

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

UWAGA: Oferowane produkty muszą pochodzić z autoryzowanego kanału sprzedaży na terenie Polski.

Spis treści

I.	SYSTEM DO WIRTUALIZACJI I BUDOWY KLASTRA HA.....	2
A.	SERWER DO WIRTUALIZACJI— 2SZT.....	2
B.	LICENCJA NA WINDOWS SERVER.....	8
C.	MACIERZ DYSKOWA.....	9
II.	SYSTEM KOPII ZAPASOWYCH.....	12
A.	LICENCJA NA OPROGRAMOWANIE.....	12
B.	MACIERZ DYSKOWA – 2 SZT.	14
C.	URZĄDZENIE NAS Z ZASILACZEM AWARYJNYM – 5SZT.....	18
III.	SYSTEM BEZPIECZEŃSTWA SIECIOWEGO I OCHRONY STACJI ROBOCZYCH.....	22
A.	TRADEUP JEDNOSTKI UTM FORTIGATE.....	22
B.	UTM DLA JEDNOSTEK GMINNYCH – 5SZT.....	31
C.	LICENCJA NA UWIERZYTELNIANIE DWUSKŁADNIKOWE.....	37
D.	LICENCJA NA OPROGRAMOWANIE DO OCHRONY STACJI ROBOCZYCH - ANTYWIRUS Z KLIENT VPN.....	38
E.	PRZEŁĄCZNIK ZARZĄDZANLNY Z VLAN, MACSEC – 8 SZT.....	40
IV.	SYSTEM MONITORINGU SIECIOWEGO ORAZ DO MONITOROWANIA I INWENTARYZACJI SPRZĘTU.....	42
A.	LICENCJA NA OPROGRAMOWANIE DO MONITOROWANIA SIECI ORAZ ZBIERANIA I ANALIZOWANIA LOGÓW.....	42
B.	LICENCJA NA OPROGRAMOWANIE DO MONITOROWANIA I INWENTARYZACJI SPRZĘTU KOMPUTEROWEGO.....	44
C.	OPROGRAMOWANIE DO OCHRONY I FILTROWANIA POCZTY ELEKTRONICZNEJ.....	49
V.	WDROŻENIE	52
A.	SYSTEM DO WIRTUALIZACJI I BUDOWY KLASTRA HA.....	53
B.	SYSTEM KOPII ZAPASOWYCH.....	53
C.	SYSTEM BEZPIECZEŃSTWA SIECIOWEGO I OCHRONY STACJI ROBOCZYCH.....	55
D.	SYSTEM MONITORINGU SIECIOWEGO ORAZ DO MONITOROWANIA I INWENTARYZACJI SPRZĘTU.....	57

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

I. System do wirtualizacji i budowy klastra HA

A. Serwer do wirtualizacji– 2szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 1U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	<ul style="list-style-type: none"> Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 pkt w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	<ul style="list-style-type: none"> Minimum 256GB DDR5 RDIMM 5600MT/s, Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	<ul style="list-style-type: none"> Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Gniazda PCI	<ul style="list-style-type: none"> minimum dwa sloty PCIe generacji 5
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane dwa dyski M.2 SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Wbudowane porty	<ul style="list-style-type: none"> 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1100W każdy o efektywności min. 90% w pełnym zakresie obciążenia
Bezpieczeństwo	<ul style="list-style-type: none"> Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. 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
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<p>prędkości obrotowej wentylatorów, konfiguracji serwera);</p> <ul style="list-style-type: none">○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;○ możliwość podmontowania zdalnych wirtualnych napędów;○ wirtualną konsolę z dostępem do myszy, klawiatury;○ 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;○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;○ integracja z Active Directory;○ możliwość obsługi przez dwóch administratorów jednocześnie;○ 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 <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none">○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej○ Przesyłanie danych telemetrycznych w czasie rzeczywistym○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none">• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważną

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> Serwer musi posiadać deklarację CE lub równoważną. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Serwer musi spełniać normę co najmniej Epeat Silver (według normy wprowadzonej w 2019 roku).
Dokumentacja użytkownika	<ul style="list-style-type: none"> Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	<ul style="list-style-type: none"> Gwarancji producenta: min. 2 lata Możliwość rozszerzenia gwarancji przez producenta. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. 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. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<p>pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <ul style="list-style-type: none"> Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. <p>Możliwość rozszerzenia gwarancji o:</p> <ul style="list-style-type: none"> Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało: <ul style="list-style-type: none"> Monitorowanie zdarzeń w obrębie infrastruktury Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) Zdalne lub na miejscu wdrażanie poprawek - 2x w roku Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)

B. Licencja na Windows Server.

Ze względu na posiadaną infrastrukturę oraz specyficzne wymagania związane z jej działaniem i zarządzaniem, Zamawiający oczekuje dostarczenia licencji Microsoft Windows Server 2022 Datacenter w

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

ilości, która będzie w pełni pokrywać liczbę rdzeni procesorów zainstalowanych w zaoferowanych serwerach. Zamawiający wymaga dostarczenia licencji w formie, która umożliwi ich natychmiastową aktywację i integrację z już istniejącą infrastrukturą IT, w sposób zgodny z polityką licencyjną Microsoft, w szczególności dotyczącą licencjonowania środowisk zwirtualizowanych oraz serwerów o dużej liczbie rdzeni procesorowych.

C. Macierz dyskowa.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa RACK o wysokości maksymalnie 2U umożliwiającą montaż w standardowej szafie RACK
Kontrolery	Dwa kontrolery wyposażone w przynajmniej 16GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania baterijnego przez 72 godziny lub jako zrzut na pamięć flash.
Dyski	System musi zostać dostarczony w konfiguracji zawierającej minimum: 10 dysków o pojemności min. 1.92TB NVMe SSD Obsługa wszystkich dysków musi się odbywać przez te same dwa kontrolery macierzy. System musi mieć możliwość rozbudowy do minimum 500TB przestrzeni RAW oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami) jeżeli istnieje model wyższy. System musi pozwalać o rozbudowę o dyski NVMe, SSD oraz HDD (co najmniej NL-SAS) poprzez dokładanie zewnętrznych półek dyskowych.
Wydajność	Macierz musi umożliwiać osiągnięcie nie mniej niż 550 000 IOps przy ruchu random dla bloku 4KB 100% odczytów. Wydajność macierzy w oferowanej konfiguracji opartej o dyski pojemności 1,92TB lub NVMe SSD przy dostępie losowym „random” to minimum 180 000 IOPS przy proporcji 70/30% odczyt/zapis blokiem 4KB z pominięciem Cache, wydajność z

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<p>samych dysków w konfiguracji Raid 5 przy opóźnieniu max. 6 ms.</p> <p>Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy potwierdzający spełnienie tego wymogu.</p>
Porty	<p>Oferowana macierz musi mieć minimum:</p> <ul style="list-style-type: none"> • 8 portów 25Gb iSCSI z wkładkami lub 8 x 25Gb SFP • 2 porty 1Gb do zarządzania
Raid	<p>Wsparcie dla RAID: 0, 1, 5, 6, 10</p> <p>Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.</p>
Protokoły	<p>Wspierane protokoły: FC, iSCSI, CIFS, NFS, S3</p> <p>Zamawiający dopuszcza zaoferowania rozwiązania, które realizuje CIFS, NFS czy S3 za pomocą oprogramowania typu Software Defined Storage ze wsparciem aktualizacyjnym i technicznym zgodnie z zaoferowaną gwarancją na macierz.</p> <p>W przypadku zaoferowania rozwiązania opartego o „Software Defined Storage” należy w ofercie podać nazwę proponowanego rozwiązania.</p>
Wymagania funkcjonalne	<p>a) Macierz musi posiadać wsparcie dla wielościeżkowych dla systemów:</p> <p>b) Microsoft® Windows Server®, Red Hat Enterprise Linux®, VMware® ESX®</p> <p>c) Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen.</p> <p>d) Macierz musi posiadać funkcjonalność klonowania danych.</p> <p>e) Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie</p> <p>f) Macierz musi posiadać funkcjonalność balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online wolumenów logicznych. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.</p> <p>g) Z poziomu graficznego interfejsu do zarządzania istnieje możliwość sprawdzenia</p>

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<p>stanu zużycia dysków flash.</p> <p>h) Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków.</p> <p>i) Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:</p> <ul style="list-style-type: none"> wydajności i opóźnień na wolumenach wydajności I/Ops, MB/s trafności w cache kontrolerów <p>j) Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem uwierzytelniania i dostępu dla użytkowników/administratorów.</p> <p>k) Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:</p> <ul style="list-style-type: none"> Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter VMware VASA Microsoft Virtual Disk Service (VDS) Microsoft Virtual Shadow Service (VSS) <p>l) Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.</p> <p>m) Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.</p>
Certyfikaty	<p>a) Macierz musi być wyprodukowany zgodnie z normą: ISO-9001:2025, ISO-14001 lub równoważną.</p>
Gwarancja producenta	<p>Min. 2 lata serwisu producenta macierzy z czasem dostawy części zamiennych na następny dzień roboczy</p> <p>Dostęp do centrum serwisowego 24/7</p> <p>Możliwość zgłaszania awarii 24/7</p> <p>3 lata aktualizacji do oprogramowania oraz dostęp do portalu serwisowego</p>



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	<p>producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.</p> <p>W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 oraz posiadać autoryzacje producenta urządzeń.</p> <p>Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p>

II. System kopii zapasowych.

A. Licencja na oprogramowanie.

Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych min. 15 maszyn wirtualnych uruchomianych w środowisku Zamawiającego.

Zamawiający wymaga, aby oprogramowanie było objęte wsparciem technicznym producenta oprogramowania (wraz z prawem do używania najnowszej wersji oprogramowania) na okres min. 24 miesięcy.

Wymagania minimalne dotyczące funkcjonalności dostarczonego oprogramowania

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE

Rozwiązanie musi wspierać systemy operacyjne macOS

Rozwiązanie musi wspierać wykonywanie kopii zapasowych następujących systemów plików:

NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Btrfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów

Rozwiązanie musi wspierać backup podłączonych dysków USB

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym

Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:

- Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny
- Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
- Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
- Zcentralizowanym repozytorium danych
- Bezpośrednio na zasobach Chmury

Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft

Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.

Rozwiązanie musi wspierać technologię BitLocker

Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:

- Microsoft Exchange 2010 i nowszych
- Microsoft Active Directory 2003 i nowszych
- Microsoft Sharepoint 2010 i nowszych
- Microsoft SQL 2005 i nowszych
- Oracle 11g i nowszych

Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2

Rozwiązanie musi wspierać szyfrowanie

Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego

Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

B. Macierz dyskowa – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Procesor 64-bitowy x86 osiągający w teście PassMark Performance Test, co najmniej 13 0000 punktów w kategorii Average CPU Marko, o taktowaniu nie

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
	mniej niż 3,4 GHz
Zainstalowana pamięć RAM	Min. 16 GB ECC DDR4, możliwość rozbudowy do 128 GB
Pamięć Flash	Min. 5 GB
Liczba zatok na dyski	Min.18, w tym min. 12 x 3,5-calowych SATA oraz min. 6 x 2,5-calowych SATA
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD
Zainstalowane dyski twarde	Min. 12 szt. dysków o pojemności min. 12TB 7200 obr/min dedykowanych do pracy w urządzeniu typu NAS. Dyski muszą znajdować się na liście kompatybilności publikowanej przez producenta urządzenia.
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Min 2 x RJ-45
Porty LAN 10 GbE	Min2
Porty USB 3.2 Gen2	Minimum 4 x typu A
Port PCIe	Min. 3 szt.
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Zasilanie	Zasilacz redundatny 2 x max 550 W, 100-240 V
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Agregacja łączy	Tak



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Warunki gwarancji	Wymagane min. 2 lata gwarancji producenta urządzenia. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

C. Urządzenie NAS z zasilaczem awaryjnym – 5szt.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	64-bitowy ARM
Procesor liczba rdzeni	Nie mniej niż 4, minimalne taktowanie 1,7GHz



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Pamięć RAM	Nie mniej niż 4GB DDR4
Pamięć RAM liczba slotów	Minimum 1 slot
Pamięć RAM - możliwość rozszerzenia	nie mniej niż do 16GB
Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 9, w tym minimum 5 zatok na dyski 3,5 calowe
Obsługiwane dyski twarde	3.5" oraz 2.5" SATA o pojemności do 22TB
Zainstalowane dyski	min. 3 dyski o pojemności min. 8TB dedykowanych do pracy w oferowanym serwerze NAS, dyski muszą się znajdować na liście kompatybilności producenta oferowanego urządzenia
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej dwóch
Porty LAN	Minimum 2 x 2,5 Gb/s oraz 2 x 10GbE SFP+
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2	Minimum 3
Przyciski	Zasilanie, Reset, Kopiowanie USB
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Zasilanie	Zasilacz 120 W, 100-240 V
Agregacja łącz	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	Tak, min AES 256

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	<p>Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek woluminów i LUN blokowych Obsługa replikacji migawek</p>
Wbudowana obsługa iSCSI	<p>Multi-LUN na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN</p>
Zarządzanie prawami dostępu	<p>Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL</p>
Obsługa Windows AD	<p>Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP</p>
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	<p>Monitoring i zarządzanie urządzeniem Synchronizacja plików Obsługa kamer Dostępne na systemy iOS oraz Android</p>

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Ustawienia: Back up, przywracania, resetowania systemu
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Parametr	Charakterystyka (wymagania minimalne)
Gwarancja	Gwarancja producenta min. 2 lata door-to-door

Do każdego urządzenia NAS Wykonawca dostarczy zasilacz UPS o następujących parametrach:

- Moc pozorna min. 1200 VA
- Moc czynna min 650 W
- Architektura UPS-a: line-interactive
- Liczba faz na wejściu 1 (230V)
- Liczba akumulatorów 1
- Czas podtrzymania (obciążenie 100%) min. 1 min
- Typ obudowy Tower
- Funkcje specjalne: AVR
- Porty zasilania wy. 4 x typ C/F (Schuko)
- Gniazda we/wy: 1 x USB (Type B) 2 x RJ-45 (iLO Remote Management Network)
- Wymiary: suma wymiarów szer/dł/wys maks. 75 cm
- Waga: maks. 8 kg

III. System bezpieczeństwa sieciowego i ochrony stacji roboczych.

A. TradeUp jednostki UTM Fortigate.

Zamawiający jest w posiadaniu urządzenia UTM firmy Fortinet model Fortigate 80E, które w ramach niniejszego postępowania zamierza zmodernizować. Wykonawca zobowiązany jest dostarczyć nowe, kompatybilne urządzenie UTM o poniższych parametrach:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 10 portami Gigabit Ethernet RJ-45.
 - 8 gniazdami SFP 1 Gbps.
 - 4 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
- Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
- Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługę protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen aktywne przez okres min. 2 lat od daty rejestracji.

Gwarancja oraz wsparcie

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. System jest objęty serwisem gwarancyjnym producenta przez okres min.2 lat od daty rejestracji.
2. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora obowiązującym przez okres 2 lat. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 - wymagane dostarczenie dokumentu potwierdzającego spełnienie warunku
3. Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
4. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym
5. Certyfikat ISO 9001 podmiotu serwisującego.

B. UTM dla Jednostek Gminnych – 5szt.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
 - 4 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 900 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 450 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19 i 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
 - Routingu statycznego.
 - Policy Based Routingu.
 - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 24 miesięcy.

Gwarancja oraz wsparcie



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. System jest objęty serwisem gwarancyjnym producenta przez okres min.2 lat od daty rejestracji.
2. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora obowiązującym przez okres 2 lat. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 - wymagane dostarczenie dokumentu potwierdzającego spełnienie warunku
3. Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
4. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym
5. Certyfikat ISO 9001 podmiotu serwisującego.

C. Licencja na uwierzytelnianie dwuskładnikowe.

Parametr	Charakterystyka (wymagania minimalne)
Sposób autoryzacji	Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych współpracujące z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site
Ilość tokenów programowalnych	min. 100 szt.
Wsparcie dla tokenów programowych (software token) dla systemów operacyjnych	iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
Wymagania dla tokenów na system iOS i Android	<ul style="list-style-type: none"> ▪ aktywacji z systemu firewall FortiGate ▪ generowania kodu (cyfr) co 30 lub 60 sekund, ▪ możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ▪ ochrony dostępu poprzez konfigurowalny kod PIN
Typ licencji	<ul style="list-style-type: none"> ▪ wieczysta

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

D. Licencja na oprogramowanie do ochrony stacji roboczych - antywirus z klient VPN.

W ramach postępowania wymagany jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.

Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

Parametry systemu ochrony dla stacji roboczych.

1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:
 - Kontrola antywirusowa.
 - Funkcja analizy plików w zewnętrznym systemie Sandbox.
 - Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.
 - URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
 - Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
 - Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
 - Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
 - Mechanizmy uwierzytelniania dwuskładnikowego
 - AntiExploit,
 - blokowanie dysków przenośnych typu USB,
2. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows Serwer 2019, Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.
3. Wymagany jest aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach postępowania powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. W ramach postępowania muszą zostać dostarczone niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji.

Parametry systemu centralnego zarządzania.

1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.

2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.
3. Ponadto wymagane jest aby system zapewniał:
 - integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,
 - definiowanie różnych profili (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,
 - zautomatyzowany proces zarządzania aplikacją kliencką,
 - przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.
 - możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,
 - panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,
 - panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,
 - możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,
 - automatyczne wykrywanie stacji klienckich w grupach roboczych,
 - logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcją filtrów oraz możliwością pobierania logów przez administratora,
 - generowanie alarmów: związanych z zarządzaniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.
 - definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcją przypisywania uprawnień do elementów panelu konfiguracyjnego,
 - zarządzanie certyfikatami na potrzeby połączeń IPsec VPN oraz SSL VPN,
 - automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,
 - możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,
 - możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
 - możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.
4. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.
5. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

Licencje oraz serwisy.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje aktywne przez okres 2 lat od daty rejestracji upoważniające do:

1. Zainstalowania i centralnego zarządzania aplikacjami klienckimi na min. 100 stacjach roboczych.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:
 - a) Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access, Sandbox Agent with Cloud Sandbox subscription, centralne zarządzanie

System musi być objęty serwisem producenta ważnym przez okres 2 lat od daty rejestracji, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

E. Przełącznik zarządzalny z VLAN, MACsec – 8 szt.

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z systemem bezpieczeństwa, wyspecyfikowanym w punkcie III.A. OPZ posiadający następujące parametry:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Budżet mocy dla portów PoE min.: 740 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 160 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - 48 porty GE RJ-45 (W tym porty PoE w ilości co najmniej: 48, zgodne ze standardem: 802.3af oraz 802.3at.).
 - 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty autoryzowanym serwisem gwarancyjnym producenta przez okres min. 2 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

IV. System monitoringu sieciowego oraz do monitorowania i inwentaryzacji sprzętu.

A. Licencja na oprogramowanie do monitorowania sieci oraz zbierania i analizowania logów.

W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
 - Listę najczęściej wykrywanych ataków.
 - Listę najbardziej aktywnych użytkowników.
 - Listę najczęściej wykorzystywanych aplikacji.
 - Listę najczęściej odwiedzanych stron www.
 - Listę krajów , do których nawiązywane są połączenia.
 - Listę najczęściej wykorzystywanych polityk Firewall.
 - g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - Malware.
 - Aplikacje sieciowe.
 - Email.
 - IPS.
 - Traffic.
1. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
5. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.
6. Funkcję, która umożliwia administratorom wyświetlanie alertów typu Outbreak i automatyczne pobieranie powiązanych zdarzeń oraz raportów od producenta rozwiązania.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

Licencja na system musi być aktywna przez okres min. 2 lat od daty rejestracji oraz upoważniać do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

B. Licencja na oprogramowanie do monitorowania i inwentaryzacji sprzętu komputerowego.

Wymagania ogólne

Zamawiający wymaga dostarczenia licencji wieczystej ze wsparciem producenta na minimum 24 miesiące.

Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

Zamawiający posiada 250 komputerów, na których wymagane jest zainstalowanie dedykowanego oprogramowania w postaci agenta. Instalacja musi zostać przeprowadzona na każdym z tych urządzeń, zapewniając pełną funkcjonalność agenta zgodnie z jego przeznaczeniem.

Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych strictly technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agent, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agent. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na pie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
 - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
 - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem)
 - program ma możliwość wykonywania operacji testowych
 - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
 - zmian stanu interfejsów sieciowych
 - ruchu sieciowego
 - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
 - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- wydajności systemów Windows:
 - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0

Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

- Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
- Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
- Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
- Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
- Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.
- Umożliwia odczytanie numeru seryjnego (klucze licencyjne).
- Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
- Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości
 - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV), przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczanego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencji/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

- Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
- Informacje o aplikacjach używanych w organizacji.
- Tworzenie własnych wzorców aplikacji.
- Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- Informacje o komputerach, na których aplikacja została wykryta.
- Zarządzanie posiadanymi licencjami.
- Wskazywanie osób odpowiedzialnych za licencję.
- Wskazanie użytkowników licencji.
- Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
- Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- Zarządzanie posiadanymi licencjami: raport zgodności licencji.
- Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział.

C. Oprogramowanie do ochrony i filtrowania poczty elektronicznej.

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiającą zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz IMAP.
11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
7. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
8. Ochronę typu wirus outbrake.

Kontrola antyspamowa

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Ochrona typu outbrake.
13. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
14. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 7 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

W ramach zamówienia powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu virus outbreak oraz usługa sandbox w chmurze na okres 2 lat od daty rejestracji.

Gwarancja oraz wsparcie

1. System musi być objęty autoryzowanym serwisem producenta przez okres min. 2 lat, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7
2. Wykonawca musi posiadać autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

V. Wdrożenie

Zamawiający nie dopuszcza możliwości wykonywania prac wdrożeniowych w formie zdalnej, co oznacza, że wszystkie prace związane z wdrożeniem muszą być realizowane na miejscu, w siedzibie Zamawiającego lub

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

w innym wskazanym przez niego lokalizacji. Wymóg ten wynika z konieczności zapewnienia pełnej kontroli nad procesem wdrożenia, bezpośredniego nadzoru nad wykonywanymi pracami oraz możliwości bieżącej współpracy z zespołem technicznym Zamawiającego. Ponadto, prace wdrożeniowe na miejscu umożliwią szybkie reagowanie na ewentualne problemy, a także bezpośrednie testowanie i weryfikację poprawności działania systemu w rzeczywistym środowisku operacyjnym. Realizacja prac na miejscu ma na celu również minimalizację ryzyka związanego z bezpieczeństwem danych i dostępem do infrastruktury IT.

A. System do wirtualizacji i budowy klastra HA.

Dostawca zapewni instalację oraz konfigurację dostarczonego sprzętu i oprogramowania w miejscu wskazanym przez Zamawiającego. W zakres prac wdrożeniowych wchodzić będzie:

- Prawidłowe zamontowanie serwerów oraz macierzy w szafie rack, z zachowaniem odpowiedniej organizacji okablowania oraz zapewnieniem poprawnej wentylacji i zasilania urządzeń.
- Konfiguracja systemu wirtualizacji, klastra HA (High Availability) oraz macierzy dyskowej zgodnie z wymaganiami funkcjonalnymi i wydajnościowymi Zamawiającego, w tym konfiguracja redundancji oraz mechanizmów failover.
- Zapewnienie optymalnych ustawień sieciowych, w tym konfiguracja sieci VLAN, portów trunkingowych, a także parametrów związanych z bezpieczeństwem sieci, takich jak firewall, VPN oraz mechanizmy kontroli dostępu zgodnie z polityką bezpieczeństwa Zamawiającego.
- Integracja z systemami zarządzania tożsamością (np. Active Directory) w celu zapewnienia bezpiecznego i scentralizowanego zarządzania uprawnieniami dostępu do zasobów w nowym środowisku.
- Migracja maszyn wirtualnych Zamawiającego do nowego środowiska wirtualizacyjnego, obejmująca planowanie migracji, zabezpieczenie danych, testowanie procesu migracji oraz zapewnienie minimalizacji przestojów w pracy systemów.
- Testowanie poprawności działania środowiska po wdrożeniu, w tym weryfikacja poprawności działania systemów wysokiej dostępności (HA), wydajności macierzy dyskowych oraz komunikacji sieciowej.
- Szkolenie techniczne dla zespołu Zamawiającego w zakresie obsługi i podstawowej administracji nowego środowiska, obejmujące kluczowe aspekty zarządzania i monitoringu systemów.
- Dostarczenie pełnej dokumentacji powdrożeniowej, w tym opisów konfiguracji, parametrów systemowych oraz procedur awaryjnych, umożliwiających samodzielną administrację środowiskiem przez Zamawiającego.
- Zapewnienie wsparcia technicznego w okresie wdrożeniowym oraz w ustalonym okresie po zakończeniu wdrożenia w ramach umowy serwisowej, obejmujące diagnozowanie i rozwiązywanie problemów oraz doradztwo w zakresie optymalizacji środowiska.

B. System kopii zapasowych.

Dostawca zapewni instalację, konfigurację oraz uruchomienie kompleksowego systemu kopii zapasowych, składającego się z profesjonalnego oprogramowania do backupu oraz dedykowanych macierzy dyskowych typu NAS. System ten będzie odpowiadał za zabezpieczenie danych Zamawiającego oraz umożliwienie ich szybkiego odtworzenia w przypadku awarii, uszkodzenia lub utraty danych. W systemie kopii zapasowych będą wykorzystywane dwie macierze, zlokalizowane w różnych miejscach. Pierwsza macierz będzie pełniła rolę głównej jednostki przechowującej kopie zapasowe, podczas gdy druga będzie pełniła rolę dodatkowej lokalizacji, zapewniającej redundantność oraz bezpieczeństwo danych. Obie macierze będą ze sobą zsynchronizowane w sposób zapewniający regularne tworzenie kopii zapasowych danych. Dzięki

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

geograficznemu rozproszeniu macierzy, system zapewni wysoką dostępność oraz ochronę danych na wypadek awarii lub zdarzeń losowych w jednej z lokalizacji. Ponadto, dla jednostek gminnych wdrożone zostaną niezależne macierze NAS (5 szt.) w celu zapewnienia lokalnej ochrony danych. Wdrożenie obejmie:

System kopii zapasowych dla Urzędu

1. **Instalacja i konfiguracja oprogramowania do tworzenia kopii zapasowych** – instalacja specjalistycznego oprogramowania backupowego na wyznaczonych serwerach lub maszynach wirtualnych, które zostaną skonfigurowane zgodnie z wymaganiami infrastruktury Zamawiającego. W ramach prac zostaną wdrożone:
 - **Harmonogramy kopii zapasowych** – zdefiniowanie regularnych kopii zapasowych dla maszyn wirtualnych, baz danych oraz innych kluczowych danych, w oparciu o politykę bezpieczeństwa i czas retencji danych.
 - **Polityki backupu** – określenie strategii wykonywania kopii zapasowych (pełnych, przyrostowych, różnicowych), ich częstotliwości oraz sposobu przechowywania, zgodnie z priorytetami dla kluczowych danych.
 - **Optymalizacja transferu danych** – zastosowanie deduplikacji, kompresji oraz innych mechanizmów optymalizacji, aby zapewnić efektywne wykorzystanie przestrzeni dyskowej i minimalne obciążenie sieci podczas przesyłu danych.
2. **Wdrożenie i konfiguracja macierzy dyskowych typu NAS** – instalacja i uruchomienie dedykowanych macierzy dyskowych NAS w celu przechowywania kopii zapasowych:
 - **Podłączenie macierzy** – fizyczna instalacja i podłączenie macierzy NAS do sieci Zamawiającego w miejscu wskazanym przez Zamawiającego.
 - **Konfiguracja przestrzeni dyskowych** – utworzenie wolumenów oraz udziałów sieciowych na macierzach, aby optymalnie zarządzać przechowywaniem kopii zapasowych oraz wydajnością zapisu/odczytu danych.
 - **Bezpieczeństwo i dostępność danych** – zastosowanie konfiguracji RAID dla redundancji danych, a także zabezpieczenia takie jak szyfrowanie, kontrola dostępu oraz monitoring dostępu do danych.
3. **Integracja oprogramowania backupowego z macierzami NAS** – skonfigurowanie ścisłej współpracy pomiędzy systemem backupu a macierzami dyskowymi:
 - **Miejsca docelowe kopii zapasowych** – wskazanie udziałów sieciowych na macierzach NAS jako głównych miejsc przechowywania kopii zapasowych zgodnie z politykami retencji.
 - **Testy procesu backupu i przywracania danych** – przeprowadzenie próbnych backupów oraz testowego odtwarzania danych, weryfikując poprawność działania całego procesu i jego zgodność z oczekiwaniami Zamawiającego.

Niezależne systemy kopii zapasowych dla jednostek gminnych

Dla zapewnienia lokalnej ochrony danych w jednostkach gminnych, Dostawca wdroży pięć niezależnych macierzy NAS, które będą służyć jako lokalne systemy kopii zapasowych. Prace będą obejmować:

4. **Wdrożenie i konfiguracja niezależnych macierzy NAS dla jednostek gminnych (5 szt.)** – każda z jednostek gminnych zostanie wyposażona w dedykowaną macierz NAS, która umożliwi lokalne przechowywanie kopii zapasowych i szybkie odzyskiwanie danych:
 - **Podłączenie i montaż macierzy w jednostkach gminnych** – instalacja macierzy w wyznaczonych lokalizacjach oraz integracja z lokalną infrastrukturą sieciową każdej jednostki gminnej.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- **Konfiguracja przestrzeni dyskowej na macierzach** – utworzenie i skonfigurowanie odpowiednich wolumenów na macierzach NAS dla przechowywania lokalnych kopii zapasowych.
 - **Zabezpieczenie danych i kontrola dostępu** – wdrożenie odpowiednich poziomów zabezpieczeń, takich jak szyfrowanie danych, kontrola dostępu oraz tworzenie lokalnych strategii backupu w celu ochrony danych gminnych.
5. **Konfiguracja lokalnego oprogramowania backupowego** – każda jednostka gminna zostanie wyposażona w lokalne rozwiązanie do backupu, umożliwiające tworzenie i zarządzanie kopią zapasową danych bezpośrednio na lokalnej macierzy NAS:
- **Ustawienie harmonogramów i polityk backupu** – skonfigurowanie odpowiednich planów wykonywania kopii zapasowych w każdej jednostce gminnej, zgodnie z ich potrzebami oraz wymogami bezpieczeństwa.
 - **Testy działania i odtwarzania kopii zapasowych** – przeprowadzenie testów w celu weryfikacji poprawności backupu oraz możliwości szybkiego odtwarzania danych na poziomie lokalnej jednostki.
6. **Szkolenie zespołów Jednostek Gminnych oraz Zamawiającego** – przekazanie wiedzy niezbędnej do obsługi i zarządzania systemami kopii zapasowych:
- Szkolenie dla zespołu Zamawiającego w zakresie obsługi i administracji systemu backupu i macierzy NAS.
 - Szkolenie dla wybranych pracowników jednostek gminnych w zakresie lokalnego backupu, odzyskiwania danych oraz zarządzania lokalnymi macierzami NAS.
7. **Dostarczenie dokumentacji powdrożeniowej** – przygotowanie pełnej dokumentacji wdrożeniowej dla centralnego systemu kopii zapasowych oraz dla niezależnych macierzy w jednostkach gminnych, obejmującej:
- Szczegółowe opisy konfiguracji systemów backupu oraz macierzy.
 - Procedury odzyskiwania danych i instrukcje obsługi.
 - Zalecenia dotyczące dalszego utrzymania i rozwoju systemów.
8. **Wsparcie techniczne po wdrożeniu** – zapewnienie okresowego wsparcia technicznego po zakończeniu wdrożenia przez 30 dni, w tym:
- Pomoc w rozwiązywaniu ewentualnych problemów z systemami kopii zapasowych.
 - Aktualizacje oprogramowania oraz doradztwo w zakresie optymalizacji polityk backupu zarówno dla centralnego systemu, jak i jednostek gminnych.

Dzięki wdrożeniu systemu kopii zapasowych zarówno w głównej infrastrukturze Zamawiającego, jak i w lokalnych jednostkach gminnych, Zamawiający uzyska kompleksową ochronę danych, zapewniającą ich bezpieczne przechowywanie i szybkie odzyskiwanie w przypadku awarii lub utraty danych.

C. System bezpieczeństwa sieciowego i ochrony stacji roboczych.

Dostawca zapewni instalację, konfigurację oraz uruchomienie kompleksowego systemu bezpieczeństwa sieciowego i ochrony stacji roboczych w lokalizacjach wskazanych przez Zamawiającego. System będzie obejmować rozwiązania zapewniające ochronę sieci, kontrolę dostępu oraz zabezpieczenie stacji roboczych, gwarantując spójność polityki bezpieczeństwa w całej infrastrukturze. Zakres prac wdrożeniowych będzie obejmować:

1. **Modernizacja jednostki UTM FortiGate** – wymiana obecnego urządzenia UTM FortiGate 80E na wydajniejszy w celu poprawy działania oraz bezpieczeństwa sieci. Dostawca przeprowadzi instalację

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

nowych urządzeń w sposób minimalizujący przestoje, przenosząc istniejące konfiguracje oraz reguły bezpieczeństwa do nowych urządzeń. Proces ten obejmie także:

- Szczegółowe dostosowanie reguł firewall, filtrowania treści, kontroli aplikacji, systemu zapobiegania włamaniom (IPS), oraz mechanizmów antywirusowych.
 - Optymalizację ustawień QoS (Quality of Service) dla ruchu sieciowego w celu zapewnienia wysokiej wydajności sieci i niezawodności komunikacji.
2. **Wdrożenie urządzeń UTM dla jednostek gminnych (5 szt.)** – instalacja oraz konfiguracja dodatkowych urządzeń UTM w wybranych jednostkach gminnych, zapewniając spójność polityk bezpieczeństwa z centralnym systemem FortiGate. Każde z urządzeń będzie dostosowane do specyficznych potrzeb danej lokalizacji, a konfiguracja obejmie:
- Ustawienie filtrów bezpieczeństwa oraz monitorowanie ruchu sieciowego w celu wykrywania i zapobiegania zagrożeniom.
 - Konfigurację reguł dostępu, aby umożliwić kontrolowany i bezpieczny ruch pomiędzy jednostkami gminnymi a siecią główną.
3. **Implementacja dwuetapowego uwierzytelniania (2FA) dla VPN** – uruchomienie licencji na uwierzytelnianie dwuskładnikowe dla użytkowników zdalnie łączących się z siecią poprzez VPN. Dwuetapowe uwierzytelnianie zwiększy poziom bezpieczeństwa dostępu do zasobów wewnętrznych. Wdrożenie obejmie:
- Integrację mechanizmu 2FA z systemami zarządzania tożsamością, takimi jak Active Directory.
 - Konfigurację i przetestowanie poprawności działania mechanizmu 2FA, obejmującą zarówno uwierzytelnianie użytkowników, jak i poprawność procesu logowania do VPN.
4. **Wdrożenie oprogramowania ochrony stacji roboczych (80 stanowisk)** – instalacja oraz konfiguracja oprogramowania antywirusowego zintegrowanego z klientem VPN na stacjach roboczych Zamawiającego. Dostawca zadba o:
- Wdrożenie centralnego systemu zarządzania, który umożliwi zdalne monitorowanie stanu ochrony wszystkich stanowisk oraz dystrybucję aktualizacji.
 - Konfigurację zasad bezpieczeństwa, w tym regularne skanowanie antywirusowe, wykrywanie złośliwego oprogramowania, kontrolę dostępu do urządzeń peryferyjnych (takich jak nośniki USB), oraz ustawienie parametrów zabezpieczenia połączeń VPN.
5. **Konfiguracja zarządzalnych przełączników z obsługą VLAN oraz MACsec (8 szt.)** - w ramach wdrożenia Dostawca przeprowadzi wymianę istniejących przełączników sieciowych na nowe, zarządzalne przełączniki z obsługą VLAN oraz protokołu MACsec. Nowe urządzenia będą odpowiadać za zasilanie telefonów VoIP (Power over Ethernet – PoE), dlatego konfiguracja będzie uwzględniać zapewnienie nieprzerwanej pracy systemu telefonii IP. Zakres prac obejmuje:
- Bezprzerwowa migracja i wymiana przełączników – planowa wymiana istniejących urządzeń na nowe przełączniki zarządzalne, z zachowaniem ciągłości pracy systemu VoIP. Dostawca zadba o odpowiednie skonfigurowanie portów PoE, aby zapewnić natychmiastowe i stabilne zasilanie telefonów VoIP, minimalizując ryzyko przestojów.
 - Konfiguracja VLAN – utworzenie odpowiednich segmentów sieci VLAN w celu oddzielenia ruchu danych oraz głosu (VoIP), zgodnie z najlepszymi praktykami bezpieczeństwa i wydajności sieci. Dzięki temu możliwe będzie:
 - Osiągnięcie optymalizacji ruchu VoIP, zapewniając jego priorytetowe traktowanie (QoS).
 - Zwiększenie bezpieczeństwa sieci poprzez izolację ruchu różnych rodzajów usług (np. rozdzielanie sieci użytkowników od sieci administracyjnej).
 - Obsługa MACsec – skonfigurowanie zabezpieczeń warstwy łącza danych za pomocą protokołu MACsec, zapewniając szyfrowanie ruchu sieciowego pomiędzy przełącznikami oraz ochronę przed nieuprawnionym dostępem na poziomie fizycznym sieci.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

- Integracja z UTM FortiGate – skonfigurowanie przełączników w pełnej zgodności z urządzeniami UTM FortiGate, umożliwiając spójne zarządzanie politykami bezpieczeństwa w całej sieci. Obejmuje to dynamiczne kierowanie ruchu pomiędzy VLAN-ami przez FortiGate oraz zarządzanie dostępem sieciowym z centralnego punktu kontrolnego.
 - Konfiguracja portów przełączników – odpowiednie ustawienie portów trunkingowych oraz dostępowych z obsługą PoE dla telefonów VoIP, a także skonfigurowanie portów dla stacji roboczych zgodnie z polityką dostępu Zamawiającego. Wszystkie porty zostaną zabezpieczone zgodnie z wymogami bezpieczeństwa, w tym z obsługą MACsec i przypisaniem do właściwych VLAN-ów.
6. **Testy funkcjonalne i bezpieczeństwa** – po wdrożeniu, Dostawca przeprowadzi kompleksowe testy systemu, w tym:
- Weryfikację poprawności działania urządzeń UTM oraz skuteczności w ochronie sieci przed zagrożeniami.
 - Testowanie działania połączeń VPN z uwierzytelnianiem dwuskładnikowym oraz poprawności funkcjonowania klientów antywirusowych na stacjach roboczych.
 - Sprawdzenie integracji wszystkich komponentów, w tym przełączników z UTM FortiGate, zapewniając właściwe przekierowanie ruchu sieciowego oraz bezpieczeństwo danych.
7. **Szkolenie zespołu Zamawiającego** – przekazanie wiedzy z zakresu obsługi i administracji wdrożonych systemów bezpieczeństwa, obejmujące:
- Zarządzanie urządzeniami FortiGate, konfigurowanie i monitorowanie polityk bezpieczeństwa oraz podstawy analizy zdarzeń sieciowych.
 - Zarządzanie klientami antywirusowymi oraz VPN na stacjach roboczych, w tym aktualizacje i podstawowe działania naprawcze.
 - Zarządzanie i utrzymanie przełączników sieciowych, w tym tworzenie i zarządzanie VLAN-ami oraz monitorowanie bezpieczeństwa warstwy łącza danych.
8. **Dostarczenie dokumentacji powdrożeniowej** – przygotowanie i przekazanie szczegółowej dokumentacji obejmującej:
- Szczegółowe opisy konfiguracji urządzeń UTM, przełączników sieciowych oraz klientów ochrony stacji roboczych.
 - Instrukcje dotyczące zarządzania, procedury postępowania w sytuacjach awaryjnych oraz wytyczne dotyczące aktualizacji systemu.
9. **Wsparcie techniczne po wdrożeniu** – Dostawca zapewni wsparcie techniczne po zakończeniu wdrożenia przez 30 dni, obejmujące:
- Pomoc w rozwiązywaniu problemów związanych z działaniem systemu bezpieczeństwa sieciowego.
 - Aktualizacje oraz doradztwo w zakresie utrzymania i optymalizacji infrastruktury.

D. System monitoringu sieciowego oraz do monitorowania i inwentaryzacji sprzętu.

W ramach wdrożenia zostanie zainstalowany i skonfigurowany kompleksowy system monitoringu sieciowego oraz inwentaryzacji sprzętu komputerowego, a także system ochrony poczty elektronicznej. Celem wdrożenia jest zapewnienie efektywnego nadzoru nad infrastrukturą sieciową, sprzętem komputerowym oraz bezpieczeństwem komunikacji e-mail. Cały proces wdrożenia zostanie przeprowadzony z zachowaniem minimalnych przestoju w pracy Urzędu, aby zapewnić ciągłość działania systemów.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

1. Instalacja i konfiguracja oprogramowania do monitoringu sieciowego

Wdrożenie oprogramowania do aktywnego monitorowania infrastruktury sieciowej Zamawiającego, które będzie odpowiadać za zbieranie danych o stanie sieci, wydajności oraz dostępności jej elementów:

- **Konfiguracja serwera monitoringu** – zainstalowanie i skonfigurowanie dedykowanego serwera, który będzie odpowiadał za zbieranie i analizę danych dotyczących sieci. Serwer zostanie przygotowany zgodnie z wymaganiami infrastruktury, z uwzględnieniem odpowiedniej wydajności i redundancji.
- **Monitorowanie urządzeń sieciowych** – skonfigurowanie systemu monitoringu w celu bieżącej kontroli stanu urządzeń sieciowych (np. routerów, przełączników, firewalli), w tym sprawdzanie dostępności, obciążenia, przepustowości oraz wykrywanie ewentualnych problemów.
- **Tworzenie map sieci oraz alarmów** – zdefiniowanie graficznych map sieci przedstawiających topologię infrastruktury, połączonych z systemem alertów. W przypadku wykrycia problemów (np. awarii, przeciążenia) system automatycznie wyśle powiadomienia do odpowiednich osób odpowiedzialnych za utrzymanie.
- **Raportowanie i analiza trendów** – wdrożenie mechanizmów umożliwiających generowanie raportów dotyczących stanu i wydajności sieci, analizę trendów oraz identyfikację potencjalnych problemów zanim wpłyną na działanie infrastruktury.

2. Wdrożenie oprogramowania do monitorowania oraz inwentaryzacji sprzętu

Równolegle z monitoringiem sieci zostanie wdrożone dedykowane oprogramowanie do inwentaryzacji i monitorowania komputerów oraz innych urządzeń końcowych w sieci, z uwzględnieniem zbierania danych z komputerów Urzędu oraz Jednostek Gminnych (250 sztuk):

- **Inwentaryzacja sprzętu i oprogramowania** – zainstalowanie narzędzi umożliwiających automatyczne zbieranie informacji o sprzęcie (np. komputerach, serwerach, drukarkach) oraz zainstalowanym na nich oprogramowaniu. Dane te będą na bieżąco aktualizowane w centralnej bazie, co umożliwi szybki dostęp do informacji o stanie i konfiguracji każdego urządzenia.
- **Monitorowanie stanu komputerów i urządzeń końcowych** – wdrożenie modułu do bieżącego monitorowania stanu pracy stacji roboczych i serwerów w Urzędzie oraz Jednostkach Gminnych, w tym kontrola wydajności, wykorzystania zasobów (CPU, RAM, dysk) oraz analiza potencjalnych problemów (np. brak miejsca na dysku, wysokie obciążenie procesora).
- **Kontrola bezpieczeństwa** – oprogramowanie umożliwi również monitorowanie stanu zabezpieczeń, w tym zainstalowanego oprogramowania antywirusowego, poziomu aktualizacji systemowych oraz wykrywanie nieautoryzowanych zmian w konfiguracji sprzętu lub oprogramowania.
- **Zarządzanie licencjami oprogramowania** – dzięki zebranych danym system pozwoli na kontrolę ilości zainstalowanych licencji na oprogramowanie oraz ich zgodność z posiadanymi umowami licencyjnymi, ułatwiając zarządzanie zasobami IT w organizacji.

3. Integracja i konfiguracja mechanizmów powiadomień oraz raportowania

W celu efektywnego zarządzania całą infrastrukturą IT wdrożone zostaną mechanizmy powiadamiania i raportowania:

- **Alerty i powiadomienia** – skonfigurowanie systemów monitoringu, aby w przypadku wykrycia incydentów (np. awarii, przeciążenia zasobów, niezgodności sprzętowych) automatycznie powiadamiać administratorów za pomocą e-maili, SMS-ów lub komunikatorów, zgodnie z ustalonymi zasadami eskalacji.
- **Generowanie raportów** – stworzenie szablonów raportów, które pozwolą na regularne przeglądanie stanu infrastruktury (np. dziennych, tygodniowych, miesięcznych raportów) oraz umożliwią analizę długoterminową wydajności sieci, stanu sprzętu i zgodności licencyjnej.

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

4. **Wdrożenie systemu ochrony i filtrowania poczty elektronicznej**

Dodatkowym elementem wdrożenia będzie system ochrony poczty elektronicznej, który zostanie wdrożony jako centralny serwer pocztowy oraz zintegrowany z Active Directory (AD). Serwer pocztowy będzie pełnił kluczową rolę w zabezpieczeniu komunikacji e-mailowej i zapewnieniu jej zgodności z wymaganiami bezpieczeństwa.

- **Konfiguracja serwera pocztowego z ochroną** – zainstalowanie serwera pocztowego na specjalnie przygotowanej maszynie wirtualnej, dostosowanej do wymagań wydajnościowych i bezpieczeństwa. Serwer poczty będzie zintegrowany z Active Directory, co umożliwi automatyczne tworzenie i zarządzanie kontami e-mail na podstawie istniejących kont użytkowników w AD.
- **Ochrona antywirusowa, antyspamowa oraz filtrowanie treści** – wdrożenie mechanizmów ochrony poczty w czasie rzeczywistym, w tym filtrowanie niechcianych wiadomości (spam), blokowanie złośliwych załączników oraz ochronę przed zagrożeniami takimi jak phishing.
- **Wdrożenie sandboxa i kwarantanny** – uruchomienie sandboxa jako środowiska do analizy podejrzanych załączników i wiadomości. Sandbox umożliwi izolowanie niebezpiecznych elementów wiadomości w specjalnej kwarantannie, gdzie będą one dokładnie analizowane przed ewentualnym dostarczeniem do odbiorcy.
- **Wykorzystanie mechanizmów DKIM, SPF i DMARC** – wdrożenie technologii DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework) oraz DMARC (Domain-based Message Authentication, Reporting, and Conformance) w celu uwierzytelniania wiadomości e-mail, zapobiegania spoofingowi oraz ochrony przed innymi atakami na konta e-mail.
- **Przechowywanie danych na maszynie wirtualnej typu NAS** – wszystkie dane związane z pocztą elektroniczną będą przechowywane na odrębnej maszynie wirtualnej pełniącej rolę NAS (Network Attached Storage). Maszyna ta będzie regularnie backupowana w celu zapewnienia bezpieczeństwa i dostępności danych pocztowych.
- **Migracja obecnych kont pocztowych** – wdrożenie obejmie proces migracji istniejących skrzynek pocztowych do nowego systemu ochrony poczty, z zachowaniem wszystkich wiadomości, konfiguracji kont oraz struktury folderów. Cały proces migracji zostanie zaplanowany w taki sposób, aby zminimalizować przestoje w pracy Urzędu i zapewnić nieprzerwane działanie komunikacji e-mailowej.

5. **Konfiguracja rekordów DNS i polityk bezpieczeństwa**

W ramach wdrożenia systemu ochrony poczty zostanie również wykonana kompleksowa konfiguracja wszystkich niezbędnych rekordów DNS, w tym:

- **Konfiguracja rekordów MX** – ustawienie odpowiednich rekordów MX, które będą wskazywać na nowy serwer pocztowy, aby zapewnić prawidłowe dostarczanie wiadomości e-mail.
- **Rekordy SPF, DKIM i DMARC** – konfiguracja rekordów SPF w celu autoryzacji wysyłania wiadomości e-mail przez wyznaczone serwery, DKIM dla podpisywania wiadomości oraz DMARC do zarządzania politykami bezpieczeństwa poczty i monitorowania naruszeń.

6. **Testy funkcjonalne i optymalizacja systemu**

Po wdrożeniu systemu monitoringu, inwentaryzacji sprzętu oraz ochrony poczty, dostawca przeprowadzi testy funkcjonalne:

- **Testy wydajności i stabilności systemów** – weryfikacja poprawności działania serwerów monitoringu oraz systemu ochrony poczty.
- **Testy alertów i powiadomień** – sprawdzenie skuteczności mechanizmów powiadomień, w tym automatycznych alarmów o zagrożeniach bezpieczeństwa.
- **Optymalizacja konfiguracji** – dokonanie niezbędnych korekt ustawień systemów w celu zapewnienia ich optymalnego działania.



Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

7. Szkolenie personelu Zamawiającego

Dostawca przeprowadzi szkolenie dla wyznaczonego personelu Urzędu z zakresu obsługi oraz zarządzania wdrożonymi systemami:

- **Obsługa monitoringu sieciowego i ochrony poczty** – szkolenie z przeglądania stanu sieci, konfiguracji zabezpieczeń poczty, analizy alertów oraz generowania raportów.
- **Zarządzanie inwentaryzacją sprzętu** – instruktaż dotyczący zarządzania danymi o sprzęcie komputerowym, analizowania stanu stacji roboczych oraz monitorowania licencji oprogramowania.

8. Dostarczenie, montaż oraz konfiguracja 3 szt. Telewizorów do wyświetlania w czasie rzeczywistym bieżących parametrów sieci, serwerów oraz aktualnych problemów w miejscu wskazanym przez Zamawiającego.

Wymagania techniczne telewizorów:

- Liczba złączy HDMI: min. 4
- Standard VESA: 200 x 200 mm
- Wi-Fi: z Wi-Fi
- Liczba złączy USB: min. 2
- Złącze cyfrowe audio: Optyczne
- Tuner: DVB-S2, DVB-C, DVB-T2 (HEVC)
- Format HD: 4K Ultra HD
- Liczba głośników: min. 2
- Przekątna ekranu w calach: 50"
- Moc łączna głośników: min. 40 W
- Złącze Ethernet (LAN)
- Bluetooth: z Bluetooth
- DLNA
- Częstotliwość odświeżania: 100 Hz / 120 Hz
- Smart TV
- Kolor ramki: Srebrne
- Typ matrycy: QLED
- Technologia HDR: HDR10+
- HDMI ARC: Tak
- Technologie Dolby: Dolby Atmos

9. Dostarczenie dokumentacji powdrożeniowej

Po zakończeniu wdrożenia zostanie przygotowana pełna dokumentacja zawierająca:

- Szczegółowe opisy konfiguracji systemów.
- Instrukcje użytkownika, procedury dotyczące zarządzania oraz działania w sytuacjach awaryjnych.
- Zalecenia dotyczące dalszej konserwacji, aktualizacji oraz optymalizacji systemów.

10. Wsparcie techniczne po wdrożeniu

Dostawca zapewni wsparcie techniczne w okresie 30 dni po wdrożeniu systemu, obejmujące:

- Pomoc w rozwiązywaniu bieżących problemów związanych z monitoringiem sieciowym, inwentaryzacją sprzętu oraz serwerem pocztowym.
- Doradztwo w zakresie rozszerzania funkcji systemu oraz jego integracji z innymi narzędziami do zarządzania infrastrukturą IT.

W efekcie wdrożenia systemu monitoringu sieciowego oraz inwentaryzacji sprzętu, Zamawiający uzyska kompleksowe narzędzie do nadzoru nad infrastrukturą IT, zapewniając wydajność, bezpieczeństwo i

Załącznik nr 1 do SWZ: Opis przedmiotu zamówienia

zgodność z licencjami. Ponadto, wdrożenie systemu ochrony poczty elektronicznej zwiększy bezpieczeństwo komunikacji e-mail dzięki filtrowaniu zagrożeń, takim jak spam, phishing czy malware, oraz zastosowaniu mechanizmów DKIM, SPF i DMARC. Integracja z Active Directory usprawni zarządzanie kontami, a sandbox i kwarantanna zapewnią dokładną analizę podejrzanych wiadomości. Dzięki temu ochrona poczty będzie bardziej skuteczna, a ryzyko nieuprawnionego dostępu czy wycieku danych zminimalizowane.