

## OPIS PRZEDMIOTU ZAMÓWIENIA – ZADANIE I

1. Przedmiotem umowy jest zakup i dostawa sprzętu komputerowego i oprogramowania wraz z usługą wdrożenia w ramach realizacji projektu „Cyberbezpieczne Wodociągi” realizowanego przez Gminny Zakład Gospodarki Komunalnej Trzebnica – ERGO Sp. z o.o.

Niniejsze zamówienia ma na celu podniesienie poziomu cyberbezpieczeństwa aby zapewnić odpowiedni poziom bezpieczeństwa kluczowych usług i zasobów Gminnego Zakładu Gospodarki Komunalnej Trzebnica – ERGO Sp. z o.o.

L.p.	Grupa	Przedmiot zamówienia	Ilość / jednostka miary
1.	Z1-IT	Serwer klastrowy	2 szt.
2.	Z1-IT	Macierz dyskowa	1 szt.
3.	Z1-IT/OT	Serwer do wykonywania kopii bezpieczeństwa	2 szt.
4.	Z1-IT/OT	Oprogramowanie do wykonywania kopii bezpieczeństwa	2 szt.
5.	Z1-IT	Przełącznik zarządzalny	2 szt.
6.	Z1-OT	Przełącznik zarządzalny PoE	2 szt.
7.	Z1-IT/OT	Zasilacz awaryjny (UPS)	2 szt.
8.	Z1-OT	Szafa RACK	1 szt.
9.	Z1-IT	UTM klastrowy	2 szt.
10.	Z1-OT	Zestaw UTM + Router wAP LTE	7 szt.
11.	Z1-IT/OT	Usługa wdrożeniowa	1 szt.
12.	Z1-IT	Antywirus Pro z XDR	1 szt.
13.	Z1-IT	Usługa bezpiecznej poczty SPF/DKIM/DMARC/DLP	1 szt.

### 1) Serwer klastrowy – 2 szt.

Nazwa	Minimalne wymagania
Obudowa	<ul style="list-style-type: none"> <li>• Typu RACK, wysokość nie więcej niż 1U;</li> <li>• Szyny umożliwiające wysunięcie serwera z szafy stelażowej;</li> <li>• Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;</li> <li>• Opcjonalne ramię porządkujące kable;</li> <li>• Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;</li> <li>• Zainstalowane 2 szt. dysków SSD 480GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID;</li> <li>• Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.</li> </ul>
Płyta główna	<ul style="list-style-type: none"> <li>• Dwuprocessorowa;</li> <li>• Wyprodukowana i zaprojektowana przez producenta serwera;</li> <li>• Możliwość instalacji procesorów 40-rdzeniowych;</li> <li>• Zainstalowany moduł TPM 2.0;</li> <li>• 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5; <ul style="list-style-type: none"> <li>▪ Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;</li> </ul> </li> <li>• 32 gniazda pamięci RAM;</li> <li>• Obsługa 6TB pamięci operacyjnej RAM DDR5;</li> <li>• Wsparcie dla technologii: <ul style="list-style-type: none"> <li>▪ Memory Scrubbing;</li> <li>▪ SDDC;</li> <li>▪ ECC;</li> <li>▪ Memory Mirroring;</li> <li>▪ ADDDC;</li> </ul> </li> <li>• Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug ;</li> <li>• BIOS UEFI w specyfikacji 2.7.</li> </ul>
Procesory	<p>Dwa procesory min. 8-rdzeniowe, taktowanie bazowe min. 2,5 GHz, architektura x86_64, osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 260 pkt (wynik osiągnięty dla zainstalowanych dwóch procesorów).</p> <p>Wynik musi być opublikowany na stronie <a href="http://spec.org/cpu2017/results/cpu2017.html">http://spec.org/cpu2017/results/cpu2017.html</a> dla dowolnego serwera.</p>



Pamięć RAM	<ul style="list-style-type: none"><li>• 128 GB pamięci RAM;</li><li>• DDR5 Registered</li></ul>
Kontrolery LAN	<ul style="list-style-type: none"><li>• Interfejsy LAN, :<ul style="list-style-type: none"><li>▪ 4x 1Gbit Base-T;</li></ul></li><li>• 2x 10Gbit SFP+.</li></ul>
Kontrolery I/O	<ul style="list-style-type: none"><li>• Kontroler RAID dla dysków wewnętrznych obsługujący RAID-1;</li></ul>
Porty	<ul style="list-style-type: none"><li>• Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera;</li><li>• 2 porty USB 3.0 dostępne z tyłu serwera;</li><li>• 2 porty USB 3.0 na panelu przednim;</li><li>• Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;</li><li>• Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy</li></ul>



	dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
Zasilanie, chłodzenie	<ul style="list-style-type: none"> <li>Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy min. 900W;</li> <li>Redundantne wentylatory hotplug.</li> </ul>
Zarządzanie	<ul style="list-style-type: none"> <li>Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; <ul style="list-style-type: none"> <li>informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: <ul style="list-style-type: none"> <li>karty rozszerzeń zainstalowane w dowolnym slotie PCI Express;</li> <li>procesory CPU;</li> <li>pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;</li> <li>status karty zarządzającej serwera;</li> <li>wentylatory;</li> <li>bateria podtrzymująca ustawienia BIOS płyty głównej;</li> <li>zasilacze;</li> <li>system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub baterijnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).</li> </ul> </li> </ul> </li> <li>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: <ul style="list-style-type: none"> <li>Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; <ul style="list-style-type: none"> <li>Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;</li> <li>Dostęp poprzez przeglądarkę Web, SSH;</li> <li>Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;</li> <li>Zarządzanie alarmami (zdarzenia poprzez SNMP)</li> <li>Możliwość przejęcia konsoli tekstowej</li> <li>Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)</li> <li>Obsługa serwerów proxy (autentykacja)</li> <li>Obsługa VLAN</li> <li>Możliwość konfiguracji parametru Max. Transmission Unit (MTU)</li> <li>Wsparcie dla protokołu SSDP</li> <li>Obsługa protokołów TLS 1.2, SSL v3</li> </ul> </li> </ul> </li> </ul>



	<ul style="list-style-type: none"> <li>▪ Obsługa protokołu LDAP</li> <li>▪ Integracja z HP SIM</li> <li>▪ Synchronizacja czasu poprzez protokół NTP</li> <li>▪ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej</li> <li>• Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); <ul style="list-style-type: none"> <li>• Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;</li> <li>• Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.</li> </ul> </li> </ul>
Wspierane OS	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2025, 2022, 2019;</li> <li>• VMWare vSphere 8.0;</li> <li>• Suse Linux Enterprise Server 15;</li> <li>• Red Hat Enterprise Linux 9,8;</li> <li>• Hyper-V Server 2019.</li> <li>• Ubuntu 22.04.</li> </ul>
Licencja na system operacyjny	<p>Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym i umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie 15 użytkownikom.</p> <p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> <li>1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</li> <li>2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</li> <li>4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem</li> </ol>



	<p>wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</p> <p>5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</p> <p>6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</p> <p>7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</p> <p>8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</p> <p>9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <ul style="list-style-type: none"> <li>a) pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> </ul> <p>10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>12) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET</p> <p>13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>14) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:</p> <ul style="list-style-type: none"> <li>a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b) Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.</li> </ul> <p>16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>18) Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> <li>a) Login i hasło,</li> <li>b) Karty z certyfikatami (smartcard)</li> </ul>
--	--



## Gwarancja

	<ul style="list-style-type: none"><li>• co najmniej 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Okres gwarancji stanowi pozacenowe kryterium oceny ofert. Oferta otrzyma punkty za wydłużony okres gwarancji.</li><li>• Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;</li><li>• Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych,</li><li>• Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;</li></ul>
Dokumentacja, inne	<ul style="list-style-type: none"><li>• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE;</li><li>• Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;</li><li>• W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;</li><li>• Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</li><li>• Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;</li><li>• Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.</li></ul>



## 2) Macierz dyskowa – 1 szt.

Nazwa	Minimalne wymagania
Ogólne	<ul style="list-style-type: none"><li>System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.</li><li>Macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach.</li><li>Macierz musi obsługiwać min. 48 dysków wykonanych w technologii hot-plug.</li><li>Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.</li></ul>
Pojemność macierzy	<ul style="list-style-type: none"><li>8 szt. dysków 1,8TB SAS 2.5"</li></ul>
Kontrolery	<ul style="list-style-type: none"><li>Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.</li><li>Każdy z kontrolerów macierzy musi posiadać po minimum 32GB pamięci podręcznej Cache.</li><li>W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.</li><li>Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 4TiB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD.</li><li>Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.</li><li>Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności</li></ul>





	<p>od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.</p> <ul style="list-style-type: none"> <li>• Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.</li> <li>• Oferowana macierz musi mieć wyprowadzone 4 portów dualnych iSCSI 10Gbps i 4 portów iSCSI 25Gbps do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID.</li> </ul>
Poziomy RAID	<ul style="list-style-type: none"> <li>• Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: <ul style="list-style-type: none"> <li>▪ Raid-1</li> <li>▪ Raid-10</li> <li>▪ Raid-5</li> <li>▪ Raid-6</li> </ul> </li> <li>• Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.</li> <li>• Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.</li> <li>• Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi.</li> </ul>
Dyski	<ul style="list-style-type: none"> <li>• Oferowana macierz musi wspierać dyski hot-plug: <ul style="list-style-type: none"> <li>▪ dyski elektroniczne SSD</li> <li>▪ mechaniczne HDD z interfejsem SAS12Gb/s</li> <li>▪ dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,</li> </ul> </li> <li>• Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug.</li> </ul>



	<ul style="list-style-type: none"><li>• Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.</li><li>• Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy).</li><li>• W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).</li><li>• Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).</li><li>• Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem bezpiecznego ponownego użycia w innym środowisku (Secure Erase).</li></ul>
Opcje programowe	<ul style="list-style-type: none"><li>• Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 256 kopii migawkowych.</li><li>• Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączenia macierzy oraz bez konieczności wyłączenia ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów.</li><li>• Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.</li></ul>



	<ul style="list-style-type: none"> <li>• Macierz musi posiadać wsparcie dla systemów operacyjnych: <ul style="list-style-type: none"> <li>○ Microsoft Windows Server 2016, 2019, 2022</li> <li>○ SuSE Linux Enterprise Server 15, 12</li> <li>○ Red Hat Linux Enterprise Server 9, 8, 7</li> <li>○ Oracle Linux 9, 8, 7</li> <li>○ Solaris 11</li> <li>○ Vmware vSphere 7.0, 8.0;</li> </ul> </li> <li>• Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.</li> <li>• Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.</li> <li>• Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych).</li> <li>• Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.</li> </ul>
Zarządzanie	<ul style="list-style-type: none"> <li>• Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej.</li> <li>• Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.</li> <li>• Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.</li> <li>• Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.</li> <li>• Wraz z systemem musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:</li> </ul>



	<ul style="list-style-type: none"> <li>o wydajności i opóźnień na wolumenach</li> <li>o wydajności I/Ops, MB/s</li> <li>o trafności w cache</li> <li>• Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.</li> <li>• Macierz musi posiadać oprogramowanie pozwalające na integrację Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter</li> <li>• Macierz musi posiadać wsparcie dla VMware vSphere Storage APIs Array Integration (VAAI)</li> </ul>
Gwarancja i serwis	<ul style="list-style-type: none"> <li>• Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem wizyty technika do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. Okres gwarancji stanowi pozacenowe kryterium oceny ofert. Oferta otrzyma punkty za wydłużony okres gwarancji.</li> <li>• Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.</li> <li>• Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.</li> <li>• Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia.</li> <li>• Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).</li> <li>• Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia.</li> </ul>



GMINA  
TRZEBNICA  
trzebnica.pl

### 3) Serwer do wykonywania kopii bezpieczeństwa – 2 szt.



GMINNY  
ZAKŁAD  
GOSPODARKI  
ENERGETYCZNEJ

Nazwa	Minimalne wymagania
Obudowa	<ul style="list-style-type: none"> <li>• Typu RACK, wysokość 1U;</li> </ul>
	<ul style="list-style-type: none"> <li>• Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy;</li> <li>• Możliwość zainstalowania 4 dysków twardych hot plug 2,5”;</li> <li>• Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;</li> <li>• Zainstalowane 2 szt. dysków SSD 480GB podpięte do sprzętowego kontrolera RAID 1;</li> <li>• Możliwość zainstalowania dysku M.2 NVMe bezpośrednio na płycie głównej;</li> <li>• Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.</li> </ul>
Płyta główna	<ul style="list-style-type: none"> <li>• Wyprodukowana i zaprojektowana przez producenta serwera;</li> <li>• Możliwość instalacji procesorów 8-rdzeniowych;</li> <li>• Zainstalowany moduł TPM 2.0;</li> <li>• Złącza PCI Express: <ul style="list-style-type: none"> <li>▪ 2 fizyczne złącza PCIe 5.0 o prędkości x8;</li> <li>▪ Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości;</li> </ul> </li> <li>• 4 gniazda pamięci RAM;</li> <li>• Obsługa minimum 128 GB pamięci RAM DDR5 ECC;</li> <li>• Możliwość instalacji 2 dysków M.2 NVMe skonfigurowanych w RAID-1 na płycie głównej lub dedykowanej karcie PCI Express, dyski nie mogą zajmować klatek dla dysków hot-plug.</li> </ul>
Procesory	<ul style="list-style-type: none"> <li>• Zainstalowany jeden procesor 8-rdzeniowy, taktowanie bazowe min 3,0 GHz, architektura x86_64; osiągający w teście Average CPU Mark 30 000 pkt. Wynik musi być dostępny na stronie <a href="https://www.cpubenchmark.net">https://www.cpubenchmark.net</a></li> </ul>
Pamięć RAM	<ul style="list-style-type: none"> <li>• 64GB pamięci RAM;</li> <li>• DDR5 ECC 4800MT/s;</li> <li>• Pamięci obsadzone w trybie dwukanałowym.</li> </ul>
Kontrolery LAN	<p>Interfejsy LAN,:</p> <ul style="list-style-type: none"> <li>• 2x 1Gbit Base-T;</li> <li>• 2x 10Gbit SFP+.</li> </ul>
Kontrolery I/O	Brak wymagań
Porty	<ul style="list-style-type: none"> <li>• Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera;</li> <li>• 4x USB 3.2 Gen1 Type A wyprowadzone na tył obudowy</li> </ul>

	<ul style="list-style-type: none"> <li>• 2x USB 3.2 Gen1 Type A + 1x USB3.2 Gen2x2 Type C wyprowadzone na przód obudowy</li> <li>• 5x SATA 6G</li> <li>• Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;</li> <li>• Ilość dostępnych złączy USB/SATA nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.</li> </ul>
Zasilanie, chłodzenie	<ul style="list-style-type: none"> <li>• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy min. 450W;</li> </ul>
Zarządzanie	<ul style="list-style-type: none"> <li>• Wbudowane diody informacyjne lub wyświetlacz informujący o stanie serwera - system przewidywania, rozpoznawania awarii;</li> <li>• Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: <ul style="list-style-type: none"> <li>▪ karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express;</li> <li>▪ procesory CPU;</li> <li>▪ pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;</li> <li>▪ status karty zarządzającej serwerem;</li> <li>▪ wentylatory;</li> <li>▪ bateria podtrzymująca ustawienia BIOS płyty głównej;</li> <li>▪ zasilacze;</li> </ul> </li> <li>• Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: <ul style="list-style-type: none"> <li>▪ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;</li> <li>▪ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;</li> <li>▪ Dostęp poprzez przeglądarkę Web, SSH;</li> </ul> </li> <li>• Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; <ul style="list-style-type: none"> <li>▪ Zarządzanie alarmami (zdarzenia poprzez SNMP);</li> </ul> </li> <li>• Możliwość przejęcia konsoli tekstowej;</li> <li>▪ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);</li> <li>• Obsługa serwerów proxy (autentykacja);</li> <li>▪ Obsługa VLAN;</li> <li>• Możliwość konfiguracji parametru Max. Transmission Unit (MTU);</li> <li>• Wsparcie dla protokołu SSDP;</li> </ul>



	<ul style="list-style-type: none"> <li>• Obsługa protokołów TLS 1.2, SSL v3;</li> <li>• Obsługa protokołu LDAP;</li> <li>• Integracja z HP SIM;</li> <li>• Synchronizacja czasu poprzez protokół NTP;</li> <li>• Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;</li> <li>• Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjną);</li> <li>• Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;</li> <li>• Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.</li> </ul>
Wspierane OS	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2022;</li> <li>• VMWare vSphere 8.0;</li> <li>• Suse Linux Enterprise Server 15;</li> <li>• Red Hat Enterprise Linux 9, 8;</li> <li>• Ubuntu 22.04.</li> </ul>
Gwarancja	<ul style="list-style-type: none"> <li>• co najmniej 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Okres gwarancji stanowi pozacenowe kryterium oceny ofert. Oferta otrzyma punkty za wydłużony okres gwarancji.</li> <li>• Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;</li> <li>• Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;</li> <li>• Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;</li> <li>• Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat</li> </ul>





GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

w trybie onsite z gwarantowanym skutecznym zakończeniem



KRAJOWY  
PLAN  
ODBUDOWY



Rzeczpospolita  
Polska

Sfinansowane przez  
Unię Europejską  
NextGenerationEU





naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja,  
inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z normami: CB, RoHS, WEEE oraz CE.



GMINA  
TRZEBNICA  
trzebnica.pl

Licencja na system  
operacyjny

	<p>Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym i umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie 15 użytkownikom.</p> <p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</p> <p>5) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</p> <p>6) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</p> <p>7) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</p> <p>8) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem</p>
--	--



wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

10) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

11) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

12) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

13) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

14) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

- a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
- b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

16) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

17) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

18) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

19) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.

20) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

21) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

- a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
- b) Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.

19) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

20) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

21) Mechanizmy logowania w oparciu o:

- a) Login i hasło,
- b) Karty z certyfikatami (smartcard)

Dostawa licencji oprogramowania do zabezpieczania danych, tworzenia kopii zapasowych oraz replikacji środowisk IT w formie subskrypcji na okres min. 24 miesięcy

Model licencjonowania:

Uniwersalna licencja subskrypcyjna (Universal License), umożliwiająca ochronę różnych typów obciążeń (maszyny wirtualne, serwery fizyczne, stacje robocze, aplikacje chmurowe) w ramach jednej puli licencji.

Licencje muszą umożliwiać swobodne przenoszenie między chronionymi zasobami bez konieczności kontaktu z producentem lub zakupu nowych jednostek (tzw. licencjonowanie przenośne).

Ilość: pakiet dla 20 instancji

Rozwiązanie nie może posiadać ograniczenia co do maksymalnej liczby zakupionych licencji w obrębie jednej organizacji (brak limitu typu "Small Business").

Oprogramowanie musi oferować pełen zakres funkcjonalności, w tym:

**Tworzenie kopii zapasowych:** Obsługa środowisk zwirtualizowanych (np. VMware vSphere, Microsoft Hyper-V) oraz fizycznych (Windows, Linux, Unix) z wykorzystaniem mechanizmów przyrostowych i deduplikacji.

**Odzyskiwanie danych:** Funkcja natychmiastowego uruchamiania maszyn wirtualnych bezpośrednio z pliku kopii zapasowej (Instant VM Recovery) oraz odzyskiwanie granularne obiektów aplikacji (np. Active Directory, SQL Server, Exchange, SharePoint).

**Replikacja i DR:** Wbudowana replikacja maszyn wirtualnych do zapasowej lokalizacji oraz funkcja akceleracji przesyłu danych przez sieć WAN.

**Ochrona przed Ransomware:** Obsługa niezmiennych repozytoriów kopii zapasowych (Immutability), uniemożliwiająca usunięcie lub zaszyfrowanie danych przez złośliwe oprogramowanie.

**Bezpieczne przywracanie:** Automatyczne skanowanie kopii zapasowych pod kątem obecności wirusów i złośliwego kodu przed ich przywróceniem do środowiska produkcyjnego (Secure Restore).

**Weryfikacja kopii:** Mechanizm automatycznego testowania poprawności wykonanych backupów poprzez ich próbne uruchomienie w izolowanym środowisku (np. SureBackup).

#### 5) Przełącznik zarządzalny – 2 szt.

Nazwa	Minimalne wymagania
Porty	min. 16 portów SFP+
Typ przełącznika	Zaawansowany, Zarządzany L3/L2+
Obudowa	Typu RACK 19", zestaw do montażu w szafie RACK 19"
Możliwości zarządzania	Support SNMPv1/v2/v3, SSH2.0, SSLv3 and OAM Support CLI (Command Line Interface), web management, Telnet and FTP connection



GMINA  
TRZEBNICA

Funkcje	Agregacja łączy, Zabezpieczenia STP, Wykrywanie pętli zwrotnych na portach oraz VLAN, Kontrola przepływu, Port Mirroring, MAC ACL, IP
	ACL, Wiązanie adresów IP, MAC i portów, Routing statyczny na poziomie min. 48 tras statycznych i min. 128 wpisów ARP, Automatyczne wykrywanie urządzeń, Inteligentne monitorowanie stanu sieci, Ostrzeżenia o nietypowych zdarzeniach, Diagnostyka kabli, Logi systemowe
Wydajność przełączania	min. 320 Gb/s
Zasilanie	Hot-swap dwa redundantne zasilacze
Gwarancja	min. 3 lata

#### 6) Przełącznik zarządzalny POE – 2 szt.

Nazwa	Minimalne wymagania
Porty	min. 16 portów min 8 portów POE, 2 porty SFP
Typ przełącznika	Zarządzany
Obudowa	Typu RACK 19", zestaw do montażu w szafie RACK 19"
Możliwości zarządzania	web management, Telnet and FTP connection
Funkcje	Agregacja łączy, Zabezpieczenia STP, Wykrywanie pętli zwrotnych na portach oraz VLAN, Kontrola przepływu, Port Mirroring, MAC ACL, IP
Wydajność przełączania	min. 35 Gb/s
Zasilanie	Zasilacz min. 60W
Gwarancja	min. 3 lata

#### 7) Zasilacz awaryjny (UPS) – 2 szt.

Nazwa	Minimalne wymagania
Moc pozorna	min. 2000VA
Moc rzeczywista	min. 2000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	93%
Typ obudowy	rack/tower
Ilość wydzielanego ciepła dla nominalnych warunków pracy	< 520 BTU / h
Napięcie wejściowe	110 ÷ 300 V AC ± 2%
Częstotliwość napięcia wejściowego	50 / 60 Hz
Zakres napięcia wyjściowego	200 V AC / 208 V AC / 220 V AC / 230 V AC / 240 V AC ± 2 %
Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – UPS	0ms



Współczynnik odkształceń prądu wyjściowego THDI	< 1% (liniowe), < 5% (nieliniowe)
Napięcie wyjściowe	~230V
Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 0,1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie wyjściowe	Praca falownikowa – elektroniczne zwarciove i przeciążeniowe
Zabezpieczenie wejściowe	Przeciwwprzeięciowe
Akumulatory wewnętrzne w UPS	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania dla obciążenia 1000W	minimum 240 min
Czas ładowania baterii wew w UPS - po 80% wyładowaniu baterii	≤ 3 h
<b>pozostałe</b>	
Przeciążalność	100 ÷ 105 - ostrzeżenie (praca normalna); 105 ÷ 125 - 5 min; 125 ÷ 150 - 30 s; > 150 ÷ - 500 ms
Wejście zasilania	1 x IEC 320 C20 (16 A)
Ilość i typ gniazd wyjściowych	min 8x IEC 320 C13 (10 A), z czego minimum 4 gniazda sterowalne
Sygnalizacja	Wyświetlacz LCD
Test baterii	wymagana możliwość uruchomienia testu baterii z poziomu menu zasilacza
Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia do 4 zewnętrznych modułów bateryjnych
Możliwość pracy w trybie konwertera częstotliwości	wymagane
Interfejs komunikacyjny	RS232, sieciowa karta zarządzająca SNMP/HTTP ( <b>wymagane</b> ), styki bezpotencjałowe: wejściowe (1), wyjściowe (1), MODBUS TCP, USB (2.0) HID
Przewody	min 1szt USB + 1szt IEC 320 C13-C14 10A
Wsporniki do montażu w szafie RACK	wymagane
Złącze EPO	wymagane ustawienie NC
Waga UPS	do 26 kg
Waga pojedynczego MODUŁU BATERYJNEGO - jeżeli występuje	do 40 kg
Wymiary UPS w wersji RACK	nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 600mm
Wymiary pojedynczego MODUŁU BATERYJNEGO w wersji RACK - jeżeli występuje	nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 600mm
Wysokość rozwiązania w szafie rack	nie więcej niż 10 U
Gwarancja	minimum 36 miesięcy na elektronikę i 36 miesięcy na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	naprawa w maksymalnie 5 dni roboczych
	serwis realizowany w systemie door to door





	Tego samego producenta co UPS, bezpłatnie, bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPSów
	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.
	Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
	możliwość zarządzania różnymi UPSami tego samego producenta
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
Oświadczenia / dokumenty	deklaracja CE producenta sprzętu
	oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
	gwarancja ma być realizowana wyłącznie przez serwis producenta - należy przedstawić odpowiednie oświadczenie producenta



GMINA  
TRZEBNICA  
trzebnica.pl

## 8) Szafa Rack



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

### Szafa teleinformatyczna stojąca 19" 42U

Przeznaczenie: Montaż urządzeń w standardzie 19 cali, serwerów oraz osprzętu sieciowego.

Wysokość montażowa: min. 42U.

Wymiary zewnętrzne: Szerokość min. 800 mm, Głębokość min. 1000 mm.

Konstrukcja: Solidna, stalowa, skrucana lub spawana rama o wysokiej nośności (min. 800 kg).

Drzwi:

Przednie: perforowane (wysoki stopień wentylacji), wyposażone w zamek z klamką.

Tylne: dwuskrzydłowe, perforowane, zamykane na klucz.

Panele boczne: Zdejmowane, z możliwością montażu zamka.

Kolor: Czarny (RAL 9004 lub zbliżony).

Wyposażenie: Kółka transportowe z hamulcem oraz nóżki, zestaw śrub montażowych, panel wentylacyjny z 6 wentylatorami, 2 pionowe organizery kabli.

## 9) UTM klastrowy z pakietem serwisowym

Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive.

### OBSŁUGA SIECI

1. 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)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interfejs (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.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.



9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzna oraz zewnętrzna), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

### **INTRUSION PREVENTION SYSTEM (IPS)**

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. 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.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.



1. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

2. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

### **KSZTAŁTOWANIE PASMA (Traffic Shapping)**

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

### **OCHRONA ANTYWIRUSOWA**

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
4. Skaner antywirusowy ma pochodzić od europejskiego producenta.
5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
6. 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 ANTYSYSPAM**

1. 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)**

1. 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,  
TRZEBNICA  
SSL VPN.



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

1. SSL VPN ma działać w trybie tunelu.
2. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
3. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
4. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
5. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
6. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

#### FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
4. Administrator ma mieć możliwość dodawania własnych kategorii URL.
5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  6. blokowanie dostępu do adresu URL,
  7. zezwolenie na dostęp do adresu URL,
  8. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
9. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
10. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
11. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
12. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
13. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
14. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

#### 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.



Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

1. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
2. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
3. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
4. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

### ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

Mechanizm równoważenia obciążenia łączy 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 łącznie zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).

Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.

W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.

### ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącznie zapasowe w przypadku awarii łączy podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.

### ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.





1. GMINA  
TRZEBNICA  
trzebnica.pl

Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

2. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH)
3. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
4. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
5. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
6. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
7. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
8. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).
9. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
10. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
11. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
12. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

## RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).





## POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
7. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
8. Urządzenie musi mieć zaimplementowane Open API.
9. 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

1. Urządzenie ma być objęte 60-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

## PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min.4.
4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
5. Przepustowość Firewall (1518 bajtów UDP) – minimum 3Gbps.
6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.
7. Przepustowość filtrowania Antywirusowego – minimum 300Mbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
9. Przepustowość tunelu SSLVPN – minimum 200Mbps.
10. Liczba tuneli VPN IPSec – minimum 50.
11. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 25.
12. Obsługa interfejsów 802.11q (VLAN) – minimum 128.
13. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 15 000 nowych sesji/sekundę.
14. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
15. Urządzenie nie ma limitu na liczbę użytkowników.
16. Liczba reguł filtrowania – minimum 1024.
17. Liczba tras statycznego routingu – minimum 512.
18. Liczba tras dynamicznego routingu – minimum 10 000.
19. Urządzenie musi posiadać pasywny system chłodzenia.
20. Urządzenie ma być przystosowane do pracy w temperaturach od -20oC do +60oC przy wilgotności od 0% do 95% (bez kondensacji).
21. Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 50,1 lat.
22. Urządzenie musi być wyposażone w moduł TPM.

## 10) Zestaw UTM z pakietem serwisowym + Router wAP LTE

### OBSŁUGA SIECI

1. 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)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. 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.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

### INTRUSION PREVENTION SYSTEM (IPS)

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. 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.



8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. 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).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

#### **KSZTAŁTOWANIE PASMA (Traffic Shapping)**

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

#### **WIRTUALNE SIECI PRYWATNE (VPN)**

1. 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 w trybie tunelu.

Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.

Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

#### **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.
- Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).



GMINA  
TRZEBNICA  
trzebnica.pl



- Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
- Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

### ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

Mechanizm równoważenia obciążenia łączy 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 łącznie zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).

Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.

W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

Monitorowanie dostępności łączy 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 łącznie zapasowe w przypadku awarii łączy podstawowego.
- Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
- Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.

### 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 niezasyfrowany 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.



1. GMINA  
TRZEBNICA

Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

2. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH).
3. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
4. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
5. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
6. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
7. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
8. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).
9. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
10. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
11. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
12. 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 serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

## RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
4. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
5. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
6. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
7. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
8. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).





## POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przysyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć zaimplementowane Open API.
10. 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

1. Urządzenie ma być objęte 60-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

## PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
3. Liczba portów Ethernet 10/100/1000Mbps – min. 2, z możliwością rozszerzenia do 4.
4. Urządzenie ma pozwalać na dodanie min. 2 portów światłowodowych 1Gbps.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 2.4Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 0,6 Gbps.
9. Liczba tuneli VPN IPSec – minimum 100.
10. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
11. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
12. Liczba równoczesnych sesji – minimum 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.
13. Liczba reguł filtrowania – minimum 8 192.
14. Liczba tras statycznego routingu – minimum 2 048.
15. Liczba tras dynamicznego routingu – minimum 10 000.
16. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
17. Urządzenie musi być wyposażone w moduł TPM.
18. Urządzenie ma posiadać pasywny system chłodzenia.
19. Urządzenie ma posiadać redundantne zasilanie DC, 2x12-48VDC.
20. Urządzenie ma być przystosowane do pracy w temperaturach od -40oC do +70oC przy wilgotności od 0% do 95% (bez kondensacji).
21. Obudowa urządzenia ma zapewniać ochronę wg. kodów IP – IP30.



1. Urządzenie ma pozwalać na aktywowanie funkcjonalności tzw. hardware bypass, tj. zapewnienie ciągłości transmisji pomiędzy dwoma dedykowanymi interfejsami Ethernet pomimo awarii sprzętowej lub programowej urządzenia.

2. Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 35.1 lat.
3. Urządzenie nie ma limitu na liczbę użytkowników.
4. Urządzenie ma umożliwiać bezpośredni montaż na szynie typu DIN (35mm).

#### **Dołączony Router wAP LTE**

Typ: bezprzewodowy punkt dostępu z wbudowanym modemem obsługującym połączenia 2G, 3G i 4G (LTE).  
wbudowany moduł radiowy pracujący w standardzie 802.11b/g/n oraz 1x port Fast Ethernet 10/100 Mb/s  
PoE-in

możliwość transmisji sieci bezprzewodowej WiFi w paśmie 2,4 GHz

kompatybilność ze standardami 802.11 b/g/n

2x2 MIMO, anteny WiFi o zysku 2 dBi

moduł LTE z jednym slotem SIM

antena LTE o zysku 4 dBi

obsługa 2G, 3G i 4G

możliwość montażu na zewnątrz budynków

różne sposoby zasilania

system RouterOS z licencją Level 4

Pamięć RAM min DDR2 64MB oraz wbudowana 16 MB Flash

#### **11) Usługa wdrożeniowa**

Usługi wdrożeniowa (instalacja, konfiguracja i migracja do nowego klastra)

Usługa polegająca na wdrożeniu rozwiązań cyberbezpieczeństwa zakupionych w ramach niniejszego postępowania z zachowaniem ciągłości pracy systemu. W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług:

Wykonawca stworzy plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający wytyczne Zamawiającego.

- montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów,
- uruchomienia systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera,
- podłączenia serwerów, macierzy do przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera,
- testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania,
- konfiguracji środowiska,
- migracji maszyn wirtualnych (max. 5 maszyn) do nowego klastra
- instalacji i konfiguracji rozwiązań cyberbezpieczeństwa zakupionych w ramach niniejszego postępowania.



## 12) Oprogramowanie antywirusowego z XDR

Podniesienie do wyższej wersji posiadanego przez Zamawiającego oprogramowania wraz z jednoczesnym rozszerzeniem licencji o 5 stanowisk. Zamawiający wymaga licencji ważnej do min. 28.05.2029 r.

### Administracja zdalna

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
  - 5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
  - 5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
  - 5.3. Buforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
  - 7.1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    - 7.1.1. Google Authenticator,
    - 7.1.2. Microsoft Authenticator,
    - 7.1.3. Authy,
    - 7.1.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
  - 9.1. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:



GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

9.1.1. adresy sieciowe IP,

9.1.2. aktywne zagrożenia,

9.1.3. stan funkcjonowania oraz ochrony,

9.1.4. wersja systemu operacyjnego,

9.1.5. podzespoły komputera.

10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:

10.1. wyrażenie CRON,

10.2. codziennie,

10.3. cotygodniowo,

10.4. co miesiąc,

10.5. co rok,

10.6. po wystąpieniu nowego zdarzenia,

10.7. po automatycznym umieszczeniu hosta w grupie dynamicznej.

11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim

11.1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania

12. Rozwiązanie musi mieć możliwość tagowania obiektów.

13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

13.1. Eksport danych musi być możliwy w co najmniej następujących formatach:

13.1.1. JSON,

13.1.2. LEEF,

13.1.3. CEF.

14. Rozwiązanie musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania.

#### Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,



GMINA  
TRZEBNICA  
trzebnica.pl

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.

7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.

7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.

7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).

7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.

8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

10.1. całego dysku,

10.2. wybranych katalogów,

10.3. pojedynczych plików,

10.4. plików spakowanych oraz skompresowanych,

10.5. dysków sieciowych,

10.6. dysków przenośnych.

11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

11.1. wybranych plików,

11.2. wybranych procesów,

11.3. wybranych lokalizacji,

11.4. wybranych rozszerzeń,



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ



GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

11.5. nazwy wykrycia,

11.6. sumy kontrolnej (SHA1).

12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

14. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.

16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

17.1.1. pamięci masowe,

17.1.2. optyczne pamięci masowe,

17.1.3. pamięci masowe Firewire,

17.1.4. urządzenia do tworzenia obrazów,

17.1.5. drukarki USB,

17.1.6. urządzenia Bluetooth,

17.1.7. czytniki kart inteligentnych,

17.1.8. modemy,

17.1.9. porty LPT/COM,

17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

17.2.1. numer seryjny,

17.2.2. producent,

17.3. typ dostępu:

- 17.3.1. brak możliwości zapisu,
- 17.3.2. pełen dostęp,
- 17.3.3. ostrzeżenie użytkownika,
- 17.3.4. brak dostępu.

18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

18.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

19.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

19.3. Raport musi posiadać co najmniej:

- 19.3.1. Listę zainstalowanych aplikacji,
- 19.3.2. Listę usług systemowych,
- 19.3.3. Informacje o systemie operacyjnym i sprzęcie,
- 19.3.4. Listę aktywnych procesów i połączeń sieciowych,
- 19.3.5. Harmonogram systemu operacyjnego,
- 19.3.6. Szczegóły pliku hosts,
- 19.3.7. Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu



GMINA  
TRZEBNICA  
trzebnica.pl



GINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

20.1. antywirus,

20.2. zapor osobista

20.3. sandbox,

20.4. antyspyware,

20.5. metody heurystyczne.

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.

22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.

22.2. Ochrona musi być realizowana w oparciu o co najmniej:

22.2.1. globalna czarna lista RBL,

22.2.2. czarna lista użytkownika,

22.2.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.

23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

23.1.1. Skanowanie portów TCP oraz UDP,

23.1.2. Wykrywanie duplikacji adresu IP,

23.1.3. Atak zatrutowania ARP,

23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.

23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

23.2.1. RDP,

23.2.2. SMB,

23.2.3. My SQL,

23.2.4. MS SQL.

23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

24.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

24.2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

24.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

24.2.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

24.2.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

24.2.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

24.2.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.

25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.

26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:

26.2.1. Treść komunikatu,

26.2.2. Obraz.

### Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.

2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.





4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6. Rozwiązanie musi chronić pliki co najmniej za pomocą:

6.1. Sygnatur wirusów.

6.2. Reputacji chmurowej.

7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.

8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

9.1. całego dysku,

9.2. wybranych katalogów,

9.3. pojedynczych plików,

9.4. plików spakowanych oraz skompresowanych,

9.5. Dysków sieciowych,

9.6. dysków przenośnych.

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

10.1. wybranych plików,

10.2. wybranych procesów,

10.3. wybranych lokalizacji,

10.4. wybranych rozszerzeń,

10.5. nazwy wykrycia,

10.6. sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.



GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
OSPODARKI  
KOMUNALNEJ

11.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.

11.2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

11.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

11.2.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

### Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:

1.1. Ubuntu Desktop,

1.2. Red Hat Enterprise Linux

1.3. Linux Mint.

2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:

2.1. Cinnamon,

2.2. GNOME,

2.3. KDE,

2.4. MATE,

2.5. XFCE.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:



GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARSTWA  
KOMUNALNEJ

- 6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
- 6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

- 7.1. całego dysku,
- 7.2. wybranych katalogów,
- 7.3. pojedynczych plików,
- 7.4. plików spakowanych oraz skompresowanych,
- 7.5. dysków sieciowych,
- 7.6. dysków przenośnych.

8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

- 8.1. wybranych plików,
- 8.2. wybranych procesów,
- 8.3. wybranych lokalizacji,
- 8.4. wybranych rozszerzeń,

9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

- 9.1. typ urządzenia:
  - 9.1.1. pamięci masowe,
  - 9.1.2. optyczne pamięci masowe,
- 9.2. parametry urządzenia:
  - 9.2.1. numer seryjny,
  - 9.2.2. producent,
  - 9.2.3. model.
- 9.3. typ dostępu:
  - 9.3.1. brak możliwości zapisu,
  - 9.3.2. pełen dostęp,
  - 9.3.3. brak dostępu.

### Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:

- 1.1. Microsoft Windows Server 2012 R2,
- 1.2. Microsoft Windows Server 2016,



GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

1.3. Microsoft Windows Server 2019,

1.4. Microsoft Windows Server 2022,

1.5. Microsoft Windows Server 2025.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

9.1. całego dysku,

9.2. wybranych katalogów,

9.3. pojedynczych plików,

9.4. plików spakowanych oraz skompresowanych,

9.5. dysków sieciowych,



9.6. dysków przenośnych.

TRZEBNICA  
Gmina



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

10.1. wybranych plików,

10.2. wybranych procesów,

10.3. wybranych lokalizacji,

10.4. wybranych rozszerzeń,

10.5. nazwy wykrycia,

10.6. sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

12.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

13.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

13.3. Raport musi posiadać co najmniej:

13.3.1. Listę zainstalowanych aplikacji,

13.3.2. Listę usług systemowych,

13.3.3. informacje o systemie operacyjnym i sprzęcie,

13.3.4. Listę aktywnych procesów i połączeń sieciowych,

13.3.5. harmonogram systemu operacyjnego,

13.3.6. Szczegóły pliku hosts,



13.3.7. Informacje o sterownikach.

TRZEBNICA  
Trzebnica.pl



GINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

---

14.1.

antywirus,

14.2.

zapora osobista

14.3.

sandbox,

14.4.

antyspyware,

14.5.

metody heurystyczne.

15.

Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

16.

Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

17.

Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1.

typ urządzenia:

17.1.1.

pamięci masowe,

17.1.2.

optyczne pamięci masowe,

17.1.3.

pamięci masowe Firewire,

17.1.4.

urządzenia do tworzenia obrazów,

17.1.5.



urządzenia Bluetooth,

17.1.7.

czytniki kart inteligentnych,

17.1.8.

modemy,

17.1.9.

porty LPT/COM,

17.1.10.

urządzenia przenośne.

17.2.

parametry urządzenia:

17.2.1.

numer seryjny,

17.2.2.

producent,

17.2.3.

model.

17.3.

typ dostępu:

17.3.1.

brak możliwości zapisu,

17.3.2.

pełen dostęp,

17.3.3.

ostrzeżenie użytkownika,

17.3.4.

brak dostępu.

18.

Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:



18.2.

Active Directory,

18.3.

IIS,

18.4.

Sysvol,

18.5.

DNS,

18.6.

DHCP,

18.7.

Hyper-V,

18.8.

Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19.

Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

19.1.

Ochrona przed anomaliami sieciowymi, w tym co najmniej:

19.1.1.

Skanowanie portów TCP oraz UDP,

19.1.2.

Wykrywanie duplikacji adresu IP,

19.1.3.

Atak zatruwania ARP,

19.1.4.

Nieprawidłowa długość pakietu TCP oraz UDP.

19.2.

Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

19.2.1.

SMB,

19.2.3.

My SQL,

19.2.4.

MS SQL.

19.3.

Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

20.

Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

21.

Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

21.1.

Zapora osobista musi posiadać co najmniej cztery tryby pracy:

21.1.1.

tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

21.1.2.

tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

21.1.3.

tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

21.1.4.

tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

21.1.4.1.

Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Ochrona serwera – Linux

1.

Rozwiązanie musi wspierać systemy w tym co najmniej:

1.1.



Red Hat Enterprise Linux (RHEL),

1.2.  
GMINA  
TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

Rocky Linux,

1.3.

Ubuntu,

1.4.

Debian,

1.5.

SUSE Linux Enterprise Server (SLES),

1.6.

Oracle Linux,

1.7.

Amazon Linux.

2.

Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

2.1.

wirus,

2.2.

trojan,

2.3.

robak,

2.4.

adware,

2.5.

spyware,

2.6.

dialer,

2.7.

phishing,

2.8.

backdoor.

3.



4.

Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAPS oraz

Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5.

Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

6.

Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

7.

Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

7.1.

Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

7.2.

Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

8.

Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

8.1.

całego dysku,

8.2.

wybranych katalogów,

8.3.

pojedynczych plików,

8.4.

plików spakowanych oraz skompresowanych,

8.5.

dysków sieciowych,

8.6.

dysków przenośnych.

9.



wybranych plików,

9.2.

wybranych procesów,

9.3.

wybranych lokalizacji,

9.4.

wybranych rozszerzeń,

10.

Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

10.1.

Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

11.

Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

12.

Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

13.

Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:

13.1.

proces budowania obrazu kontenera,

13.2.

wdrażanie obrazu kontenera.

Mobile Device Management

1.

Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

2.



MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.

MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:

2.1.1.

Android,

2.1.2.

iOS,

2.1.3.

iPadOS.

2.2.

MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:

2.2.1.

Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),

2.2.2.

Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

2.2.3.

VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

2.2.4.

Apple Business Manager (ABM),

2.2.5.

Android Enterprise (co najmniej w zakresie Device Owner).

3.

MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

3.1.

usunięcie zawartości urządzenia,

3.2.

przywrócenie urządzenia do ustawień fabrycznych,

3.3.

zablokowanie urządzenia,

3.4.



lokalizację GPS,

3.6.

Resetowanie hasła blokady ekranu.

4.

MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

5.

MDM musi umożliwiać co najmniej:

5.1.

Dla systemów iOS oraz iPadOS

5.1.1.

konfigurację kont e-mail,

5.1.2.

konfigurację połączeń VPN,

5.1.3.

Konfigurację połączeń Wi-Fi,

5.1.4.

Konfigurację listy certyfikatów,

5.1.5.

możliwość uruchomienia trybu jednej aplikacji.

5.2.

Dla systemu Android:

5.2.1.

blokadę wykonywania połączeń,

5.2.2.

blokadę konfiguracji sieci Wi-Fi,

5.2.3.

blokadę konfiguracji tuneli VPN,

5.2.4.

zarządzenie aktualizacjami systemu operacyjnego,

5.2.5.





blokadę zmiany tapety urządzenia.

TRZEBNICA  
trzebnica.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

## Mobile Threat Defense (MTD) dla systemu Android

1.

Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.

2.

Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:

2.1.

Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.

2.2.

Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

3.

Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4.

Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

4.1.

Złożoność kodu blokady ekranu:

4.1.1.

Wzór,

4.1.2.

PIN,

4.1.3.

Hasło,

4.2.

Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

4.3.

Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

5.

Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

5.1.

nazwę aplikacji,



5.3.

kategorię sklepu Google Play,

5.4.

uprawnienia aplikacji,

5.5.

pochodzenie aplikacji z nieznanego źródła.

6.

Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1.

Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.

2.

Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.

3.

Rozwiązanie musi wspierać systemy w tym co najmniej:

3.1.

Microsoft Windows 10 oraz 11,

3.2.

Microsoft Windows Server,

3.3.

macOS 11 (Big Sur) oraz nowszych

3.4.

RedHat Enterprise Linux (RHEL),

3.5.

Rocky Linux,

3.6.

Ubuntu,

3.7.

Debian,



SUSE Linux Enterprise Server (SLES),

3.9.

Oracle Linux,

3.10.

Amazon Linux.

4.

Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

5.

Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.

6.

Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:

6.1.

archiwa,

6.2.

skrypty,

6.3.

pliki wykonywalne,

6.4.

pliki rejestru systemowego (.reg),

6.5.

możliwy spam,

6.6.

dokumenty.

7.

Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:

7.1.

natychmiast po ich przeanalizowaniu,

7.2.

po upływie 30 dni,

8.

Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

9.

Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

10.

Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.

11.

Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

12.

Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.

12.1.

Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.

13.

Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:

13.1.

czysty,

13.2.

podejrzany,

13.3.

bardzo podejrzany,

13.4.

szkodliwy.

14.

W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:



wstrzymania uruchamiania pobieranych plików z następujących źródeł:

14.1.1.

przeglądarki internetowe,

14.1.2.

programy poczty e-mail,

14.1.3.

nośniki wymienne,

14.1.4.

pliki wyodrębnione z archiwum.

15.

W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

16.

Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

Szyfrowanie

1.

Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.

2.

Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.

3.

Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

4.

Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.

5.

Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.

5.1.

Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.

5.2.



Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.

6.

W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.

6.1.

Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.

6.2.

Hasło odzyskiwania nie może być krótsze niż 8 znaków.

6.3.

Hasło odzyskiwania nie może być dłuższe niż 20 znaków.

7.

Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

8.

Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.

9.

Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.

10.

Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.

11.

W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

### **Endpoint Detection and Response / eXtended Detection and Response**

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.

2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.

3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:

3.1. tworzenie procesów,

3.2. uruchamianie, zatrzymanie i modyfikacja usług,

3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,

3.4. usuwanie oraz zmiana nazw plików,

3.5. tworzenie i usuwanie kluczy rejestru systemowego,

3.6. ładowanie bibliotek DLL,



3.7. zalogowanie użytkowników,

3.8. elementy sieciowe, w tym co najmniej



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

3.8.1. pobranie plików wykonywalnych,

3.8.2. zestawienie połączeń TCP/IP,

3.8.3. zapytania HTTP,

3.8.4. zapytania DNS.

4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:

4.1.1. blokowanie pliku wykonywalnego,

4.1.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,

4.1.3. blokowanie podejrzanej biblioteki DLL,

4.1.4. zakończenie procesu,

4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,

4.1.6. wyłączenie komputera,

4.1.7. izolacja sieciowa hosta,

4.1.8. wylogowanie użytkownika.

4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

5.2.1. proces,

5.2.2. proces nadrzędny (proces rodzica),

5.2.3. nazwę procesu,

5.2.4. ścieżkę procesu,

5.2.5. wiersz polecenia,

5.2.6. wydawcę,

5.2.7. typ podpisu,

5.2.8. SHA-1,

5.2.9. SHA-2,





5.2.10. użytkownika.

TRZEBNICA  
gmina.pl



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.

6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.

6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):

6.2.1. SHA-1,

6.2.2. SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:

7.1. hash pliku SHA-1,

7.2. hash pliku SHA-256,

7.3. hash pliku MD5,

7.4. typ sygnatury podpisu cyfrowego,

7.5. wydawcę certyfikatu,

7.6. wersję pliku,

7.7. oryginalną nazwę pliku,

7.8. rozmiar pliku,

7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,

7.10. pierwsze uruchomienie pliku w środowisku,

7.11. ostatnie uruchomienie pliku w środowisku,

8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:

8.1. oznaczania ich jako bezpieczne lub niebezpieczne,

8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,

8.3. zablokowania wykonywania i wykorzystania pliku,

8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.

9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).

9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,



9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.

9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.



GINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.

10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.

11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.

12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.

### **Ochrona serwera pocztowego MS Exchange**

1. Rozwiązanie musi wspierać co najmniej następujące serwery poczty:

1.1. Microsoft Exchange 2010 SP3,

1.2. Microsoft Exchange 2013,

1.3. Microsoft Exchange 2016,

1.4. Microsoft Exchange 2019.

2. Rozwiązanie musi zapewniać wsparcie co najmniej dla następujących ról

2.1. Mailbox,

2.2. Edge,

2.3. Hub.

3. Rozwiązanie musi być instalowane na maszynie z serwerem pocztowym Exchange

4. Wszystkie komponenty rozwiązania ochrony serwera pocztowego Exchange muszą pracować na tym samym serwerze, na którym zainstalowany jest Microsoft Exchange (Rozwiązanie nie może pracować jako rozwiązanie typu gateway).

5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.

6. Rozwiązanie musi skanować pocztę wewnętrzną (ruch pocztowy w obrębie serwera Microsoft Exchange).

7. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.

8. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.

8.1. Rozwiązanie musi posiadać co najmniej następujące warunki:

8.1.1. nadawca,

8.1.2. odbiorca,



8.1.3. temacie wiadomości,

8.1.4. adres IP nadawcy,



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

8.1.5. nazwa, rozmiar i typ załącznika,

8.1.6. rozmiar wiadomości,

8.1.7. nagłówek wiadomości,

8.1.8. godzina odbioru,

8.1.9. obecność załącznika chronionego hasłem,

8.1.10. wynik SPF, DKIM i DMARC.

8.2. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:

8.2.1. poddaj wiadomość kwarantannie,

8.2.2. odrzuć wiadomość,

8.2.3. porzuć wiadomość w trybie dyskretnym,

8.2.4. usuń załącznik,

8.2.5. dodaj prefix tematu,

8.2.6. wyślij powiadomienie e-mail,

8.2.7. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.

9. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.

10. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.

11. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.

12. Rozwiązanie musi posiadać mechanizm greylisting (szara lista).

13. Rozwiązanie musi umożliwiać podpisywanie wiadomości za pomocą DKIM.

### Ochrona usług chmurowych

1. Rozwiązanie musi posiadać odrębną konsolę centralnego zarządzania:

1.1. konsola centralnego zarządzania musi być dostępna w wersji chmurowej (SaaS),

1.2. konsola centralnego zarządzania musi być dostępna z poziomu interfejsu WWW,

1.3. konsola centralnego zarządzania musi być zabezpieczona za pośrednictwem protokołu szyfrowanego SSL/TLS.

1.4. Konsola centralnego zarządzania musi być dostępne co najmniej w języku polskim oraz angielskim.

2. Rozwiązanie musi obejmować ochronę dla co najmniej następujących usług:

2.1. Microsoft Exchange Online,



2.2. Microsoft OneDrive,

2.3. Microsoft Sharepoint,

2.4. Microsoft Teams,

2.5. Google Workspace, w tym co najmniej

2.5.1. Gmail,

2.5.2. Google Drive.

3. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.

4. Rozwiązanie musi umożliwiać:

4.1. Wybór ręczny kont użytkowników, które będą objęte ochroną,

4.2. Wybór automatyczny całego tenantu, gdzie nowo utworzone konta będą automatycznie chronione.

5. Rozwiązanie musi posiadać możliwość raportowania w tym co najmniej:

5.1. kont użytkowników, otrzymujących najwięcej spamu,

5.2. kont użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,

5.3. kont użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,

5.4. kont użytkowników, które mogą być podejrzane.

6. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty.

7. Rozwiązanie musi mieć możliwość tworzenia reguł ochrony przesyłania poczty, gdzie po spełnieniu określonego warunku, zostanie wykonana określona czynność.

7.1. Rozwiązanie musi posiadać co najmniej następujące warunki:

7.1.1. nadawca,

7.1.2. temacie wiadomości,

7.1.3. adres IP nadawcy,

7.1.4. nazwa, rozszerzenie i typ załącznika,

7.1.5. nagłówek wiadomości,

7.1.6. godzina odbioru,

7.1.7. wynik SPF, DKIM, DMARC i ARC.

7.2. Rozwiązanie musi posiadać co najmniej następujące akcje w regułach:

7.2.1. poddaj wiadomość kwarantannie,

7.2.2. usuń wiadomość,

7.2.3. usuń załącznik,



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ



7.2.4. dodaj prefix tematu,

TRZEBNICA  
trzebnica.pl

7.2.5. Wyślij powiadomienie e-mail,



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

7.2.6. pomiń skanowanie w poszukiwaniu spamu, wirusów oraz phishing.

8. Rozwiązanie musi umożliwiać pobranie plików z kwarantanny co najmniej

8.1. w formie oryginalnego pliku,

8.2. w formie pliku zabezpieczonego hasłem.

9. Rozwiązanie musi umożliwiać przypisanie polityk co najmniej na poziomie:

9.1. całego tenantu,

9.2. grupy,

9.3. grupy Teams,

9.4. lokacji Sharepoint,

9.5. Pojedynczego użytkownika.

10. Rozwiązanie musi korzystać z chmury reputacji plików, pochodzącego od tego samego producenta rozwiązania antywirusowego:

10.1. możliwość automatycznego wysłania sumy kontrolnej

10.2. możliwość automatycznego wysłania fragmentu pliku.

11. Rozwiązanie musi umożliwiać określenie czynności realizowanej po wykryciu zagrożenia, w tym co najmniej następujące czynności:

11.1. brak czynności,

11.2. przenieś do spamu,

11.3. poddaj wiadomość kwarantannie,

11.4. poddaj załącznik kwarantannie,

11.5. przenieś do kosza,

11.6. usuń załącznik,

11.7. zastąp załącznik

11.8. usuń wiadomość.

12. Rozwiązanie musi umożliwiać dodanie znacznika do tematu wiadomości zaklasyfikowanej co najmniej jako:

12.1. SPAM,

12.2. phishing.

13. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:

13.1. archiwa,



13.4. pliki rejestru systemowego (.reg),

13.5. możliwy spam,

13.6. Dokumenty.

14. Administrator musi mieć możliwość zdefiniowania po jakim czasie przestane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:

14.1. natychmiast po ich przeanalizowaniu,

14.2. po upływie 30 dni,

14.3. nigdy.

15. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail.

15.1. Powiadomienia muszą dotyczyć wykryć co najmniej:

15.1.1. zagrożeń w wiadomościach,

15.1.2. phishing w wiadomościach,

15.1.3. zagrożeń w plikach onedrive,

15.1.4. zagrożeń na dysku Google Drive,

15.2. Powiadomienia muszą być możliwe do wysłania w co najmniej jednym z następujących języków:

15.2.1. Język polski,

15.2.2. Język angielski.

#### Vulnerability Assessment and Patch Management

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.

2. Rozwiązanie musi mieć możliwości wykrywania podatności:

2.1. w tym co najmniej następujących systemach operacyjnych:

2.1.1. Windows,

2.1.2. macOS,

2.1.3. Linux

2.2. w aplikacjach zainstalowanych na zarządzanych stacjach.

3. Rozwiązanie musi posiadać bazę podatności zawierającą co najmniej 35000 CVE.

4. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych. Zarządzanie musi się odbywać z poziomu tej samej konsoli co rozwiązanie antywirusowe, pochodzące od tego samego producenta.

5. Rozwiązanie musi umożliwiać utworzenie harmonogramu automatycznego wykrywania podatności.



6. Rozwiązanie musi umożliwiać wyświetlanie szczegółów danej podatności zawierające co najmniej:  
6.1. nazwę aplikacji lub systemu operacyjnego



GMINNY  
ZAKŁAD  
GOSPODARSTWA  
KOMUNALNEJ

6.2. punktacje CVSS

6.3. opis wykrytej podatności

6.4. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta

7. Rozwiązanie musi wykrywać podatności w minimum 700 aplikacjach.

8. Rozwiązanie musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 300 popularnych aplikacji.

9. Rozwiązanie musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji.

9.1. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście.

9.2. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

10. Rozwiązanie musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.

10.1. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.

10.2. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

11. Rozwiązanie musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.

12. Rozwiązanie musi być zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.

13. Rozwiązanie musi umożliwiać wyłączenie powiadomień dla wybranej podatności.

#### Two-factor authentication / Multi-factor authentication

1. Rozwiązanie musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).

2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.

3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.

4. Rozwiązanie musi pozwalać na instalację oprogramowania na co najmniej następujących systemach operacyjnych:

4.1. Systemy serwerowe:

4.1.1. Microsoft Windows Server 2012 R2,

4.1.2. Microsoft Windows Server 2016,

4.1.3. Microsoft Windows Server 2019,

4.1.4. Microsoft Windows Server 2022,



4.1.5. Microsoft Windows Server 2025.

4.2. Systemy kliente:



GMINNY  
ZAKŁAD  
GOSPODARKI  
KOMUNALNEJ

4.2.1. Windows 8.1,

4.2.2. Windows 10,

4.2.3. Windows 11.

5. Rozwiązanie musi posiadać integrację z następującymi rozwiązaniami:

5.1. Microsoft Exchange,

5.2. Microsoft Dynamics CRM,

5.3. Microsoft Sharepoint,

5.4. Microsoft Remote Desktop Web Access,

5.5. Microsoft Terminal Services Web Access,

5.6. Microsoft Remote Web Access,

5.7. Active Directory Federation Services.

6. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników podczas logowania do co najmniej:

6.1. klienta VPN,

6.2. systemu macOS

6.3. systemu Linux,

6.4. połączenia SSH.

7. Rozwiązanie musi oferować dedykowaną bezpłatną aplikację mobilną pochodzącą od tego samego producenta rozwiązania 2FA/MFA.

7.1. Aplikacja mobilna musi wspierać następujące systemy:

7.1.1. Android,

7.1.2. iOS.

7.2. Aplikacja mobilna musi umożliwiać uwierzytelnienie użytkownika przy pomocy co najmniej:

7.2.1. Generowanego kodu OTP w tym co najmniej:

7.2.1.1. HOTP,

7.2.1.2. TOTP.

7.2.2. Powiadomienia PUSH.

7.3. Aplikacja mobilna musi posiadać możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.

7.4. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP musi odbywać się w trybie offline.



- 8.1. OTP dostarczonego przy pomocy wiadomości SMS,
- 8.2. OTP dostarczonego przy pomocy wiadomości e-mail,
- 8.3. tokenu sprzętowego,
- 8.4. FIDO,
- 8.5. klucza odzyskiwania (MRK).

### 13) Usługa Bezpiecznej Poczty

Subskrypcja profesjonalnej poczty elektronicznej klasy biznesowej, świadczonej w modelu hostowanym (Cloud Computing) na okres 12 miesięcy dla 40 użytkowników.

- Pojemność skrzynki: Minimum 100 GB powierzchni dyskowej na dane użytkownika (wiadomości i załączniki).
- Maksymalny rozmiar załącznika w Outlook: Obsługa wysyłania i odbierania wiadomości o rozmiarze co najmniej 150 MB.
- Archiwum nieograniczone: Funkcja automatycznego, rozszerzalnego archiwum online (Auto-expanding archiving), pozwalająca na przechowywanie historycznych wiadomości e-mail bez limitu pojemności (zgodnie z polityką sprawiedliwego użytkownika dostawcy).
- Wbudowane mechanizmy identyfikowania, monitorowania i ochrony wrażliwych informacji (np. dane finansowe, numery identyfikacyjne, dane osobowe) poprzez głęboką analizę treści wiadomości i załączników. Możliwość wymuszania polityk bezpieczeństwa (np. blokowanie wysyłki poza organizację).
- Możliwość zachowania całości zawartości skrzynki użytkownika (w tym elementów usuniętych i edytowanych) na potrzeby procesów prawnych lub dowodowych przez czas nieokreślony.
- Zaawansowane narzędzia do przeszukiwania, identyfikowania i eksportowania danych z wielu skrzynek pocztowych jednocześnie w celach audytowych.
- Pełna obsługa przez przeglądarkę WWW, aplikacje desktopowe (protokół MAPI/HTTP) oraz urządzenia mobilne (ActiveSync).
- Usługi hostowanej ujednoliconej obsługi wiadomości (Unified Messaging), zapewniające funkcje automatycznej sekretarki i integrację z systemami telefonicznymi.
- Możliwość tworzenia skrzynek współdzielonych oraz kalendarzy zasobów (sale, sprzęt) bez dodatkowych opłat licencyjnych.
- Wielowarstwowe filtrowanie antyspamowe oraz zaawansowana ochrona przed malware aktualizowana w trybie ciągłym.
- Obsługa szyfrowania wiadomości wewnątrz i na zewnątrz organizacji (np. Office 365 Message Encryption lub równoważne).

- Wykonawca zapewni dostęp do portalu administracyjnego umożliwiającego samodzielne zarządzanie subskrypcjami (dodawanie/usuwanie użytkowników).

- Przechowywanie i przetwarzanie danych musi odbywać się zgodnie z obowiązującymi przepisami RODO.

Wymagania ogólne dotyczące identyfikacji oferowanego sprzętu oraz zasad równoważności.

1. Dla jednoznacznej identyfikacji oferowanych rozwiązań należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego produktu lub jego oznaczenie kodowe wg. producenta. Zamawiający wymaga określenia oferowanych produktów i faktycznych parametrów, o których mowa w powyższym opisie, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowane rozwiązanie spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane rozwiązania spełniają wymagania Zamawiającego. Ciężar wykazania spełnienia przez oferowane rozwiązania wymogów określonych przez Zamawiającego w specyfikacji spoczywa na składającym ofertę.
2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
4. W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
5. Pod pojęciem rozwiązań równoważnych, o ile nie dokonano doprecyzowania w danym zakresie, Zamawiający rozumie taki sprzęt i oprogramowanie, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w Opisie Przedmiotu Zamówienia.
6. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.
7. Ciężar udowodnienia równoważności w stosunku do wymogów określonych przez Zamawiającego spoczywa na składającym ofertę. W takim przypadku Wykonawca musi przedłożyć odpowiednie dokumenty, opisujące parametry techniczne, wymagane prawem certyfikaty i inne dokumenty, dopuszczające dane produkty do użytkowania oraz pozwalające jednoznacznie określić, że są równoważne.