TOM II

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest dostawa:

1. **ZADANIE 1: Oprogramowania do wykonywania kopii zapasowych – 1 kpl.**
2. **ZADANIE 2: Zapory sieciowej klasy UTM – 2 szt.**

w ramach projektu grantowego „Cyfrowa Gmina", spełniających poniższe minimalne parametry techniczne, wymagania i funkcje:

ZADANIE 1*: DOSTAWA OPROGRAMOWANIA DO WYKONYWANIA KOPII ZAPASOWYCH: 1 komplet

Lp.	Temat	Wymagane funkcje oprogramowania
1.	**Ogólne**	1. Interfejs systemu w języku: a) polskim b) angielskim 2. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, 3. Oprogramowanie może być uruchomione w kontenerze docker, 4. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: a) Debian: 9+ b) Ubuntu: 16.04+ c) Fedora: 29+ d) centOS: 7+ e) RHEL: 6+ f) openSUSE: 15+ g) SUSE Enterprise Linux (SLES): 12 SP2+ h) Windows Client: 7, 8.1, 10 (1607+) i) Windows Server: 2008 R2+ 5. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji 6. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju)
2.	**Wsparcie techniczne**	Pomoc techniczna oraz baza wiedzy w językach: a) polskim b) angielskim
3.	**Zarządzanie**	1. Zarządzanie całością działania systemu (backup, przywracanie) z poziomu jednej konsoli webowej, 2. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego 3. Wbudowane predefiniowane zadania backupowe 4. Tworzenie zadań backupowych w oparciu o kalendarz 5. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem 6. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem 7. Monitorowanie postępu działania zadania 8. Powiadamianie poprzez e-mail o zdarzeniach w następujących przypadkach: a) zadanie zostało zakończone pomyślnie, b) zadanie zostało zakończone z ostrzeżeniami, c) zadanie zostało zakończone z błędem, d) zadanie zostało anulowane, e) zadanie nie zostało uruchomione. 9. Generowanie alertów w przypadku zaistnienia określonego zdarzenia systemowego 10. Możliwość zdefiniowania okna backupowego dla każdego z zadań 11. Wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów

		12. Klonowanie planów kopii zapasowych 13. Reset hasła administratora w przypadku jego utraty 14. Tworzenie kont użytkowników nie będących administratorami 15. Tworzenie grup urządzeń 16. Zoptymalizowana trasa transmisji danych poprzez możliwość wybrania dowolnego urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług oraz urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów 17. Tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: a) System Administrator, b) Backup operator, c) Restore operator, d) Viewer.
4.	**Składowanie danych**	1. Możliwość tworzenia repozytoriów danych jednocześnie z poziomu jednej konsoli, 2. Umożliwienie składowanie danych: a) lokalnie: ▪ zasób SMB ▪ zasób NFS ▪ zasób ISCSI ▪ zasób S3 ▪ katalog zabezpieczonego urządzenia b) w chmurze: ▪ Amazon Web Service, ▪ magazyn zgodny z S3, ▪ dostarczanej bezpośrednio przez producenta. 3. Zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, 4. Mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. 5. Możliwość replikacji pomiędzy dowolnymi wspieranymi magazynami według ustalonego przez administratora harmonogramu.
5.	**Odtwarzanie**	1. Odtwarzanie pojedynczych plików z kopii obrazu dysku 2. Wykorzystanie funkcjonalności Bare Metal Restore (kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: a) Windows: 10+, b) Windows Server: 2008 R2+ 3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 4. Odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK) 5. Odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) 6. Odtwarzanie zasobów plikowych z prawami dostępu 7. Przywracanie plików pomiędzy systemami operacyjnymi (np. odtwarzanie danych plikowych Linux na systemie Windows) 8. Odtwarzanie danych według harmonogramu 9. Przywracanie danych z określonego urządzenia/użytkownika 10. Przywracanie kopii z wybranego magazynu
6.	**Backup**	1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: a) Systemów operacyjnych: ▪ Debian: 9+, ▪ Ubuntu: 16.04+, ▪ Fedora: 29+, ▪ centOS: 7+, ▪ RHEL: 6+, ▪ openSUSE: 15+, ▪ SUSE Enterprise Linux(SLES): 12 SP2+, ▪ Windows: 7, 8.1, 10(1607+),

		▪ Windows Server: 2008 R2+, 2019 b) Środowisk wirtualnych: ▪ Hyper-V, ▪ VMware: 6.7+. ▪ Dowolne inne w sposób agentowy 2. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla baz danych: a) Microsoft SQL b) MySQL c) PostgreSQL d) Firebird 3. Szyfrowanie danych wykonywane po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: a) 128 bit b) 192 bit c) 256 bit 4. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: a) Zstandard b) LZ4 5. Możliwość zarządzania poziomem kompresji, 6. Wykonywanie kopii zapasowej otwartych plików(VSS), 7. Możliwość uruchamiania skryptów przed i po backupie, 8. Możliwość uruchamiania skryptów po wykonaniu migawki VSS, 9. Możliwość automatycznego ponawiania prób utworzenia kopii zapasowej w przypadku błędów, 10. Backup jednego oraz wielu dysków/całego systemu operacyjnego (Windows) ze wsparciem dla partycji MBR oraz GPT, 11. Backup plikowy, 12. Funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, 13. Możliwość automatycznego uruchomienia kopii zapasowej podczas zamykania systemu operacyjnego. 14. Możliwość backupu zaszyfrowanych partycji.
8.	**Licencjonowanie**	1. Licencja w wersji dożywotniej na zabezpieczenie 3 fizycznych hostów maszyn wirtualnych oraz 90 fizycznych stacji roboczych. 2. Wsparcie techniczne a) świadczone w języku polskim, b) zapewnia dostęp do aktualizacji oprogramowania, c) umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, d) obowiązuje przez okres 36 miesięcy.
9.	**Wdrożenie dostarczonego oprogramowania**	Zamawiający wymaga aby dostarczone oprogramowanie zostało zainstalowane i skonfigurowane wraz z wdrożeniem polityk backupowych w środowisku zamawiającego. Obejmuje to: 1. Zaprojektowanie we współpracy z Zamawiającym harmonogramu wykonywania kopii, z uwzględnieniem środowiska Zamawiającego. 2. Instalację oprogramowania w środowisku Zamawiającego. 3. Implementację harmonogramu wykonywania kopii w zainstalowanym programowaniu. 4. Wykonanie testowych kopii wraz z weryfikacją poprawności ich wykonania. 5. Testy odtworzenia danych. 6. Przygotowanie i przekazanie Zamawiającemu dokumentacji powykonawczej.
10.	**Szkolenie z obsługi**	Zamawiający wymaga aby szkolenie z zakresu instalacji, konfiguracji i obsługi oprogramowania było autoryzowane przez producenta oprogramowania, i: 1. trwało co najmniej 8 h w tym wykłady i warsztaty praktyczne, 2. zawierało omówienie funkcji oprogramowania, metod wdrożenia, konfiguracji i czynności administracyjnych, 3. wydany był certyfikat lub zaświadczenie wystawione przez ośrodek szkoleniowy, świadczące o ukończeniu szkolenia. Zamawiający wymaga aby szkolenie przeprowadzone było w trybie on-line.

ZADANIE 2*: DOSTAWA ZAPORY SIECIOWEJ KLASY UTM: 2 szt.

Lp.	Temat	Wymagane funkcje
1.	**Obsługa sieci**	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2.	**Zapora (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, 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).
3.	**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, FTPS, 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.
4.	**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.
5.	**Ochrona Antywirusowa**	1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. 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.
6.	**Ochrona Antyspam**	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a) białe/czarne listy, b) DNS RBL, c) Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
7.	**Wirtualne Sieci Prywatne (VPN)**	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a) PPTP VPN, b) IPSec VPN, c) SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
8.	**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 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a) blokowanie dostępu do adresu URL, b) zezwolenie na dostęp do adresu URL, c) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

		7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
9.	**Uwierzytelnianie**	1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a) lokalną bazę użytkowników (wewnętrzny LDAP), b) zewnętrzną bazę użytkowników (zewnętrzny LDAP), c) usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a) SSL, b) Radius, c) Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
10.	**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. 5. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 6. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 7. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 8. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 9. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 10. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 11. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a) manualnego eksportu do pliku w dowolnym momencie czasu, b) automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 12. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 13. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
11.	**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 edycję konfiguracji bezpośrednio z poziomu raportu. 5. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 6. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 7. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
12.	**Gwarancja**	1. Urządzenie ma być objęte 36-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.
13.	**Parametry sprzętowe**	1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB. 2. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 3. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 4. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. 5. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 3.3Gbps. 6. Przepustowość filtrowania Antywirusowego – minimum 950Mbps. 7. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1.3Gbps. 8. Obsługa interfejsów 802.11q (VLAN) – minimum 256. 9. Liczba równoczesnych sesji – minimum 500 000 i nie mniej niż 25 000 nowych sesji/sekundę. 10. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 11. Urządzenie nie ma limitu na liczbę użytkowników. 12. Liczba reguł filtrowania – minimum 8 192. 13. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.
14.	**Szkolenie z obsługi**	Zamawiający wymaga aby szkolenie z zakresu instalacji, konfiguracji i obsługi urządzenia było autoryzowane przez producenta, i: 1. trwało co najmniej 24 h w tym wykłady i warsztaty praktyczne, 2. wydany był certyfikat lub zaświadczenie wystawione przez ośrodek szkoleniowy, świadczące o ukończeniu szkolenia. Zamawiający wymaga aby szkolenie przeprowadzone było w trybie on-line.

***Zamawiający dopuszcza składanie ofert częściowych, na jedno lub dwa zadania.**