**Wymagania szczegółowe, minimalne dla sprzętu ujętego w ramach przedmiotu zamówienia dla Części III postępowania w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina”**

## Dostawa sprzętu:

# Serwer usług AD : szt.1

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory 8-rdzeniowe, klasy x86, dedykowane do pracy z zaoferowanym serwerem, taktowane zegarem min. 2.8 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 33 000 punktów w teście PassMark dla konfiguracji Dual CPU- CPU Mark dostępnym na stronie internetowej: https://www.cpubenchmark.net/multi\_cpu.htmlz dnia 01.06.2023 (wyniki załączone do dokumentów zapytania). |
| **Pamięć operacyjna** | 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing |
| **Gniazda PCI** | Minimum jeden slot PCIe x16 generacji 4 oraz dwa sloty PCIe x8 |
| **Interfejsy sieciowe/FC** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Wolny wbudowany port w standardzie OCP 3.0. (wolny wbudowany port nie może zmniejszać ilość wbudowanych portów Pcie ) |
| **Napęd optyczny** | Wbudowany lub zewnętrzny DVD-RW |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSDZainstalowane 5 dyski HDD SAS o pojemności min. 600 GB, 12Gb/s, 10 tys. obr./min, Hot-PlugMożliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, |
| **Wideo** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920×1080 |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W każdy. |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* 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
 |
| **System operacyjny** | Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.Graficzny interfejs użytkownika.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.c) Zdalna dystrybucja oprogramowania na stacje robocze.d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.e) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:- Dystrybucję certyfikatów poprzez http,- Konsolidację CA dla wielu lasów domeny,- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.f) Szyfrowanie plików i folderów.g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.i) Serwis udostępniania stron WWW.j) Wsparcie dla protokołu IP w wersji 6 (IPv6).k) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF;Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.**System musi posiadać licencje dostępowe dla minimum 30 użytkowników.** Wymagana najnowsza dostępna wersja na dzień publikacji ogłoszenia o zamówieniu. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);- szyfrowane SSL- wsparcie dla IPv6;- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;- integracja z Active Directory;- wsparcie dla dynamic DNS;- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera- możliwość obsługi przez sześciu użytkowników jednocześnie;- możliwość podmontowania zdalnych wirtualnych napędów;- wirtualną konsolę z dostępem do myszy, klawiatury;- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta• Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH• Możliwość oskryptowywania procesu wykrywania urządzeń• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram• Szczegółowy opis wykrytych systemów oraz ich komponentów• Możliwość eksportu raportu do CSV, HTML, XLS• Grupowanie urządzeń w oparciu o kryteria użytkownika• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach• Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń• 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• Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu• Kreator umożliwiający dostosowanie akcji dla wybranych alertów• Możliwość importu plików MIB• Przesyłanie alertów „as-is” do innych konsol firm trzecich• Możliwość definiowania ról administratorów• Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)• Możliwość instalacji sterowników i 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 gwarancji, adresy IP kart sieciowych.• Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej). |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub równoważną oraz ISO-14001 lub równoważną.Serwer musi posiadać deklarację CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2016, Windows Server 2019.**Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 1 ustawy prawo zamówień publicznych.** |
| **Warunki gwarancji** | Wg SWZ |
| **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. |

# Zakup serwerów NAS: 2szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Procesor** | Jeden 4-rdzeniowy/8-wątkowy AMD Ryzen V1500B lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4500 pkt.W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/mid\_range\_cpus.html |
| **Pamięć** | Minimum 4GB pamięci DDR4 z możliwością rozbudowy do 32GB |
| **Obudowa** | Rack 2U o wymiarach 88 × 482 x 306,6 mmW zestawie szyny wysuwane do instalacji w szafie RACK |
| **Wskaźniki LED** | Power on, Status, HDD1 -8 |
| **Obsługiwane dyski twarde** | 8 dysków o maksymalnej pojemności 18TB każdy z możliwością podłączenia zewnętrznej półki, która rozszerza pojemność serwera o kolejne 4 dyski |
| **Zainstalowane dyski twarde** | Cztery dyski twarde o pojemności 4TB każdy znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS spełniające wymagania - pojemność: 4TB- interfejs: SATA 6Gb/s- obroty na minutę: min 5400- pamięć podręczna: 256 MB- format: 3,5” |
| **Interfejsy komunikacyjne** | - 4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation- dodatkowa karta producenta urządzenia 2 x 10 SFP+- 2 x USB 3.2- 1 x eSATA |
| **System plików** | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+ |
| **Obsługa RAID** | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10 |
| **Protokoły** | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| **Klaster HA** | Możliwość połączeniu dwóch identycznych urządzeń w jeden klaster wysokiej dostępności (high-availability) |
| **Usługi dodatkowe** | Pakiet darmowego oprogramowania dostarczony przez producenta urządzeniaz możliwością tworzenia kopii bezpieczeństwa stacji roboczych z systemem Windows 10, 11, serwerów fizycznych Windows 2012 R2, 2016, 2019, 2022, serwerów fizycznych Linux: Ubuntu 20.04, 22.04, środowisk wirtualizacji Vmware vSphere oraz Microsoft Hyper-V oraz serwerów plików SMB v2, v3 oraz RSYNC 3.0. |
| **Gwarancja** | Wg SWZ |

# Dyski SAS: 3 szt.

|  |  |
| --- | --- |
| **Dyski twarde** | Nowe dyski min. 1,2TB SAS 12Gb/s. 10K RPM. 2,5’’ hotplug dla serwera które posiada zamawiający:Dell PowerEdge R440, Service Tag: DNVBHZ2.Zaoferowane dyski muszą być dopuszczone do montażu w serwerze przed producenta serwera. |

# Serwer dziedzinowy – 1 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania jednego procesora.  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| **Procesor** | Zainstalowany jeden procesor ośmiordzeniowy dedykowany do pracy z zaoferowanym serwerem, taktowany zegarem min 2.8 GHz (częstotliwość bazowa) umożliwiający osiągnięcie wyniku minimum 22 750 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/high\_end\_cpus.html z dnia 01.06.2023 (wynika załączone do dokumentów zapytania). |
| **Pamięć operacyjna** | 32 GB pamięci RAM ECC UDIMM w kościach 32GB o częstotliwości pracy 3200MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinny znajdować się minimum 4 sloty przeznaczone dla pamięci. |
| **Interfejsy sieciowe/FC** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |
| **Kontroler dysków** | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10. |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD, NL SASZainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb/s, Hot-Plug o parametrze DWPD wynoszącym min. 1.Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Wbudowane porty** | min. 4 porty USB w tym min. 1 USB 3.01 port VGA 1 port RS232 |
| **Wideo** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920×1080 |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
 |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* szyfrowane SSL;
* wsparcie dla IPv6;
* wsparcie dla dynamic DNS;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* obsługa Public Key Authentication (PKA) przez SSH;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 |
| **System operacyjny** | Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym.Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.Graficzny interfejs użytkownika.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.b) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.**System musi posiadać licencje dostępowe dla minimum 15 użytkowników.** Wymagana najnowsza dostępna wersja na dzień publikacji ogłoszenia o zamówieniu. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub równoważną oraz ISO-14001 lub równoważną.Serwer musi posiadać deklarację CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2016, Windows Server 2019.**Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 1 ustawy prawo zamówień publicznych.** |
| **Warunki gwarancji** | Wg SWZ |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim . Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# FireWall- szt.1

Wymagane jest dostarczenie urządzenia zabezpieczającego sieć spełniających minimalne parametry funkcjonalne opisane poniżej:

|  |  |  |
| --- | --- | --- |
| **Parametr**  | **Charakterystyka (minimalne wymagania)** | **Oferowany parametr** |
| Elementy systemu bezpieczeństwa | * Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most ) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
* System pełniący funkcję zapory musi mieć co najmniej 9 interfejsów Ethernet 10/100/1000, każdy z nich może być portem interfejsu WAN lub LAN
* Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
* Musi posiadać 1x USB przodu urządzenia
* System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
 |  |
| Funkcjonalności | * Kontrola dostępu — zapora sieciowa Stateful Inspection
* Ochrona przed wirusami - antywirus
* Poufność danych - IPSec VPN i SSL VPN
* Kontrola witryn sieci Web — filtr URL
* Kontrola przepustowości i ruchu QoS i kształtowanie ruchu z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
* Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
 |  |
| Wydajność | * Analiza ruchu szyfrowanego protokołem SSL/TLS w tym wsparcie dla TLS 1.3
* Wydajność Firewall nie mniej niż 4.7 Gbps
* Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji nie mniej niż 450 Mbps
* Wydajność ochrony przed atakami (IPS) minimum 1.2 Gbps
* Wydajność IPSec VPN, nie mniej niż 850 Mbps
* W zakresie Firewall, obsługa nie mniej niż 200 000 jednoczesnych połączeń i 27 000 nowych połączeń na sekundę.
* Możliwość stworzenia minimum 512 IPSec Tunnel
* Wydajność antywirusa nie mniejsza niż 850Mbps
* Ilość sesji jednocznesnych nie mniejsza niż 400 000
* Ilość nowych sesji nie mniejsza niż 25 000
 |  |
| Funkcjonalności VPN | * Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
* Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
* Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
* Praca w topologiach Hub and Spoke i Mesh
* Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,
* Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
* Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
* Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)
* Obsługa PnPVPN (Plug and Play VPN)
 |  |
| Routing | * Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
* Obsługa Policy Based Routing
* Funkcjonalność Virtual Wire
 |  |
| Translacja adresów NAT | * Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
* Obsługa NAT46, NAT64, DNS64
* Wsparcie dla Full Cone NAT, STUN
 |  |
| Polityka bezpieczeństwa systemu | * Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
* Możliwość budowania min. 8000 polityk
* Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
* Musi być w stanie skonfigurować agregowane polityki
* Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
* Musi posiadać możliwość konfiguracji mini polityk
 |  |
| Wydzielenie stref bezpieczeństwa | * Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
* Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
* Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
 |  |
| Ochrona antywirusowa | * Silnik antywirusowy musi być oparty na przepływie tzw. flow-based
* Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB
* Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
* Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
 |  |
| Równoważenie obciążenia | * Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
* Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin
* Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
 |  |
| Ochrona IPS | * Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
* Baza danych wykrytych ataków musi zawierać co najmniej 2000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
* Funkcjonalność zapobiegania atakom SQL injection, XSS injection
* Możliwość budowania własnych niestandardowych reguł IPS
 |  |
| Kontrola aplikacji | * Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP.
* Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
 |  |
| Filtr adresów URL | * Baza filtrów URL pogrupowana w co najmniej 75 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
* Możliwość zdefiniowania własnej bazy kategorii www.
* Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
* Kategoria takie jak hazard, malware, spam, botnety
* Obsługa Safe Search
* Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
* Dostosowanie strony ostrzeżenia
 |  |
| Ochrona danych | * Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
* Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP
* Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
* Filtrowanie plików przesyłanych przez SMB
 |  |
| Uwierzytelnianie użytkownika | * System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:
	+ Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
	+ Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
	+ Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych
	+ Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
* Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
* Wsparcie usług terminalowych
* Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
* Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
 |  |
| Raportowanie i przeglądanie logów | * Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
* W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
	+ Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego
	+ Generowanie co najmniej 10 rodzajów raportów
 |  |
| System logowania | * Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.
 |  |
| Certyfikaty | Rozwiązanie musi:* posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
* być pozycjonowanym w raporcie Gartnera przez ostatnie 7 lat
 |  |
| Zarządzanie | * Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
* Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
* Musi mieć możliwość konfiguracji z użyciem NETCONF
 |  |
| Gwarancja/wsparcie | Wg SWZ |  |