OPIS PRZEDMIOTU ZAMÓWIENIA

Parametry minimalne sprzętu i oprogramowania

Spis treści

1 System kopii zapasowych

W ramach dostawy Wykonawca musi dostarczyć rozwiązanie spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami, które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.
Wykonawca jest zobowiązany do uruchomienia systemu backupowego i jego skonfigurowania zgodnie z zaleceniami Zamawiającego.

Cecha	Wymagania minimalne
Ogólne	● System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu. ● Konsola zarządzająca może być również instalowana w chmurze producenta zlokalizowanej na terenie Polski, ● Interfejs systemu dostępny jest w języku: ○ polskim, ○ angielskim, ○ ukraińskim, ● System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, w tym z możliwością odtworzenia w postaci usługi uruchomionej w chmurze producenta zlokalizowanej na terenie Polski, ● Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej), ● Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
Sprzętowe	Obudowa: Rack 1U Procesor: Intel Xeon E-2336 lub równoważny posiadający taką samą lub wyższą punktację w rankingu benchmark Pamięć RAM: 16 GB DDR4 Przestrzeń backupowa dostępna przy konfiguracji RAID 5 : min. 24 TB Osobny dyski SSD min. 2x 240 GB na konsolę zarządzającą Urządzenie powinno posiadać już zainstalowane dyski oraz skonfigurowany RAID 5 lub 6 i być gotowe do pracy zgodnie z w/w wymaganiami „Ogólne” Redundantne zasilacze o mocy min.600 W Interfejsy sieciowe: - min. 2szt. Ethernet typu 1000BaseT

	- min. 1szt. SFP+
Zarządzanie	● Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli, dostępnej za pośrednictwem przeglądarki WWW, ● Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, ● Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, ● Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, ● Monitorowanie postępu działania zadania, ● Posiada system powiadamiania poprzez e-mail bądź Slack o zdarzeniach w następujących przypadkach: ○ Zadanie zostało zakończone pomyślnie, ○ Zadanie zostało zakończone z ostrzeżeniami, ○ Zadanie zostało zakończone z błędem, ○ Zadanie zostało anulowane, ○ Zadanie nie zostało uruchomione. ● System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego ● System umożliwia wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika, ● Możliwość zdefiniowania okna backupowego dla każdego z zadań, ● Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów i innych sekretów, wykorzystywanych przez System, ● System pozwala na klonowanie planów kopii zapasowych, ● System umożliwia reset hasła administratora w przypadku jego utraty, ● Oprogramowanie umożliwia definiowanie retencji według schematów: ○ GFS(Grandfather-Father-Son), ○ FIFO(First-In, First-Out). ● Oprogramowanie umożliwia tworzenie grup urządzeń, ● Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). ● System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: ○ System Administrator, ○ Backup operator, ○ Restore operator, ○ Viewer.

	● Administrator Systemu powinien mieć możliwość logowania się z wykorzystaniem kont Google
Składowanie danych	● Dane są składowane w ramach dostępnej macierzy wymienionej w wymaganiach sprzętowych OPZ ● Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako miejsce replikacji danych: ○ Lokalnie: ■ Zasób SMB, ■ Zasób NFS, ■ Zasób ISCSI, ■ Zasób S3, ■ Katalog zabezpieczonego urządzenia. ○ W chmurze: ■ Amazon Web Service, ■ Magazyn zgodny z S3, ■ Dostarczanej przez producenta. ● System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. ● System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. ● System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych, ● System obsługuje mechanizm WORM (Write Once Ready Many) w chmurowych oraz lokalnych repozytoriów kopii,
Odtwarzanie	● Odtwarzanie granularne: ○ Pojedynczych plików z kopii obrazu dysku, ○ Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. ● 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: ○ Windows: 7+, ○ Windows Server: 2008 R2+, ● 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. ● Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, ● Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.

	● Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(RAW, VHD, VHDX, VMDK), ● Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), ● Odtwarzanie zasobów plikowych z prawami dostępu, ● Przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows), ● Odtwarzanie danych według harmonogramu, ● Przywracanie danych z określonego urządzenia/użytkownika, ● Przywracanie kopii z wybranego magazynu. ● Przywracanie danych Microsoft 365: ○ do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst ○ do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), ● System posiada możliwość nieodwracalnego kasowania danych, ● Przywracanie repozytoriów GIT: ○ Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLab), ○ przywracanie między kontami.
Wykonywanie kopii	● Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych dla: ○ Systemów operacyjnych: ■ Alpine 3.10+, ■ Debian: 9+, ■ Ubuntu: 16.04+, ■ Fedora: 29+, ■ centOS: 7+, ■ RHEL: 6+, ■ openSUSE: 15+, ■ SUSE Enterprise Linux(SLES): 12 SP2+, ■ macOS: 10.13+, ■ Windows: 7 i nowsze ■ Windows Server: 2008 R2 i nowsze ○ Środowisk wirtualnych: ■ Hyper-V, ■ VMware, ■ Dowolnych innych – agentowo. ○ Repozytoriów GIT: ■ GitHub, ■ Bitbucket ■ GitLab ○ Jira Cloud ● Wykonywanie pełnych, różnicowych oraz przyrostowych kopii zapasowych dla:

	○ Baz danych: ■ Microsoft SQL, ■ MySQL, ■ PostgreSQL, ■ Firebird, ■ Oracle ■ Dowolnych innych przez podpięcie skryptów pre/post. ● Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: ○ 128 bit, ○ 192 bit, ○ 256 bit. ● Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: ○ ZStandard, ○ LZ4. ● Oprogramowanie umożliwia zarządzanie poziomem kompresji, ● System dostarcza agenta backupu w postaci kontenera Docker, umożliwiającego wykonywanie kopii zapasowych z dowolnych środowisk kontenerowych, w tym popularnych rozwiązań NAS, ● System dostarcza agenta backupu w postaci instalatora MSI, umożliwiającego masową instalację w systemach Windows z wykorzystaniem narzędzi Active Directory - SCCM oraz GPO ● Wykonywanie kopii zapasowej otwartych plików(VSS), ● System umożliwia uruchamianie skryptów przed i po backupie, ● System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, ● System umożliwia wykonywanie spójnej kopii danych pracujących aplikacji na urządzeniach z systemem Windows oraz wspieranych środowiskach wirtualnych, ● System pobiera jedynie zmodyfikowane bloki danych podczas przyrostowej i różnicowej kopii maszyn wirtualnych VMware, ● System umożliwia wykonywanie kopii maszyn wirtualnych VMware z zastosowanie zaawansowanych trybów transportu (HotAdd, LAN, SAN), w tym metodą LAN-Free, ● System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, ● Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, ● Backup plikowy, ● Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,

	● Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, ● Oprogramowanie pozwala na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej, ● Oprogramowanie pozwala na backup zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption
GIT	● Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), ● Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).
Licencjonowanie	● Licencje powinny pozwalać na zabezpieczenie: ○ Nielimitowanej ilości maszyn wirtualnych ○ Nielimitowanej ilości serwerów fizycznych ○ Nielimitowanej ilości stacji roboczych ○ Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu
Wsparcie techniczne	○ Wsparcie techniczne producenta świadczone przynajmniej do 10.04.2026 ○ Wsparcie świadczone jest w języku polskim przez producenta, ○ Dostęp do aktualizacji oprogramowania, ○ Możliwość korzystanie z połączeń zdalnych producenta, systemu ticketowego oraz wsparcia telefonicznego, ○ Obowiązuje przez okres analogicznie do długości wsparcia warstwy sprzętowej.
Gwarancja sprzętowa	Minimum 24 miesiące gwarancji. Uszkodzone, wadliwe dyski podlegają wymianie na nowe (nie będą naprawiane) i pozostają własnością Zamawiającego

2 Pamięć masowa dla OPS

W ramach dostawy Wykonawca musi dostarczyć rozwiązanie spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.
Wykonawca jest zobowiązany do uruchomienia systemu backupowego i jego skonfigurowania zgodnie z zaleceniami Zamawiającego.

Cecha	Wymagania minimalne
Procesor	Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz
Obudowa	RACK 19" 2U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Minimum 16GB DDR4 ECC - RAM tego samego producenta, co serwer NAS, w konfiguracji 1 x 16GB. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. Możliwość rozszerzenia RAM do 32GB.
Całkowita liczba gniazd pamięci	Minimum 2 – jeden slot powinien zostać wolny
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	3.5" SATA HDD / 2.5" SATA SSD – Hot Swap Zamawiający wymaga dostarczenia minimum 5 dysków 3.5” SATA HDD o pojemności 8TB każdy o parametrach nie gorszych niż: Prędkość obrotowa: 7200 RPM MTBF: 1 000 000 Obciążenie roczne: 180 TB Gwarancja producenta dysku: 3 lata Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Dyski zgodne z listą kompatybilności producenta oferowanego serwera.
Możliwość podłączenia modułu rozszerzającego	Tak
Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	12
Porty na karty rozszerzeń	Minimum 1 x Gen3 x8 slot (x4 link)
Porty LAN	Wbudowane min. 4 x RJ-45 1GbE Min. 2 porty SFP+ (możliwe przez zastosowanie karty rozszerzeń)
Porty USB 3.2	Minimum 2
Port eSATA	Minimum 1

Zasilanie	Redundantny zasilacz o mocy minimalnej 350W
Mechanizm szyfrowania sprzętowego	Tak, min AES-NI
Wewnętrzny system plików	BTRFS, EXT4
Obsługiwane tryby RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows (ACL)
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie do kopii zapasowej	Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, - kopia zapasowa środowisk MacOS - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) - kopia zapasowa serwerów fizycznych (Windows, Linux) - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, - obsługa wielu wersji i retencji, - możliwość wyzwalania kopii zapasowej według harmonogramu, - obsługa klastra przełączania awaryjnego Microsoft Hyper-V, - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie, - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji,

	harmonogramu i woluminów objętych backupem dla poszczególnych zadań, - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta rozwiązania.
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. • Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. • Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync • Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system • Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40 jednoczesnych połączeń
Gwarancja sprzętowa	Minimum 24 miesiące gwarancji producenta. Uszkodzone, wadliwe dyski podlegają wymianie na nowe (nie będą naprawiane) i pozostają własnością Zamawiającego.

3 Pamięć masowa dla jednostek oświatowych na potrzeby kopii zapasowej

W ramach dostawy Wykonawca musi dostarczyć rozwiązanie spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.
Wykonawca jest zobowiązany do uruchomienia systemu backupowego i jego skonfigurowania zgodnie z zaleceniami Zamawiającego.

Cecha	Wymagania minimalne
Procesor	Procesor dwurdzeniowy 64-bitowy o taktowaniu nie niższym niż 2.6GHz
Obudowa	Desktop
Procesor liczba rdzeni	Nie mniej niż 2
Pamięć RAM	Minimum 4GB DDR4 ECC. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. Obsługa RAM do 32GB.
Całkowita liczba gniazd pamięci	Minimum 2
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3.5" SATA HDD / 2.5" SATA SSD – Hot Swap Zamawiający wymaga dostarczenia minimum 4 dysków 3.5” SATA HDD o pojemności 4TB każdy o parametrach nie gorszych niż: Prędkość obrotowa: 5400 RPM MTBF: 1 000 000 Obciążenie roczne: 180 TB Gwarancja producenta dysku: 3 lata Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Dyski zgodne z listą kompatybilności producenta oferowanego serwera.
Wbudowane kieszenie dysków M.2 NVMe	Minimum 2

Możliwość podłączenia modułu rozszerzającego	Tak
Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	9
Porty na karty rozszerzeń	Minimum 1 x Gen3 x2
Porty LAN	Wbudowane min. 2 x RJ-45 1GbE
Porty USB 3.2	Minimum 2
Port eSATA	Minimum 1
Zasilanie	Zasilacz o mocy minimalnej 100W
Mechanizm szyfrowania sprzętowego	Tak, min AES-NI
Wewnętrzny system plików	BTRFS, EXT4
Obsługiwane tryby RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows (ACL)
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie do kopii zapasowej	Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, - kopia zapasowa środowisk MacOS - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)

	- kopia zapasowa serwerów fizycznych (Windows, Linux) - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, - obsługa wielu wersji i retencji, - możliwość wyzwalania kopii zapasowej według harmonogramu, - obsługa klastra przełączania awaryjnego Microsoft Hyper-V, - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie, - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera.
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników.

	• Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. • Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync • Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40 jednoczesnych połączeń
Gwarancja sprzętowa	Minimum 24 miesiące gwarancji. Uszkodzone, wadliwe dyski podlegają wymianie na nowe (nie będą naprawiane) i pozostają własnością Zamawiającego.

4 UTM dla Urzędu Miejskiego w celu wdrożenia klastra HA

Cecha	Wymagania minimalne
Ogólne	Zamawiający informuje że posiada rozwiązanie klasy UTM SOPHOS XGS2100 (X21008VCKJ8YM37) z aktywnymi licencjami XSPXGS210036-7KXH9CB72 do dnia 15.08.2025. W ramach rozbudowy należy dostarczyć identyczne urządzenie w celu zestawienia Klastra wysokiej dostępności działającego w trybie Active-Pasive. Ważność licencji oraz gwarancja dla całego nowopowstałego klastra powinna być ważna minimum do 10.04.2026 w odniesieniu do daty końca aktualnej licencji.

5 UTM dla OPS

W ramach dostawy Wykonawca musi dostarczyć firewall UTM spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

Cecha	Wymagania minimalne
Ogólne	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.

	Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji. Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych. Rozwiązanie powinno ofertować możliwość zamontowanie redundantnego zasilacza. Urządzenie musi być wyposażone w wielofunkcyjny wyświetlacz LCD umożliwiający sprawdzenie statusu urządzenia i wykonywanie podstawowych czynności administracyjnych bezpośrednio na urządzeniu Pamięć operacyjna RAM nie mniej niż (GB): 8 Przestrzeń do przechowywania logów i raportów nie mniej niż (GB): 110 Liczba fizycznych interfejsów Gigabit Ethernet nie mniej niż: 8 Liczba fizycznych interfejsów SFP Fiber: 2
Wydajność	Wydajność Firewall nie mniej niż (Mbps): 29 000 Wydajność Firewall IMIX nie mniej niż (Mbps): 15 000 Wydajność IPS nie mniej niż (Mbps): 6000 Wydajność FW+IPS+AV nie mniej niż (Mbps): 1 200 Wydajność NGFW nie mniej niż (Mbps): 5 000 Liczba równoczesnych połączeń nie mniejsza niż: 6000000 Liczba nowych połączeń na sekundę nie mniejsza niż: 125 000 Wydajność IPsec VPN nie mniej niż (Mbps): 4900

	Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): 1000 Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 18000 Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 2300
Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy,

	użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpwiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja

	subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konifiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.
Zapora sieciowa	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa,

	grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.

	Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
Kontroler sieci bezprzewodowej	System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater. Uruchomienie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej. Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID). Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication). Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z

	vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. System powinien zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden. System powinien pozwalać na rozgłaszanie sieci bezprzedowodych w oparciu o harmonogramy czasowe. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.

	System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.

	System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
Intrusion Prevention System i Advanced Threat Protection	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
Ochrona przed Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).

	Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
Filtr Web	Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji. Rozwiązanie powinno umożliwiać filtrowanie stron web analzując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych. Rozwiązanie powinno oferować ochronę przed Pharmingiem.
Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sanbox do ochrony przez zadrożeniami typu Zero-Day. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal. System powinien oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów.

Licencje	Licencje na opisane funkcjonalności muszą być ważne przynajmniej do 10.04.2026
Gwarancja	Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przynajmniej do 10.04.2026

6 Zaawansowane systemy bezpieczeństwa stanowiskowego

Cecha	Wymagania minimalne
Ogólne	Zamawiający informuje że posiada rozwiązanie Sophos Central (numer licencji: D590977448) z aktywnymi licencjami: - Sophos Central Intercept X Advanced dla 80 użytkowników - Sophos Central Intercept X Advanced for Server dla 6 serwerów Licencje ważne są do dnia 19.02.2025. W ramach rozbudowy należy przedłużyć aktualną licencję przynajmniej do 10.04.2026 i rozszerzyć o dodatkowe moduły zwiększające bezpieczeństwo i reakcję na incydenty. Nowy pakiet powinien obejmować moduły: - Sophos Central Intercept X Advanced with XDR dla 80 użytkowników - Sophos Central Intercept X Advanced with XDR for Server dla 6 serwerów

7 Serwer główny – Serwer

W ramach dostawy Wykonawca musi dostarczyć serwer spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego środowiskiem sieciowo-serwerowym.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.
W ramach dostawy Wykonawca jest zobowiązany do migracji obecnego środowiska Zamawiającego na dostarczony serwer.

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack 19” o wysokości max 2U wyposażona w 12 zatok dla twardych 3,5cala na froncie obudowy wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej: SPECrate2017_int_base wynik min. 177pkt SPECrate2017_int_peak wynik min. 182pkt SPECrate2017_fp_base wynik min. 250pkt SPECrate2017_fp_peak wynik min. 254pkt Maksymalny TDP dla procesora 150W Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty. Do oferty należy załączyć wyniki testów.
RAM	128GB (w układzie 4x32GB)o częstotliwości taktowania minimum 4800MHz, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Minimum 3 slotów PCIe x16 generacji 4
Interfejsy sieciowe/	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający: • Min. 8GB nieulotnej pamięci cache • Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. • Wsparcie dla dysków samoszyfrujących
Dyski twarde	Zainstalowane dyski: • 5 dysków min. 1,92TB SSD typu ReadIntensive, DWPD>=1, Hot-Plug • 5 dysków min. 4TB HDD 7,2k RPM SAS, Hot-Plug • 2 dyski min. M.2 NVME o pojemności min. 480GB Hot-Plug skonfigurowane w RAID 1 pod virtualizator
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy. Klasy Titanium
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

	• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Diagnostyka	Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - **dołączyć do oferty jako przedmiotowy środek dowodowy**. Serwer musi posiadać deklarację CE - **dołączyć do oferty jako przedmiotowy środek dowodowy**.
System operacyjny	Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w

	postaci **2** wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
      1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
      2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
      3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
   III. zdalna dystrybucja oprogramowania na stacje robocze,
   IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
   V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
      1) dystrybucję certyfikatów poprzez http,
      2) konsolidację CA dla wielu lasów domeny,
      3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   VI. szyfrowanie plików i folderów,
   VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
   VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
   IX. serwis udostępniania stron WWW,
   X. wsparcie dla protokołu IP w wersji 6 (IPv6),
   XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
      1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Warunki gwarancji	1. Minimum 24 miesiące gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. 6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.

	7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 11. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. 13. Firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny link do strony producenta urządzenia z ogólnodostępnym dokumentem np. certyfikat lub oświadczenie, potwierdzającym autoryzację dla firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku braku takiego linku lub ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski. **Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy** Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do 60 miesięcy

8 Przełączniki sieciowe

W ramach dostawy Wykonawca musi dostarczyć klaster dwóch przełączników spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

Nazwa parametru	Minimalna wartość parametru

Ogólne	• Ilość portów: minimum 8 portów 10Gb SFP+ oraz minimum 8 portów 10GBaseT • Chłodzenie od przedu do tyłu obudowy • Tablica MAC min. 16K • Tablica ARP/NDP min. 888 • Bufor 16Mb • MTBF min. 195000 godzin • Port USB • Port zarządzania Out-of-band • CPU min 800 Mhz • Minimum 1GB RAM • Minimum 256MB Flash
Wydajność	• Wydajność min. 238 Mpps • Przepustowość min. 320 Gbps
Zarządzanie	• Web GUI • HTTPs • CLI • Telnet • SSH • SNMP
Protokoły i funkcjonalności	• MIB RSPAN • Radius • TACACS+ • DiffServ • Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram • IPv4/IPv6 Multicast filtering • IGMPv3 MLDv2 Snooping • ASM & SSM • IGMPv1,v2 Querier • Auto-VoIP • Auto-iSCSI • Policy-based routing (PBR) • LLDP-MED • Spanning Tree • Green Ethernet • STP • MTP • RSTP • PV(R)STP • BPDU/STRG Root Guard • EEE (802.3az) • GVRP/GMRP • Q in Q, • Private VLAN • DOT1X • MAB

	• Captive Portal • DHCP Snooping • Dynamic ARP • Inspection • IP Source Guard • Min ilość obsługiwanych VLAN 4K • DHCP Server min 2K rezerwacji • sFlow • Ilość interfejsów IP 128 • Double VLAN Tagging (QoQ) • Yes • PIM-DM (Multicast Routing - dense mode) • PIM-DM (IPv6) • PIM-SM (Multicast Routing - sparse mode) • PIM-SM (IPv6) • RIPv1 • RIPv2 • OSPFv2 • RFC 2328 • RFC 1583 • OSPFv3 • OSPFv2 min. sąsiadów 400 • OSPFv3 min. sąsiadów 400 • OSPFv3 min. sąsiadów na interfejs 100 • UDLD • LLPF • DHCPv6 Snooping • wysyłanie alertów na email • MMRP • Ilość ACL min. 100 • Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
Stakowanie	• Minimalna ilość przełączników w stosie: 8 • Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s • Możliwość łączenia w stos za pomocą interfejsów 10Gb/s • Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh • Non-stop forwarding (NSF) • Distributed Link Aggregation (LAGs across the stack)
Gwarancja sprzętowa	Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie minimum door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

9 Wdrożenie systemu do zbierania logów systemowych dla UM

W ramach dostawy Wykonawca musi dostarczyć system do zbierania logów spełniający poniższe wymagania.
Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.
Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

Nazwa parametru	Minimalna wartość parametru
Ogólne	1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń: 1.1. System operacyjny powinien być na licencji Open Source. 1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego fizyczny serwer będący na wyposażeniu Zamawiającego wirtualna maszyna w środowisku Hyper-V. 1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source 1.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach min. procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB. 1.5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu. 1.6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514. 1.7. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport. 1.8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.

	1.9. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego. 1.10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów). 2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń: 2.1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej. 2.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego. 2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego. 2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego. 2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły: • (1x) Klaster urządzeń klasy UTM firmy Sophos • (9x) Przełączniki zarządzalne firmy CISCO,HP,3COM,ARUBA,JUNIPER,TP-LINK • (1x) Klaster przełączników zaoferowanych w projekcie • (6x) Serwery Windows • (12x) Linux dydsrybucje Debian i Rocky-Linux • (80x) stacji roboczych Windows 10 i 11 2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego. 2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów. 2.8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.

	2.9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów. 2.10. Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

10 Szkolenia specjalistyczne dla pracowników IT

W ramach dostawy Wykonawca musi przeprowadzić szkolenia z wybranych oferowanych rozwiązań lub dostarczyć voucher umożliwiający realizację takiego szkolenia przez min. rok od daty dostawy. Zakres szkoleń:

1. Szkolenie z dostarczonego systemu kopii zapasowej:
   a. Szkolenie musi zostać przeprowadzone w formie zdalnej w języku polskim.
   b. Szkolenie jest realizowane bezpośrednio przez producenta oferowanego systemu backupowego.
   c. Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego.
   d. Szkolenie musi zakończyć się imiennym certyfikatem dla min. dwóch administratorów uczestniczących w szkoleniu.
   a. Szkolenie musi trwać minimum 8 godzin.
2. Certyfikowane szkolenie w języku polskim z obsługi dostarczonego klastra firewalli dla min. jednej osoby - Sophos Firewall Certified Administrator
3. Certyfikowane szkolenie w języku polskim z obsługi dostarczonego zaawansowanego systemu bezpieczeństwa stanowiskowego dla min. jednej osoby - Sophos Firewall Certified Administrator
4. Szkolenie z obsługi systemu do zbierania logów dla min. jednej osoby:
   a. Szkolenie ma obejmować zarządzenie i administrację wdrożonym systemem do zbierania logów.
   b. Szkolenie ma odbyć się języku polskim w formie stacjonarnej, na terenie Polski lub zdalnej.
   c. Zamawiający wymaga, aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
   d. Warsztaty muszą obejmować co najmniej poniższe zagadnienia:
      i. Wstęp do zarządzania logami
      ii. Specyfika dostarczonego oprogramowania do zbierania logów – wymagania, architektura oraz różnice w wersjach oprogramowania.
      iii. Instalacja i konfiguracja ogólnych ustawień dostarczonego oprogramowania do zbierania logów
      iv. Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
      v. Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie
      vi. Wizualizacja logów, czyli tworzenie czytelnych zestawień tabelarycznych i graficznych

vii. Konfiguracja alertów i powiadomień.
viii. Administracja i utrzymanie dostarczonego oprogramowania SIEM
ix. Case Study czyli praktyczne przykłady użycia dostarczonego oprogramowania do zbierania logów

e. Zamawiający wymaga, aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)