

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Część 2 pn.: Dostawa wraz z montażem i konfiguracją serwerów, UPSów, swicha, urządzenia UTM i urządzenia NAS.

SERWER – 2 SZT.

LP	Nazwa komponentu	Wymagane parametry techniczne komputerów
1.	Zastosowanie	Praca w roli serwera domeny Microsoft Active Directory (podstawowy i zapasowy), serwer baz danych
2.	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych.
3.	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
4.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
5.	Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 1,8 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku w teście wydajności: https://www.cpubenchmark.net/ 9000 punktów (kolumna CPU Mark)
6.	RAM	64GB, na płycie głównej powinno znajdować się minimum 8 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
7.	Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
8.	Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 porty 1GbE Base-T
9.	Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane : 1 x dysk min. 960GB SSD SATA Hot-Plug 2 x dyski o pojemności 2TB HDD SATA Hot-Plug Warunek: Wykonawca ujmie w wycenie warunków gwarancji zachowanie dysków twardych na wypadek awarii – dyski pozostają wtedy u Zamawiającego.
10.	Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.

11.	System operacyjny/System wirtualizacji	<p>Zainstalowany Windows Server 2022 Standard</p> <p>Lub system równoważny</p> <p>Licencja bez ograniczeń czasowych. Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer. Instalacja i użytkowanie aplikacji 32- i 64- bitowych na dostarczonym serwerowym systemie operacyjnym w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wieloprocessorowym - obsługa 64 procesorów fizycznych, oraz co najmniej 64 procesorów logicznych (wirtualnych). Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.</p> <p>Praca w roli klienta domeny Microsoft Active Directory. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).</p> <p>Zawarta możliwość uruchomienia roli serwera DNS</p> <p>Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)</p> <p>Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory</p> <p>Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory</p> <p>Zawarta możliwość uruchomienia roli serwera stron WWW</p> <p>Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera</p> <p>W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera - w ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego</p> <p>Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów)</p>
12.	Bezpieczeństwo i oprogramowanie dodatkowe	<p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające</p> <p>- upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</p>

		<p>- możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :</p> <ul style="list-style-type: none"> a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. <p>- wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</p> <p>- możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.</p> <p>- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)</p> <p>- sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)</p> <p>- dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</p> <p>- raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</p>
13.	Wbudowane porty	min. 1 port USB 2.0, oraz min. 3 porty USB 3.0, 2 porty RJ45 GE, port VGA, min. 1 port RS232.
14.	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
15.	Wentylatory	Redundantne
16.	Zasilacze	Redundantne, Hot-Plug maksymalnie 550W.
17.	Bezpieczeństwo	<p>Wbudowany moduł TPM 2.0</p> <p>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</p>

18.	Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. iDRAC9 Basic
19.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE.
20.	Warunki gwarancji	36 m-cy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia na żądanie oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy dostarczyć na żądanie. Możliwość rozszerzenia gwarancji przez producenta do 5 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
21.	Dokumentacja użytkownika	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.

Dodatkowo:

35 licencji: Windows Server 2022/2019 Device CALs lub równoważne

PRZELĄCZNIK SIECIOWY-1 SZT

LP	Nazwa komponentu	Wymagane parametry techniczne przełącznika
1.	Parametry fizyczne platformy	<ul style="list-style-type: none"> Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Minimalny zakres temperatury pracy: 0-40°C.
2.	Interfejsy sieciowe - wymagania minimalne	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ol style="list-style-type: none"> 48 porty GE RJ-45. 2 porty GE SFP+.
3.	Zarządzanie	<ul style="list-style-type: none"> 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.

		<ul style="list-style-type: none"> • 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.
4.	Parametry wydajnościowe	<ul style="list-style-type: none"> • Przepustowość urządzenia - min. 175 Gbps • Tablica adresów MAC o pojemności co najmniej 16k wpisów.
5.	Wymagane funkcje	<ul style="list-style-type: none"> • 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 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.
6.	Gwarancja oraz wsparcie	<ol style="list-style-type: none"> 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
7.	Rozszerzone wsparcie serwisowe	<ol style="list-style-type: none"> 1. System musi być 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 przez okres 36 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. <p>Wykonawca winien przedłożyć poniższe dokumenty na żądanie:</p> <ul style="list-style-type: none"> • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego. • Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań

SERWER NAS RACK 19" – 1 SZT.

Parametr lub warunek	Minimalne wymagania techniczne i funkcjonalne dla macierzy dyskowej
Obudowa	<p>1) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19" z zajętością maks. 2U w tej szafie.</p> <p>2) Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy.</p> <p>3) Macierz powinna dysponować przynajmniej jednym czterordzeniowym procesorem o nominalnej prędkości przynajmniej 1,7 GHz.</p> <p>4) Macierz powinna być wyposażona w co najmniej 4 GB pamięci RAM</p>
Interfejsy	Oferowana macierz musi mieć minimum 2 porty RJ-45 1GbE LAN
Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1, 1+0, 5, 6
Wspierane dyski	<p>Oferowana macierz musi wspierać dyski:</p> <p>1) dyski technologii minimum SATA (3Gb/s), wspierające operacje hot-plug prędkości obrotowej minimum 5400 obrotów na minutę,</p> <p>2) dyski SSD wykonane w technologii hot-plug,</p> <p>3) dyski w formacie 3,5" oraz 2,5".</p> <p>4) przynajmniej 4 dyski bez konieczności rozbudowy o moduły rozszerzające.</p>
Opcje software'owe	<p>1) Oferowana macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 2048 kopii migawkowych.</p> <p>2) Macierz musi umożliwiać dokonywanie migracji danych ze zmianą poziomu RAID.</p> <p>3) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server 2008/2012, SuSE Linux, RedHat Linux, SUN Solaris, VMWare 5.x, Citrix XEN Server.</p>
Konfiguracja, zarządzanie	<p>1) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW.</p> <p>2) Musi być możliwe zdalne zarządzanie macierzą bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.</p>
	Gwarancja producenta min. 24 miesiące realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. W przypadku awarii dyski twarde pozostają własnością Zamawiającego

DYSK NAS 4TB SATA – 2 SZT.

Parametr lub warunek	Minimalne wymagania
Typ i przeznaczenie	Dysk twardy – wewnętrzny, kompatybilny z serwerem NAS
Pojemność	4 TB
Rodzaj obudowy	3,5"
Interfejs	SATA 6Gb/s
Wielkość bufora	256 MB
Cechy	Obsługa "podłączania na gorąco", dostępność 24x7, czujnik wibracji obrotowych
Szybkość transmisji urządzenia	600 MBps (zewnętrzna)
Szybkość wewnętrzna danych	232 MBps
Prędkość obrotowa	7200 obr/min
Praca 24x7	Tak
Interfejsy	1 x SATA 6 Gb/s
Gwarancja i wsparcie techniczne	3-letnia gwarancja producenta

ZASILACZ AWARYJNY UPS DO SERWERÓW – 2 SZT.

Parametr lub warunek	Minimalne wymagania
Zastosowanie	Zasilacz awaryjny do serwerów. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta.
Moc	Minimum 3000VA 2700W
Typ	online
Zabezpieczenia	Zabezpieczenie przed przeładowaniem Zabezpieczenie przeciwprzepięciowe
Komunikacja	USB RJ11
Napięcie wejściowe	110-290V
Napięcie wyjściowe	200/208/220/230/240V AC
Częstotliwość wejściowa	45Hz-65Hz (automatyczne wykrywanie)
Częstotliwość wyjściowa	50Hz/60Hz
Baterie	Min. 6 x 12V/9Ah, żywotność akumulatorów min. 5lat
Gniazda	Min. 6x IEC320 C13-10A (podzielone na dwa segmenty z możliwością przydzielenia odrębnych ustawień)
Gwarancja	Min. 24 miesiące (min. 12 miesięcy na baterię)
Inne	Wyświetlacz LCD

UTM SPRZĘTOWY – 1 SZT.

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

LP	Parametr lub warunek	Minimalne wymagania
1.	Typ	Firewall sprzętowy
2.	Charakterystyka urządzenia	<p>Wymagania Ogólne</p> <p>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.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. <p>Redundancja, monitoring i wykrywanie awarii</p> <ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery 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.

		<p>4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</p> <p>Interfejsy, Dysk, Zasilanie:</p> <ol style="list-style-type: none"> System realizujący funkcję Firewall musi dysponować minimum: <ul style="list-style-type: none"> 10 portami Gigabit Ethernet RJ-45. 2 gniazdami SFP 1 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB. System musi być wyposażony w zasilanie AC. <p>Parametry wydajnościowe:</p> <ol style="list-style-type: none"> W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. <p>Funkcje Systemu Bezpieczeństwa:</p> <p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping). Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
--	--	--

		<p>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.</p> <p>11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</p> <p>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</p> <p>Polityki, Firewall</p> <p>13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.</p> <p>17. 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.</p> <ul style="list-style-type: none"> • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. <p>Połączenia VPN</p> <p>1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> • 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.
--	--	---

		<p>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> • 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. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. <p>Routing i obsługa łączności WAN</p> <ol style="list-style-type: none"> 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. <p>Funkcje SD-WAN</p> <ol style="list-style-type: none"> 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączności WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. <p>Zarządzanie pasmem</p> <ol style="list-style-type: none"> 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. <p>Ochrona przed malware</p> <ol style="list-style-type: none"> 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 licencją upoważniającą 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.
--	--	---

		<p>6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>Ochrona przed atakami</p> <ol style="list-style-type: none"> 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. 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. <p>Kontrola aplikacji</p> <ol style="list-style-type: none"> 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. <p>Kontrola WWW</p> <ol style="list-style-type: none"> 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.
--	--	--

		<p>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p> <p>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p> <p>Uwierzytelnianie użytkowników w ramach sesji</p> <ol style="list-style-type: none"> System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. <p>Zarządzanie</p> <ol style="list-style-type: none"> Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
--	--	---

		<p>Logowanie</p> <ol style="list-style-type: none"> 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. <p>Certyfikaty</p> <p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:</p> <ul style="list-style-type: none"> • ICSA lub EAL4 dla funkcji Firewall. <p>Serwisy i licencje</p> <p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:</p> <ol style="list-style-type: none"> a) 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 12 miesięcy. b) Licencja na usługę realizowaną w chmurze na okres 12 miesięcy umożliwiającą logowanie i raportowanie z czasem retencji logów minimum 1 rok. <p>Gwarancja oraz wsparcie</p> <ol style="list-style-type: none"> 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. <p>Rozszerzone wsparcie serwisowe AHB/SOS</p> <ol style="list-style-type: none"> a) System musi być 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 przez okres 12 miesięcy. b) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
--	--	--

		c) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5
--	--	---

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania

Wdrożenie domeny AD

- Instalacja oraz uruchomienie systemu operacyjnego na serwerze wraz z uruchomieniem roli domenowej
- Utworzenie domeny.
- Utworzenie schematu organizacyjnego.
- Utworzenie kont użytkowników
- Utworzenie folderów udostępnionych.
- Nadanie uprawnień do folderów po wcześniejszym uzgodnieniu macierzy uprawnień.
- Opracowanie oraz konfiguracja polityki zabezpieczeń.
- Konfiguracja kopii bezpieczeństwa.
- Instalacja drukarek – dostosowanie obecnie użytkowanych drukarek do potrzeb współpracy ze środowiskiem domenowym
- Instalacja WSUS.
- Podłączenie komputerów do utworzonej domeny – proces wykonywany etapowo (podłączenie nowych urządzeń oraz zmiana konfiguracji obecnie użytkowanych celem dołączenia do domeny)
- Migracja danych.
- Wdrożenie WSUS na komputerach.
- Instalacja odpowiednich drukarek na komputerach.
- Dokumentowanie wykonanych prac.

Instalacja oprogramowania bazodanowego

- Wykonanie instalacji oprogramowania bazodanowego wraz z wykonaniem niezbędnej konfiguracji oraz przeniesieniem dotychczas funkcjonujących baz danych oprogramowania dziedzicznego

Audyt sieci komputerowej

- Wykonanie audytu sieci komputerowej – sprawdzenie poprawności funkcjonowania sieci oraz konfiguracji urządzeń sieciowych, poprawa/ naprawa ewentualnych występujących problemów konfiguracyjnych występujących w sprzęcie.



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- Uruchomienie oraz konfiguracja UTM zgodnie z zapotrzebowaniem zamawiającego oraz obecnie funkcjonującą strukturą

Instalacja oraz konfiguracja sprzętu

- Instalacja oraz konfiguracja zakupionych urządzeń
- Migracja danych ze starych maszyn na nowy serwer.

Instruktaż

- Przeprowadzenie szkolenia dla służb informatycznych w zakresie obsługi oraz konfiguracji urządzeń a także wdrożonych rozwiązań

Wsparcie techniczne

- Wsparcie techniczne oraz nadzór autorski przez okres 12 miesięcy

Usługi

- Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska.
- Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.
- W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową.
- Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:
 - Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.
 - Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:
 - koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych elementów sprzętowych.
 - schematy połączeń
 - mechanizmy działania głównych elementów sprzętowych:
 - sieć LAN
 - system wirtualizacyjny
 - system backupu i archiwizacji danych
 - system serwerowy



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- Firewall/UTM
- testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
- sposób odbioru uzgodniony z Zamawiającym
- Listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
- opis przypadków, w których projekt dopuszcza niedziałanie systemu
- realizacja wdrożenia nastąpi według Planu Wdrożenia, po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą
- Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia

Montaż i fizyczne uruchomienie systemu

- Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:
 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
 2. Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
 3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
 4. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
 5. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
 6. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
 7. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
 8. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
 9. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem:
 - Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
 - Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
- Połączenia muszą wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.

Konfiguracja elementów bezpieczeństwa sieciowego.

Urządzenie firewall/modernizacja konfiguracji urządzenia UTM w zakresie.

1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)
4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
5. Konfiguracja dostarczonych systemów Firewall:
 - a. Konfiguracja podstawowych parametrów
 - b. Konfiguracja translacji adresów NAT
 - c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.
 - d. Konfiguracja inspekcji określonych protokołów sieciowych;
 - e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
 - f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
 - g. Testowanie działania bramy
6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
 - a. Konfiguracja podstawowych parametrów
 - b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;
 - c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
 - d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



e. Testowanie działania ochrony IPS

7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.

a. Przypisanie adresu IP do zarządzania.

b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3

c. Definicja reguł filtrowania/blokowania

d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.

8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.

9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.

10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.

11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC

12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekazuje Zamawiający) dla każdej z poniższych funkcjonalności:

a. kontrola dostępu - zaporę ogniową klasy Stateful Inspection

b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar

c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.

e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)

f. kontrola pasma oraz ruchu [QoS, Traffic shaping]

g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P

h. Ochrona przed wyciekiem poufnej informacji (DLP)

i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)

j. Inspekcja ruchu SSL

k. Ochrony przed atakami na stacje klienckie i. Kontrola pasma



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.

14. Konfiguracja logowania i raportowania.

Serwer NAS - Backup

Urządzenie NAS należy dołączyć do infrastruktury Zamawiającego celem stworzenia miejsca na przechowywanie danych backupu.

Migracja danych

Dotyczy przeniesienia obecnie wykorzystywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedziczne) muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzicznych.

Instalacja systemu operacyjnego serwerów

Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.

Uruchomienie usługi katalogowej oraz niezbędnych komponentów

Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.

Dołączenie stacji roboczych do domeny

Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół.

Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.

Opracowanie dokumentacji powykonawczej

Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu.

Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.

Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).

Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.

Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.

Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.

W ramach przedmiotu zamówienia wymagane jest przeprowadzenie szkolenia dla wyznaczonych pracowników Zamawiającego w zakresie:

- Zarządzania systemami serwerowymi i wirtualizacją.
- Archiwizacji danych oraz wykonywania kopii zapasowych.
- Polityki autentykacji i autoryzacji użytkowników sieci, usług katalogowych.
- Podstawowej konfiguracji systemu bezpieczeństwa UTM.
- Wykonywania kopii bezpieczeństwa plików konfiguracyjnych itp.