownią UM Żywiec, a wszystkie funkcje związane m.in. z ochroną każdej z 18 istniejących infrastruktur sieciowej przed malware, szkodliwymi atakami, kontrolą aplikacji, filtracji i kontroli ruchu www odbywać się musi na dostarczonych i zainstalowanych w serwerowni UM Żywiec urządzeniach opisanych w punktach 2.3, 2.5, 2.6, tworząc jednolity system bezpieczeństwa.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 3 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall,
- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	System bezpieczeństwa sieciowego typu Firewall do zabudowy w szafie RACK w każdej z 18 lokalizacji zgodnie z tabelą nr 1 dot. pozycji wskazanych jako: Sposób połączenia do zasobów sieciowych UM – światłowód.
2	Redundancja, monitoring i wykrywanie awarii	• W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN.
3	Interfejsy	System realizujący funkcję Firewall musi dysponować minimum: • 8 portami Gigabit Ethernet RJ-45. • 2 porty SFP 1 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
4	Parametry wydajnościowe	• W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz min. 45 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,3 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – minimum 1,4 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 0,8 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 0,6 Gbps.
5	Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być 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 oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami – Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

		• Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Analiza ruchu szyfrowanego protokołem SSL
6	Polityki – Firewall	• Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
7	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal – gdzie dostęp do chronionych zasobów jest realizowany za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
8	Routing i obsługa połączeń WAN oraz zarządzanie pasmem	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9	Uwierzytelnianie użytkowników	System Firewall musi umożliwiać 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. • Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
10	Zarządzanie	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach co najmniej 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
11	Logowanie	• W ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG.

12	Gwarancja,	System musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej **48 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
13	Certyfikaty i dokumenty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty /dokumenty: • certyfikacje: ICSA lub EAL4 dla funkcji Firewall. • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia. • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 2 do 5.

2.5. Urządzenie bezpieczeństwa sieciowego – 4 sztuki

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. Wykonawca zobligowany jest dostarczyć, zainstalować, skonfigurować zgodnie z wytycznymi Zamawiającego oraz uruchomić po jednej sztuce urządzenia bezpieczeństwa sieciowego w jednej lokalizacji oznaczonej w tabeli nr 1 niniejszego opracowania jako lokalizacja połączona do zasobów sieciowych UM - VPN, w sumie 4 sztuk urządzeń ma zostać uruchomionych w 4 lokalizacjach połączonych już istniejący łączem radioliniowym lub internetowym. Należy zestawić bezpieczny tunel pomiędzy daną lokalizacją a urządzeniem bezpieczeństwa sieciowego dostarczonego w ramach niniejszego postępowania, opisanego w punkcie 2.3 i zainstalowanego w głównej serwerowni UM Żywiec a wszystkie funkcje związane m.in. z ochroną każdej z 4 istniejących infrastruktur sieciowej przed malware, szkodliwymi atakami, kontrolą aplikacji, filtracji i kontroli ruchu www musi odbywać się lokalnie na dostarczonym urządzeniu bezpieczeństwa sieciowego.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 3 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall,
- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

UWAGA: urządzenie musi spełniać wszystkie minimalne parametry techniczne opisane w punkcie 2.4 oraz dodatkowo opisane w tabeli poniżej:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	System bezpieczeństwa sieciowego typu Firewall do zabudowy w szafie RACK w każdej z 4 lokalizacji zgodnie z tabelą nr 1 dot. pozycji wskazanych jako: Sposób połączenia do zasobów sieciowych UM – VPN.
2	Ochrona przed atakami i wirusami	• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. • Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

3	Kontrola aplikacji i www	• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. • Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów UR pogrupowanych w kategorie tematyczne. • W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. • W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL – system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
4	Gwarancja, serwis i licencje	W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres co najmniej **48 miesięcy**. System musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej **48 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub www (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
5	Certyfikaty i dokumenty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty /dokumenty: • certyfikacje: ICSA lub EAL4 dla funkcji Firewall. • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia. • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 2 do 5.

2.6. Urządzenie służące do kompleksowej analizy i raportowania oraz zarządzania dziennikami zabezpieczeń – 1 sztuka

Dostarczone urządzenie odpowiedzialne musi być za centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa ze wszystkich urządzeń bezpieczeństwa sieciowego dostarczonych i zainstalowanych w ramach niniejszego postępowania. Wykonawca zobligowany jest dostarczyć, zainstalować, skonfigurować zgodnie z wytycznymi Zamawiającego oraz uruchomić opisywane urządzenie jako centralny system logowania raportowania i korelacji w lokalizacji serwerowni głównej UM Żywiec. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	Urządzenie do zabudowy w szafie RACK w lokalizacji Urzędu Miasta Żywiec, Rynek 2. Dopuszcza się montaż na specjalnej półce RACK z tym, że dostawa odpowiedniej półki jest po stronie Wykonawcy.
2	Przeznaczenie	Analiza zdarzeń w sieci obejmującej 22 lokalizacje wyniesione zgodnie z tabelą nr 1 oraz lokalizację główną UM Żywiec (Rynek 2).
3	Interfejsy, pamięć masowa	Wymagania minimalne: • 2 porty Gigabit Ethernet RJ-45. • Przestrzeń dyskowa o pojemności co najmniej 4 TB z zaimplementowanym mechanizmem zabezpieczającym przed utratą danych w przypadku awarii nośnika.
4	Parametry wydajnościowe	• System musi być w stanie przyjmować minimum 25 GB logów na dzień. • System musi być w stanie przeanalizować minimum 500 logów na sekundę. • Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.

5	Wymagania dla centralnego systemu logowania	• Podgląd logowanych zdarzeń w czasie rzeczywistym. • Możliwość przeglądania logów historycznych z funkcją filtrowania. • Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia. • System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej: ✓ Listę najczęściej wykrywanych ataków. ✓ Listę najbardziej aktywnych użytkowników/źródeł ruchu. ✓ Listę najczęściej wykorzystywanych aplikacji. ✓ Listę najczęściej odwiedzanych stron www. ✓ Listę krajów, do których nawiązywane są połączenia. ✓ Listę najczęściej wykorzystywanych polityk Firewall. ✓ Informacje o realizowanych połączeniach IPSec i SSL VPN. ✓ Listę najczęściej występujących zdarzeń systemowych. • Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. • Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514. • System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów. • System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.
6	Wymagania dla centralnego systemu raportowania	• Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. • Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. • Funkcję definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP. • Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń, a także z wybranej adresacji IP. • Możliwość automatycznego usuwania raportów po określonym czasie.

7	Wymagania dla centralnego systemu korelacji zdarzeń	• Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. • Możliwość tworzenia własnych reguł korelowania logów. • Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia. • Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: ✓ Malware/AV. ✓ Aplikacje sieciowe. ✓ Email. ✓ IPS. ✓ Web Filter. ✓ Traffic (logi z ruchu sieciowego). ✓ Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN). • Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa o wystąpieniu wybranych zdarzeń korelacji.
8	Zarządzanie	• System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI. • System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania. • System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów.
9	Gwarancja	System musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej **48 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.

10	Certyfikaty i dokumenty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty /dokumenty: • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia, • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 3 do 4.

2.7. System centralnego zarządzania systemami bezpieczeństwa NGFW - 1 sztuka

W ramach niniejszego postępowania wymagane jest dostarczenie systemu centralnego zarządzania przystosowanego do współpracy z systemami bezpieczeństwa sieciowego NGFW (Next Generation Firewall).

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1	Typ	Rozwiązanie w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Proxmox.
2	Przeznaczenie	Do centralnego zarządzania wszystkimi urządzeniami bezpieczeństwa sieciowego dostarczonymi w ramach niniejszego postępowania. UWAGA: Dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dopuszcza się wykorzystanie serwera dostarczonego w ramach niniejszego postępowania o parametrach opisanych w punkcie 2.1 niniejszego opracowania.
3	Interfejsy wraz z pozostałymi wymogami technicznymi	Wymagania minimalne: • System musi obsługiwać co najmniej 4 interfejsy sieciowe. • System musi obsługiwać co najmniej 4 vCPU. • System musi obsługiwać co najmniej 8 GB pamięci RAM. • System musi wspierać możliwość pracy w klastrze HA.
4	Parametry wydajnościowe	System musi umożliwiać zarządzenie co najmniej 24 systemami bezpieczeństwa NGFW.

5	Wymagania dla centralnego systemu zarządzania	• System centralnego zarządzania musi posiadać mechanizm zarządzania zmianami konfiguracji bazujący na osobnych rolach administratorów wykonujących konfigurację oraz rolach administratorów zatwierdzających zmiany, a także mechanizm audytu oraz porównywania konfiguracji i powiadamiania za pośrednictwem poczty elektronicznej o konfiguracji oczekującej na zatwierdzenie. • System centralnego zarządzania musi dawać możliwość pełnej konfiguracji zarządzanych systemów NGFW ze wszystkimi ich funkcjami składowymi. • System centralnego zarządzania musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram instalowania zmian). • System centralnego zarządzania musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej. • System centralnego zarządzania musi umożliwiać sprawdzenie spójności polityki firewall (w tym m.in. wykrywanie zduplikowanych obiektów). • System musi umożliwiać tworzenie dynamicznych obiektów (np. adresów IP), których wartość może być definiowana niezależnie per każdy zarządzany system bezpieczeństwa NGFW. • System centralnego zarządzania musi umożliwiać wyszukiwanie obiektów po ich nazwach oraz filtrowanie widoku polityki firewall na podstawie wybranych atrybutów reguł firewall. • System centralnego zarządzania musi umożliwiać przypisywanie tych samych polityk firewall, profili bezpieczeństwa, polityk SD-WAN oraz wybranych ustawień systemowych do wielu zarządzanych systemów bezpieczeństwa NGFW. • System centralnego zarządzania musi umożliwiać tworzenie wielu wspólnych bloków polityk firewall, tzn. zestawów reguł firewall, które mogą być wykorzystane w wielu odrębnych politykach firewall przypisanych do różnych systemów bezpieczeństwa NGFW. Administrator musi mieć możliwość umieszczenia takiego bloku w wybranym przez siebie miejscu polityki firewall. • System centralnego zarządzania musi wersjonować konfiguracje w taki sposób, aby możliwe było odtworzenie wybranej konfiguracji zainstalowanej w przeszłości na systemie bezpieczeństwa NGFW a obecnie przechowywanej w systemie centralnego zarządzania jako historyczna. • System centralnego zarządzania musi umożliwiać zarządzanie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania zarządzanych systemów NGFW. Administrator musi mieć możliwość określenia daty automatycznej aktualizacji oprogramowania dla wybranych zarządzanych systemów NGFW. • System centralnego zarządzania musi oferować możliwość aktualizacji baz sygnatur na zarządzanych systemach NGFW (zarządzane systemy NGFW nie muszą mieć dostępu do sieci Internet w celu aktualizacji swoich baz sygnatur). • System centralnego zarządzania musi umożliwiać podgląd licencji (wraz z terminem ich ważności) na zarządzanych systemach bezpieczeństwa NGFW. • System centralnego zarządzania musi umożliwiać zdalne wykonywanie skryptów na zarządzanych systemach bezpieczeństwa. W skryptach powinna być możliwość wykorzystania zmiennych, których wartości przypisywane są niezależnie dla każdego zarządzanego systemu bezpieczeństwa NGFW. • System centralnego zarządzania musi umożliwiać monitoring zarządzanych systemów NGFW w zakresie m.in. aktualnych tablic routingu, funkcjonalności DHCP server, SD-WAN (opóźnienie, jitter, straty pakietów), statusu tuneli VPN IPSec.

		• System centralnego zarządzania musi zawierać informacje, kiedy po raz pierwszy i kiedy po raz ostatni ruch przetwarzany przez zarządzane systemy NGFW trafił w poszczególne reguły polityki firewall. • System centralnego zarządzania musi umożliwiać zarządzanie systemami NGFW znajdującymi się za NAT. • System centralnego zarządzania musi umożliwiać uruchamianie systemów NGFW w trybie ZTP (Zero Touch Provisioning). • System musi optymalizować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh poprzez obiekty typu community/topologie VPN, umożliwiające proste dodawanie zarządzanych urządzeń w celu dołączenia ich do danej topologii VPN. • System zarządzania musi mieć możliwość pracy w trybie klastra niezawodnościowego, złożonego przynajmniej z dwóch elementów. Konfiguracja zarządzanych urządzeń musi być automatycznie synchronizowana pomiędzy wszystkimi elementami tego klastra. • System centralnego zarządzania musi mieć możliwość podziału na wirtualne systemy zarządzania (konteksty), które będą posiadały odrębne definicje obiektów. Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych wirtualnych systemów zarządzania. • System centralnego zarządzania musi umożliwiać pracę wielu administratorów jednocześnie System musi mieć możliwość blokady kontekstu (domeny administracyjnej), aby różni administratorzy nie mogli wykonywać w tym samym czasie zmian w tym samym kontekście. Administrator musi mieć także możliwość blokady tylko wybranej polityki firewall w obrębie całego kontekstu. • W przypadku pracy w trybie z kontekstami (domenami administracyjnymi) musi istnieć możliwość definiowania globalnych obiektów (np. adresów IP, portów TCP/UDP, profili bezpieczeństwa), które będą dostępne w wybranych kontekstach i gotowe do użycia np. w politykach firewall. • System musi pozwalać na włączanie lub wyłączanie widoczności w GUI systemu centralnego zarządzania wybranych elementów konfiguracji zarządzanych urządzeń. • System musi pozwalać na łatwą zamianę zarządzanego urządzenia NGFW, które uległo awarii, na nowe urządzenie tego samego modelu bez konieczności ponownego wykonywania jego pełnej konfiguracji czy ręcznego przenoszenia konfiguracji.
6	Zarządzanie w trybie pracy lokalnej	• System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI. • System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do wybranych elementów zarządzania oraz wybrania zarządzanych systemów dostępnych dla tego administratora. • Komunikacja pomiędzy systemem centralnego zarządzania a zarządzanymi systemami NGFW musi odbywać się w sposób szyfrowany. • System musi posiadać API, które umożliwia zarówno zarządzenie urządzeniami podłączonymi do systemu jak i samym systemem centralnego zarządzania.

7	Gwarancja	System musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej **48 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub www (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
8	Certyfikaty i dokumenty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty /dokumenty: • Deklaracja zgodności UE lub równoważna dla oferowanego urządzenia. • Dokument (karta katalogowa, oświadczenie producenta lub autoryzowanego przedstawiciela producenta) potwierdzający zaoferowane parametry w zakresie wskazanym w punktach od 3 do 4.

2.8. Centralny system służący do monitorowania bezpieczeństwa w systemach informatycznych (SIEM ang. Security Information and Event Managment) – 1 sztuka / licencja

Wymagania Ogólne

1). **Dostarczone platformy sprzętowe:** Dostawca zapewni niezbędne platformy sprzętowe z odpowiednio zabezpieczonym systemem operacyjnym, lub wykorzysta serwer dostarczony zgodnie z punktem 2.1 niniejszego opracowania.
2). **Architektura:** System będzie działał w architekturze klient-serwer, z agentami zbierającymi dane z urządzeń i przesyłającymi je do centralnego serwera (menadżera) do analizy i zarządzania.
3). **Uruchomienie i konfiguracja:** Dostawca jest zobowiązany do uruchomienia systemu SIEM w środowisku Zamawiającego oraz przeprowadzenia pełnej konfiguracji systemu, zapewniając jego poprawne działanie zgodnie z niniejszą specyfikacją.
4). Zaoferowany przez Wykonawcę system ma charakteryzować się następującymi minimalnymi cechami / funkcjami a jego głównym zadaniem jest:
- umożliwiać zbieranie i monitorowanie w czasie rzeczywistym zdarzeń bezpieczeństwa, takich jak nieautoryzowane logowania, zmiany plików, ataki sieciowe i inne niebezpieczne zachowania,
- pomagać w zarządzaniu zgodnością z różnymi regulacjami i standardami, takimi jak GDPR, HIPAA, PCI DSS i innymi,
- wspierać analizę zgodnie z MITRE ATT&CK,
- umożliwiać skalowania rozwiązania, w przypadku potrzeby rozbudowy rozwiązania,
- działać na zasadzie architektury klient-serwer, gdzie agenty zainstalowane na chronionych urządzeniach przesyłają dane do centralnego serwera (menadżera), który przeprowadza analizę i zarządzanie zdarzeniami,
- wspierać możliwość wykonywania programowalnych akcji "Active response",
- wspierać możliwość pracy bez-agentowej,
- wspierać możliwość zbierania logów przy użyciu protokołu syslog,

- posiadać agenta na systemy Windows, Linux i MacOS,
- oferować interaktywny interfejs, działający z przeglądarki bez potrzeby instalacji dodatkowego oprogramowania, pozwalający na łatwe przeglądanie i analizowanie danych zebranych przez system, oraz definiowanie własnych widoków,
- wbudowane reguły analizy,
- posiadać funkcjonalność FIM, rootkit detection,
- posiadać wsparcie dla "Security Configuration Assessment", z dynamicznie generowanym raportem,
- posiadać moduł do sprawdzania podatności zainstalowanego oprogramowania oparty o bazy NVD, dla systemów Windows, Linux,
- posiadać RESTful API,
- posiadać możliwość integracji z innymi rozwiązaniami np. Virus Total,
- posiadać możliwość wykonywania aktualizacji Offline,
- umożliwiać konfigurację alertów i powiadomień, które mogą być wysyłane za pomocą różnych kanałów, takich jak e-mail, Slack czy Webhook-i,
- umożliwiać zbieranie i analizę logów (poprzez wbudowane dashboard-y) z Office 365,
- wspierać monitorowanie i zabezpieczanie środowisk chmurowych, takich jak AWS, Azure i GCP, czy środowisk opartych o Docker-a,
- system ma nie mieć ograniczeń licencyjnych co do ilości zbieranych danych.

5). Uwagi dodatkowe:

- System SIEM powinien być łatwy w konfiguracji i obsłudze, z intuicyjnym interfejsem użytkownika.
- Dostawca powinien zapewnić wsparcie techniczne i szkolenia dla użytkowników.
- System powinien być regularnie aktualizowany, aby zapewnić ochronę przed najnowszymi zagrożeniami.

2.9. Audyt bezpieczeństwa systemów IT

Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa, którego celem jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa i oceny podniesienia poziomu bezpieczeństwa teleinformatycznego. Audytu (raport) musi obejmować realizację obowiązków, jakich od jednostki samorządu terytorialnego wymaga prawodawca.

Usługa oferowana przez Wykonawcę musi obejmować:

2.9.1. Audyt zerowy zgodności z KRI

– Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC):

- wyznaczenie osoby do kontaktu – Art. 21 KSC
- przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC
- zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC
- zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC
- zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC
- zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC
- opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI

- monitorowanie i przegląd SZBI – Par. 20 KRI
- doskonalenie SZBI – Par. 20 KRI
- aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI
- inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI
- przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI
- postępowanie z ryzykiem – Par. 20 pkt 3) KRI
- zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI
- szkolenia i uświadamianie – Par. 20 pkt 6) KRI
- monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI
- monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI
- zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI
- ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI
- zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI
- zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI
- zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI
- zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI
- ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – Par. 20 pkt 11) KRI
- aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI
- minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI
- ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI
- stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI
- zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI
- zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI
- kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI
- zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI.

– Opracowanie raportu z audytu.

2.9.2. Wdrożenie SZBI

Wdrożenie warsztatowe Systemu Zarządzania Bezpieczeństwem Informacji, które będzie polegało na zapewnieniu zgodności z wymaganiami KRI zgodnie z powyższymi punktami oraz sposobem działania jednostki. Wdrożenie ma obejmować procesy, procedury, dokumenty. Musi zostać przeprowadzane na podstawie wyników z audytu zerowego zgodności z KRI, który określi aktualny stan zgodności oraz wskaże punkty do doskonalenia. Wdrożenie opiera się na: KRI, UoKSC, ISO27001, ISO22301.

Wynikiem wdrożenia jest wprowadzony System Zarządzania Bezpieczeństwem Informacji, który będzie wykorzystywany w jednostce oraz pozwoli zapewnić zgodność podczas audytu końcowego.

2.9.3. Audyt końcowy zgodności z KRI/ISO 27001

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / normy ISO 27001
2. Opracowanie raportu z audytu
3. Uzupełnienie załącznika nr 6 – ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego.

Wymagania dla jednostki przeprowadzającej audyt:
Certyfikaty (co najmniej 2 audytorów posiadających, każdy z nich, co najmniej jeden z certyfikatów):

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 1854), w zakresie certyfikacji osób;
- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami w/w ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

3. PRZYGOTOWANIE DOKUMENTACJI POWYKONAWCZEJ

Wykonawca powinien przygotować dokumentację powykonawczą w formie papierowej i elektronicznej, która powinna zawierać:

Lp.	Nazwa	Wymaganie
1	Schematy sieci:	Szczegółowe schematy sieci logicznej i fizycznej, przedstawiające topologię sieci, rozmieszczenie urządzeń, połączenia kablowe. Dokumentacja zdjęciowa zainstalowanego sprzętu w poszczególnych lokalizacjach, wraz z zestawieniem nazwy, modelu i numerów seryjnych zainstalowanych urządzeń w każdej lokalizacji, zebrane w tabelę.
2	Konfiguracja serwerów, hypervisora:	Dokumentacja konfiguracji serwerów (hypervisor, system operacyjny, role serwerów, aplikacje zainstalowane), hasła dostępowe.
3	Parametry sprzętu	Specyfikacja techniczna wszystkich urządzeń sieciowych i serwerów producent, model, parametry techniczne).
4	Licencje	Informacje o licencjach na oprogramowanie i wsparcie serwisowe użyte w projekcie.