**Znak sprawy: OR.272.2.2024 ZAŁĄCZNIK NR 12 do SWZ**

***Parametry minimalne sprzętu i oprogramowania oraz zakres prac do wykonania***

Spis treści

[ETAP I – minimalne parametry sprzętu i oprogramowania 3](#_Toc177983555)

[1 Serwer NAS 3](#_Toc177983556)

[2 Dostawa i wdrożenie rozwiązania klasy NAC 5](#_Toc177983557)

[3 Odnowienie wsparcia serwisowego dla posiadanego UTM na 1rok 12](#_Toc177983558)

[4 Wdrożenie narzędzi wspomagających zarządzanie ryzykami i uprawnieniami 12](#_Toc177983559)

[5 Odnowienie licencji posiadanego oprogramowania antywirusowego ESET 14](#_Toc177983560)

[6 Przełącznik sieciowy klasy enterprise 15](#_Toc177983561)

[7 Urządzenie brzegowe UTM typ 1 17](#_Toc177983562)

[8 Urządzenie brzegowe UTM typ 2 22](#_Toc177983563)

[9 Urządzenie NAS wraz z oprogramowaniem do backup-u 26](#_Toc177983564)

[10 UPS Stanowiskowy 29](#_Toc177983565)

[11 Serwer aplikacyjny tower z serwerowym system operacyjnym oraz licencjami dostępowymi 30](#_Toc177983566)

[12 Punkt dostępowy dla sieci WiFi 35](#_Toc177983567)

[ETAP II – wdrożenie dostarczonych rozwiązań i usługa segmentacji sieci 37](#_Toc177983568)

[1 Segmentacja sieci 37](#_Toc177983569)

[1.1 Segmentacja sieci 37](#_Toc177983570)

[1.2 Wdrożenie systemu NAC w ramach pkt.2 OPZ 37](#_Toc177983571)

# ETAP I – minimalne parametry sprzętu i oprogramowania

# Serwer NAS

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Procesor | Jeden 8-rdzeniowy/16-wątkowy procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 10000 pkt. |
| Obudowa | Rack 2U  W zestawie szyny wysuwane do instalacji w szafie RACK |
| Pamięć RAM | 32GB DDR4 ECC RAM  Możliwością rekonfiguracji do 64GB |
| Ilość obsługiwanych dysków | 12 dysków 3,5”/2,5” SATAIII/II;  Możliwość rozszerzenia do 36 dysków poprzez dołożenie dodatkowych półek rozszerzających |
| Ilość zainstalowanych dysków | Min. 12 dysków w formacie 3,5” znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 8TB |
| Interfejsy sieciowe | 4x Gigabit (10/100/1000)  2x 10GbE SFP+ obsadzone wkładkami 10GB MM SR |
| Porty | 2 x USB3.2, 2 x Infiniband do podłączania dodatkowych półek dyskowych |
| Gniazda PCIe | 2 gniazda PCIe Gen3 x8 (minimum 1 gniazdo wolne) |
| Wskaźniki LED | Status, LAN, HDD1 -12 |
| Obsługa RAID | Basic, JBOD, RAID F1,0,1,5,6,10 + Hot Spare 1,5,6,10. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów |
| Licencja na Kamery IP | W zestawie licencja na 2 kamery ( z możliwością rozszerzenia do 90.  Funkcja CMS. |
| Obsługa SSD Cache | Wymagane wsparcie dla SSD Cache |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP, |
| Usługi | Wsparcie dla High Availability  Serwer VPN  Serwer pocztowy dla kilku domen  Stacja monitoringu  Windows ACL  Integracja z Windows ADS  Firewall z kontrolą ruchu  Serwer WWW  Serwer plików  Manager plików przez WWW  Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie  Antyvirus  Klient VPN  Usługa DDNS  Oprogramowanie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware |
| Oprogramowanie do kopii zapasowej | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu:   1. kopie zapasowe klastrów wirtualizacyjnych failover opartych o Hyper-V 2. kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, 3. kopia zapasowa środowisk MacOS 4. kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) 5. kopia zapasowa serwerów fizycznych (Windows, Linux) 6. obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, 7. obsługa wielu wersji i retencji, 8. możliwość wyzwalania kopii zapasowej według harmonogramu, 9. obsługa klastra przełączania awaryjnego Microsoft Hyper-V, 10. automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, 11. centralne zarządzanie, 12. konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, 13. portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), 14. delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, 15. kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace 16. zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera. |
| Oprogramowanie | 1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 2. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. 3. Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. 4. Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync 5. Obsługa minimum 1000 migawek na folder współdzielony i minimum 65000 migawek na cały system 6. Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 60jednoczesnych połączeń |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, |
| Język GUI | Polski |
| Waga | Do 15 KG |
| System plików | Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btfrs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT |
| Liczba wolumenów | 256 |
| Liczba iSCSI Targetów | 256 |
| Liczba iSCSI LUN | Do 512 |
| Liczba kont użytkowników | 16000 |
| Liczba grup | 512 |
| Liczba folderów udostępnionych | 512 |
| Ilość jednoczesnych połączeń | 2000 dla CIFS, FTP, AFP |
| Zasilanie | Dwa redundantne zasilacze HotSwap o mocy min. 550W |
| Gwarancja i serwis | Min. 12 miesięcy gwarancji realizowanej w trybie NBD Onsite przez producenta lub Autoryzowanego Partnera Serwisowego producenta; dyski objęte wsparciem pozostawienia dysku w przypadku wystąpienia awarii.  **Wraz z dostawą sprzętu Wykonawca dostarczy dokument potwierdzający warunki gwarancji wystawione przez producenta urządzenia lub autoryzowanego partnera serwisowego potwierdzający zaoferowane warunki gwarancji.**  [długość gwarancji – pozacenowe kryterium oceny ofert] |

# Dostawa i wdrożenie rozwiązania klasy NAC

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Podstawowe funkcjonalności systemu NAC** | 1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. 2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor) 3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. 4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. 5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. 6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. 7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 2 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. 8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. 9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. 10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:     * VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x     * Maszyny fizyczne - serwery wspierane przez producenta. 11. System musi posiadać funkcjonalność serwerów:     * serwera RADIUS dla infrastruktury sieciowej,     * serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,     * serwera SYSLOG,     * serwera TACACS+,     * serwera Monitoringu,     * serwera DHCP,     * serwera polityk uwierzytelniania i kontroli dostępu 802.1X,     * serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. 12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. 13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. 14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. 15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. 16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. 17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. 18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. 19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. 20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. 21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). 22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. 23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). 24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. 25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. 26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. 27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. 28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. 29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu. 30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. 31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. 32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. 33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. 34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. 35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. 36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). 37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn. 38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. 39. System musi posiadać funkcję personalizacji strony gościnnej. 40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. 41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor. 42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. 43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory. 44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. 45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. 46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. 47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). 48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. 49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. 50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. 51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. 52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. 53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. 54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. 55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. 56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. 57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). 58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. 59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:     * Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności     * Czy włączony jest firewall     * Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur     * Czy jest włączone szyfrowanie dysku systemowego     * Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory     * Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora     * Czy w systemie są uruchomione procesy wskazane przez administratora     * Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności     * Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:       + Wartości klucza rejestru       + Typu wartości: Number, String, Version 60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. 61. System musi współpracować z serwerem tokenów. 62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:     * Microsoft Windows     * Mac OS     * iOS     * Android 63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). 64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory. |
| **Mechanizmy uwierzytelniania** | 1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. 2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:    * MAC,    * PAP/ASCII,    * CHAP,    * SNMP,    * 802.1X. 3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. 4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. 5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. 6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). 7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:    * Tożsamość/Urządzenie końcowe,    * Grupa tożsamości/urządzeń końcowych,    * Parametry urządzeń końcowych, min: system operacyjny, wersja,    * Atrybuty Active Directory,    * Jednostka organizacyjna tożsamości/urządzeń końcowych,    * Urządzenia sieciowe sieci przewodowej, bezprzewodowej,    * Grupy urządzeń sieciowych,    * Porty urządzeń sieciowych,    * Grupy portów urządzeń sieciowych,    * Jednostka organizacyjna portów,    * Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),    * Data, czas ważności polityki,    * Wewnętrzny Captive Portal,    * Metoda autoryzacji. 8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal. 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. |
| **Obsługa serwerów certyfikatów CA** | 1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. 2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:    * możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.    * możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.    * Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).    * usługę OCSP (Online Certificate Status Protocol). |
| **Obsługa serwerów DHCP** | 1. System musi posiadać funkcję zintegrowanego serwera DHCP. 2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. 3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:    * Uruchamianie usługi dla wybranych podsieci,    * Przypisanie ustalonego adresu IP dla adresu MAC.    * Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,    * Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,    * Możliwość określania braku dostępu dla wybranych adresów MAC,    * Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,    * Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,    * Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,    * Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,    * Dokonywanie zmian bez konieczności wyłączania usług. |
| **Obsługa serwerów TACACS+** | System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:   1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. 2. System musi umożliwiać tworzenia haseł administratorom. 3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów 4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. 5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. 6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory. 7. System musi wspierać logowanie administratorów za pomocą tokenów OTP. 8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji. |
| **Raportowanie i monitoring** | System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:   1. Monitoring autoryzacji. 2. Monitoring dla zdarzeń systemowych. 3. Monitoring dla zdarzeń DHCP. 4. Monitoring dla tożsamości. 5. Monitoring dla urządzeń końcowych. 6. Monitoring dla urządzeń sieciowych. 7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. 8. Raport ze zdarzeń logowania z informacją o nadam adresie IP. 9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. 10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. 11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. 12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. 13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. 14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. 15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. 16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. 17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. 18. Raport zdarzeń Microsoft Active Directory, minimum:     * Logowania, wylogowania z system w tym błędne logowania     * Logowania do sieci 802.1X |
| **Alarmy** | 1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:    * wiadomości e-mail,    * Syslog,    * notyfikacji systemowych. 2. Alarmy mogą być generowane w sytuacjach, min:    * Ilości obsługiwanych transakcji RADIUS,    * Opóźnienie obsługi transkacji RADIUS,    * Statusu krytycznego modułów. 3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:    * badanie łączności IP za pomocą ping, traceroute,    * tcpdump protokołów RADIUS, TACACS+,    * wyszukiwanie zdarzeń RADIUS z uwzględnieniem:      + nazwy użytkownika,      + adresu MAC,      + statusu uwierzytelnienia (udana lub nieudana),      + powodu, jeżeli uwierzytelnienie nieudane,      + zakresu czasowego, co do dnia, godziny i minuty,    * wykonanie zdalnego polecenia na urządzeniu sieciowym. |
| **Licencja wsparcia technicznego producenta oprogramowania** | Wykonawca dostarczy wraz dożywotnią licencją systemu NAC, 12-miesięczną licencje na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:   * Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC * Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. * Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. * Dostęp do dokumentacji i instrukcji na stronie internetowej. * Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.   [długość wsparcia: pozacenowe kryterium oceny ofert] |

# Odnowienie wsparcia serwisowego dla posiadanego UTM na 1rok

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Procesor | 1. Zamawiający posiada obecnie dwa urządzenia typu firewall tj. Fortigate FG-100E i Fortigate FG-100F. 2. Urządzenie pierwsze FG-100E o nr seryjnym FG100ETK18036401 i licencją do 12 czerwca 2025 r. jest użytkowane i zainstalowane w Starostwie Powiatowym. Zamawiający oczekuje odnowienia posiadanej licencji Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Email Filtering, Cloud Sandbox, AntiVirus) wraz z serwisami 8x5 FortiCare 3. Urządzenie drugie FG-100F o nr seryjnym: FG100FTK20015632 i licencją do 18 grudnia (poprawiłem literówkę) 2024 r. jest użytkowane i zainstalowane w Powiatowym Urzędzie Pracy.   Zamawiający oczekuje odnowienia posiadanej licencji Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Email Filtering, Cloud Sandbox, AntiVirus) wraz z serwisami 24x7 FortiCare   1. W ramach dostawy należy przedłużyć posiadane wsparcie aktualizacyjne i techniczne producenta o kolejny rok od końca obecnej licencji dla w/w urządzeń |

# Wdrożenie narzędzi wspomagających zarządzanie ryzykami i uprawnieniami

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Funkcjonalności w obszarze organizacyjnym | |
| 1. | 1. Odwzorowanie schematu organizacyjnego Zamawiającego 2. Odwzorowanie procesów zachodzących w Starostwie 3. Korelację procesów z komórkami organizacyjnymi Starostwa 4. Korelację procesów ze zidentyfikowanymi ryzykami 5. Korelację ryzyk z grupami ryzyka 6. Wskazanie krytyczności procesu 7. Wskazanie typów danych osobowych przetwarzanych w procesie 8. Wskazanie szczególnych kategorii danych osobowych 9. Możliwość przypisania regulacji do ryzyk 10. Możliwość kontroli zaleceń audytowych 11. Możliwość kontroli terminów wdrożeń zaleceń audytowych 12. Możliwość kontroli ryzyk wymagających okresowych przeglądów |
| Obszary identyfikacji ryzyka | |
| 2. | 1. Środowisko teleinformatyczne 2. Kontrola dostawców usług informatycznych 3. Zarządzanie kadrami 4. Zarządzanie bezpieczeństwem fizycznym 5. Produkty i usługi, w tym usługi chmurowe 6. Inne w zakresie oceny prawdopodobieństwa, skutków finansowych, wizerunkowych, poufności, dostępności i integralności oraz kontroli mechanizmów zabezpieczających |
| Zakres oceny ryzyka | |
| 3. | 1. Prawdopodobieństwo wystąpienia 2. Skutki finansowe 3. Skutki wizerunkowe 4. Utrata poufności 5. Utrata dostępności 6. Utrata integralności 7. Analiza dodatkowych atrybutów definiowanych przez Zamawiającego |
| Ocena DPIA (Data Protection Impact Assessment) | |
| 4. | 1. Przypisanie negatywnych skutków do ryzyka 2. Ocena skutków dla ochrony danych 3. Dedykowany raport DPIA. 4. Szczegółowa analiza DPIA dla procesu |
| Plan postępowania z ryzykiem | |
| 5. | 1. Przypisanie priorytetu postępowania do planu 2. Przypisanie osoby odpowiedzialnej 3. Określenie kosztów 4. Wskazanie terminu wprowadzenia planu 5. Monitorowania realizacji przyjętego planu postępowania |
| Kluczowe Wskaźniki Ryzyka (Key Risc Indicators – KRI) | |
| 6. | 1. Monitorowania ryzyka za pomocą KRI 2. Mechanizm rejestracji pomiarów 3. Alarmowanie o wskaźnikach wymagających pomiaru 4. Raportowanie wyników |
| Rejestr incydentów | |
| 7. | 1. Możliwość rejestracji incydentów 2. Przeprowadzanie szczegółowych analiz 3. Monitorowanie wpływu na inne procesy 4. Szacowanie potencjalnych strat i rejestrowanie strat rzeczywistych 5. Kontrola czasu zgłoszenia naruszenia danych osobowych do UODO 6. Dodawanie załączników (np. raportów notatek, zrzutów ekranowych) |
| Nadzór nad zarządzaniem uprawnieniami | |
| 8. | 1. Możliwość identyfikacji ryzyka związanego z dostępem do systemu informatycznego nadanym podmiotowi zewnętrznemu 2. Nadzór nad ryzykiem pozostawienia uprawnień do systemów po zakończeniu umowy z pracownikiem 3. Nadzór nad ryzykiem nadania uprawnień niezgodnych z funkcją pracownika 4. Możliwość weryfikacji uprawnień użytkowników w dowolnym punkcie w czasie 5. Rejestracja wszystkich uprawnień nadanych do systemów informatycznych od strony formalnej oraz ich realizacji w systemach informatycznych 6. Obsługa do 250 użytkowników. |
| Powiadamianie e-mail | |
| 9. | 1. Możliwość informowania o zdarzeniach związanych z przekroczonymi terminami planów postępowania 2. Możliwość informowania i zdarzeniach związanych z potrzebą wykonania przeglądu ryzyk 3. Możliwość informowania o zdarzeniach związanych z obowiązkiem przeprowadzenia pomiaru KRI 4. Możliwość informowania o zdarzeniach związanych z realizacją zgłoszeń i incydentów 5. Możliwość informowania o zdarzeniach związanych ze zmianami uprawnień 6. Wysyłka za pomocą serwera SMTP do wskazanych użytkowników |
| Funkcjonalności ogólne oprogramowania i wsparcie | |
| 10. | 1. Dostęp w jednym czasie dla 5 użytkowników Zamawiającego 2. Możliwość rozszerzenia o dodatkowe konta dostępu 3. Dostęp do bazy predefiniowanych ryzyk online (Internet) przez okres min. 12 miesięcy 4. Tworzenie nielimitowanej ilości identyfikowanych ryzyk 5. Importowanie i eksportowanie danych w formacie Excela 6. Licencja wieczysta |

# Odnowienie licencji posiadanego oprogramowania antywirusowego ESET

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Procesor | Zamawiający posiada obecnie licencję na oprogramowanie antywirusowe ESET Protect Elite ważne do 27.10.2024 roku  W ramach dostawy należy rozszerzyć posiadaną licencję o dodatkowe 15 stanowisk oraz przedłużyć posiadane wsparcie producenta o minimum 12 miesięcy od końca obecnej licencji.  długość przedłużonego wsparcia/licencji – pozacenowe kryterium oceny ofert] |

# **Przełącznik sieciowy klasy enterprise**

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Wymagania ogólne | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack 19”. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. |
| Wymagane parametry fizyczne | 1. Obudowa rack o wysokości max. 1U 2. 2 wewnętrzne zasilacze 230V AC typu hot-swap. 3. Port USB umożliwiający podłączenie zewnętrznej pamięci flash |
| Wymagana konfiguracja portów | 1. Przełącznik musi posiadać minimum: 2. 48 portów gigabitowych w standardzie 100/1000BaseT 3. Minimum 2 porty 10Gb SFP 4. Minimum 4 portów 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). 5. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia. |
| Przełącznik | 1. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: 2. Zarządzanie stosem poprzez jeden adres IP 3. Do min. 8 jednostek w stosie 4. Przełącznik musi umożliwiać połączenie w stos z już posiadanymi przełącznikami tj. Alcatel-Lucent OS6560-48X4 5. Magistrala statkująca o wydajności 40 Gb/s 6. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie 7. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree 8. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. 9. Wbudowana pamięć RAM min. 1 GB 10. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB |
| Matryca przełączająca | 1. Matryca przełączająca o wydajności min. 216 Gbps, wydajność przełączania przynajmniej 160 Mpps. 2. Obsługa min 16 000 adresów MAC |
| VLAN | Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ) |
| Ramki JUMBO | Obsługa ramek jumbo o wielkości min. 9 216 bajtów |
| GVRP | Obsługa protokołu GVRP lub równoważny |
| Obsługa protokołów wielościeżkowych | 1. Wsparcie dla protokołów: 2. IEEE 802.1w Rapid Spanning Tree 3. IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu. 4. Ethernet Ring Protection version 2 |
| Routing IP | 1. Obsługa min. 256 tras dla routingu IPv4 2. Obsługa min. 128 tras dla routingu IPv6 3. Obsługa protokołów routingu minimum: 4. IPv4: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów). 5. IPv6: minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów). |
| Inne | 1. Obsługa protokołów LLDP i LLDP-MED 2. Przełącznik musi posiadać funkcjonalność DHCP Server 3. Obsługa ruchu multicast: IGMP Snooping v1, v2 i v3 4. Obsługa mechanizmu DHCP snooping |
| Mechanizmy związane z zapewnieniem bezpieczeństwa sieci | 1. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: 2. min. 4 poziomy dostępu administracyjnego poprzez konsolę 3. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL 4. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www 5. zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP 7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny), 8. możliwość synchronizacji czasu zgodnie z NTP |
| QoS | 1. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: 2. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP |
| OpenFlow | Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3. |
| Wymagane opcje zarządzania | 1. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, 2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), 3. urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, 4. dedykowany port konsoli zgodny ze standardem RS-232, |
| Kable DAC, modułu GBIC | 1. Minimum 8 szt. kabli DAC 10Gb SFP+ o długości min. 3m 2. Oferowane i dostarczone kable muszą być na liście kompatybilności producenta switcha w celu zapewnienia poprawnej ich pracy. |
| Inne | 1. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. 2. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. |
| Gwarancja | 1. Przełącznik być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie. 2. Dodatkowo: Zamawiający wymaga, aby przełącznik posiadał 5-letni rozszerzony serwis gwarancyjny na sprzęt i oprogramowanie. Wymiana uszkodzonego elementu w trybie 9x5, wraz z dostępem do najnowszych wersji oprogramowania w czasie trwania serwisu. 3. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność i długość **rozszerzonych uprawnień gwarancyjnych** na terenie Polski. |

# Urządzenie brzegowe UTM typ 1

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| 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 4 administratorów do poszczególnych instancji systemu.  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 klaster 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 łączy 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 i zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej 5portami Gigabit Ethernet RJ-45.  2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. System jest 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 800 Mbps.  4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4,4 Gbps.  5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.  6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps. |
| Funkcje systemu bezpieczeństwa | 1. Kontrola dostępu - zapora ogniowa 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. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.  12. 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.  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).  • Obsługa 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.  • 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 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 RIPng), 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 | 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. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  19. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  7. 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. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. 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.  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.  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. |
| Serwisy, licencje i gwarancja | 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 na okres 12 miesięcy  Gwarancja sprzętowa: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7  [długość serwisów i gwarancji sprzętowej: pozacenowe kryterium oceny ofert] |

# Urządzenie brzegowe UTM typ 2

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| 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 4 administratorów do poszczególnych instancji systemu.  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 klaster 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 łączy 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 i zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej 10portami Gigabit Ethernet RJ-45.  2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. System jest 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 10 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.  4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6,5 Gbps.  5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.  6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps. |
| Funkcje systemu bezpieczeństwa | 1. Kontrola dostępu - zapora ogniowa 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. 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.  10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.  12. 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.  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).  • Obsługa 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.  • 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 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 RIPng), 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 | 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. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  19. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  7. 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. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. 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.  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.  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. |
| Serwisy, licencje i gwarancja | 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 na okres 12 miesięcy  Gwarancja sprzętowa: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7  [długość serwisów aktualizacyjnych i gwarancji sprzętowej: pozacenowe kryterium oceny ofert] |

# rządzenie NAS wraz z oprogramowaniem do backup-u

|  |  |  |  |
| --- | --- | --- | --- |
| Cecha | Wymagania minimalne | | |
| Procesor | Jeden 2-rdzeniowy/4-wątkowy procesor AMD Ryzen R1600 | | |
| Obudowa | Tower o wymiarach max. 167 × 200 × 224 mm | | |
| Pamięć RAM | 16GB pamięci SO-DIMM DDR4 ECC z opcja rozszerzenia do 32GB SO-DIMM DDR4 ECC; zainstalowana pamięć musi być tego samego producenta co NAS | | |
| Ilość obsługiwanych dysków | 4 dyski 3,5”/2,5”  2 dyski M.2 NVMe 2280 | | |
| Ilość zainstalowanych dysków | 4 dyski o pojemności min. 8TB, 7200 RPM i MTBF min. 2000000h znajdujące się na liście zgodności serwera NAS; możliwość aktualizacji firmware dysków z poziomu serwera NAS | | |
| Interfejsy sieciowe | 2 porty 1 Gb BaseT (10/100/1000)  Wsparcie dla Link Agregation. | | |
| Porty | 2 x USB3.2, 1 x eSATA | | |
| Wskaźniki LED | Status, HDD1-4, Power on; LAN 1-4 | | |
| Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10 | | |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | | |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | | |
| Licencja na Kamery IP | W zestawie licencja na dwie kamery z możliwością rozszerzenia do 40. | | |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | | |
| Usługi | 1. Serwer VPN 2. Serwer pocztowy dla kilku domen 3. Stacja monitoringu 4. Windows ACL 5. Integracja z Windows ADS 6. Firewall 7. Serwer WWW 8. Serwer plików 9. Manager plików przez WWW 10. Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie 11. Usługa DDNS 12. Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID 13. Snapshot Replication 14. Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware 15. Wsparcie dla High Availability | | |
| Obsługa SSD Cache | Wymagane wsparcie dla SSD Cache | | |
| Oprogramowanie do kopii zapasowej | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu:   1. kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, 2. kopia zapasowa środowisk MacOS 3. kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) 4. kopia zapasowa serwerów fizycznych (Windows, Linux) 5. obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, 6. obsługa wielu wersji i retencji, 7. możliwość wyzwalania kopii zapasowej według harmonogramu, 8. obsługa klastra przełączania awaryjnego Microsoft Hyper-V, 9. automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, 10. centralne zarządzanie, 11. konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, 12. portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), 13. delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, 14. kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace 15. zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera. | | |
| Oprogramowanie | 1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 2. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. 3. Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. 4. Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync 5. Obsługa minimum 1000 migawek na folder współdzielony i minimum 65000 migawek na cały system 6. Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 60jednoczesnych połączeń | | |
| Obsługa migawek | Maksymalna liczba migawek folderów współdzielonych: 1 024  Maksymalna liczba migawek systemu: 65 536 | | |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów | | |
| Język GUI | Polski | | |
| System plików | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) | | |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) | | |
| Liczba wolumenów | Do 64 | | |
| Liczba iSCSI Targetów | Do 128 | | |
| Liczba iSCSI LUN | Do 256 | | |
| Liczba kont użytkowników | 2048 | | |
| Liczba grup | 256 | | |
| Liczba folderów udostępnionych | 512 | | |
| Ilość jednoczesnych połączeń | 1000 dla CIFS/AFP/NFS/FTP/WebDAV | | |
| Zasilacz | 100W | | |
| Gwarancja i serwis | | Min. 12 miesięcy gwarancji realizowanej w trybie NBD Onsite przez producenta lub Autoryzowanego Partnera Serwisowego producenta; dyski objęte wsparciem pozostawienia dysku w przypadku wystąpienia awarii.  **Wraz z dostawą sprzętu Wykonawca dostarczy dokument potwierdzający warunki gwarancji wystawione przez producenta urządzenia lub autoryzowanego partnera serwisowego potwierdzający zaoferowane warunki gwarancji.**  [długość gwarancji: pozacenowe kryterium oceny ofert] |

# UPS Stanowiskowy

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Moc pozorna | 700 VA |
| Moc rzeczywista | 360 W |
| Technologia | Line-Interactive |
| Gniazda wyjściowe z podtrzymaniem bateryjnym | typu E (2P+Z), minimum 2szt |
| Przewód zasilający | Przymocowany na stałe do zasilacza UPS |
| Port komunikacyjny | USB umieszczony na przednim panelu zasilacza UPS |
| Wskaźnik stanu UPS | Dioda LED |
| Parametry wejściowe | |
| Prąd znamionowy | 10A |
| Napięcie znamionowe | 220-240 V; 50/60 Hz |
| Zakres napięcia wejściowego | 140-300 V; 45-65 Hz |
| Parametry wyjściowe | |
| Znamionowe napięcie wyjściowe | 220/230/240 V |
| Regulacja napięcia w trybie bateryjnym | +/-20% |
| Sprawność w trybie normalnym | >95% |
| Sprawność w trybie bateryjnym | >60% |
| Regulacja częstotliwości w trybie normalnym | zgodnie z siecią zasilającą |
| Regulacja częstotliwości w trybie bateryjnym | +/-1 Hz |
| Częstotliwość w trybie normalnym | zgodnie z siecią zasilającą |
| Częstotliwość w trybie bateryjnym | 50/60 Hz |
| Zdolność zwarciowa w trybie bateryjnym | 16A |
| Wytrzymywany czas przepływu prądu zwarciowego | 50 ms |
| Czas przełączania | 10 ms dla przejścia z trybu normalnego do trybu bateryjnego |
| Bateria | |
| Specyfikacja | 12 V DC – 1 x 12 V, 7 Ah |
| Typ | Valve Regulated Lead-Acid (VRLA) szczelne, bezobsługowe, z minimalną żywotnością 3-5 lat w temperaturze 25°C |
| Monitoring | Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem. |
| Zimny start | Tak |
| Parametry środowiskowe i bezpieczeństwo | |
| Stopień ochrony | IP20 |
| Układ sieci | UPS można podłączyć do układów zasilania TN, TT, IT, ten sam system jest dostarczany do obciążenia. |
| Temperatura pracy | 0°C do 40°C (32°F do 104°F) |
| Wilgotność względna | Przechowywanie: 0-93% bez kondensacji  Praca: 0-85% bez kondensacji |
| Poziom hałasu | <25 dBA |
| Wymiary i waga | Maks. 300x150x100 mm, waga maks.4,5kg |
| Gwarancja | 24 miesiące |

# Serwer aplikacyjny tower z serwerowym system operacyjnym oraz licencjami dostępowymi

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Obudowa | Obudowa typu Tower posiadająca 8 zatok dla dysków twardych 3,5” HotPlug. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| Procesor | Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej:   1. SPECrate2017\_int\_base wynik min. 90pkt 2. SPECrate2017\_int\_peak wynik min. 94pkt 3. SPECrate2017\_fp\_base wynik min. 105pkt 4. SPECrate2017\_fp\_peak wynik min. 105pkt   Maksymalny TDP dla procesora 80W  Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty.  Należy załączyć do oferty wydruk ze strony [www.spec.org](http://www.spec.org) potwierdzające powyższe wymagania. |
| Pamięć RAM | Min. 64GB i minimum RAM DDR5 UDIMM o częstotliwości pracy min 5400MT/s |
| Zabezpieczenia pamięci | Demand Scrubing, Patrol Scrubing, Permanent Fault Detection |
| Wbudowane porty | Minimum 8 portów USB z czego min. 4 w technologii 3.2  1x RS-232  1x VGA |
| Karta graficzna | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT |
| Kontroler RAID | Sprzętowy kontroler dyskowy obsługujący konfiguracji poziomów RAID: 0, 1, 10.  Wsparcie dla dysków samoszyfrujących |
| Dyski twarde | Zainstalowane 2 dyski min. 1,92TB SSD SATA, typu ReadIntensive DWPD>=1, Hot-Plug.  Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| Zasilacze | Dwa Redundantne, o mocy maks. 700W każdy klasy Titanium |
| Bezpieczeństwo | Zintegrowany z płytą główną moduł TPM 2.0  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + 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   oraz z możliwością rozszerzenia funkcjonalności o:   * + 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) |
| Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - **dołączyć do oferty jako przedmiotowy środek dowodowy**.  Serwer musi posiadać deklarację CE - **dołączyć do oferty jako przedmiotowy środek dowodowy**.  Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami **dołączyć do oferty jako przedmiotowy środek dowodowy** |
| **System operacyjny** | Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.  SSO musi posiadać następujące, wbudowane cechy:  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,  d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,  f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,  h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,  k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,  o) graficzny interfejs użytkownika,  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| Licencje dostępowe | Minimum 10 licencji dostępowych typu USER CAL dla systemu operacyjnego. |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| Warunki gwarancji | * + - 1. Minimum 12 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.       2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.       3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.       4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.       5. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.       6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.       7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.       8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.       9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.       10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.       11. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.       12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty.       13. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny link do strony producenta urządzenia z ogólnodostępnym dokumentem np. certyfikat lub deklaracją producenta, potwierdzającym autoryzację dla firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku braku takiego linku lub ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski       14. W przypadku gdy producent posiada firmę serwisującą w jego imieniu sprzęt należy potwierdzić autoryzację producenta dla Firma serwisująca – na potwierdzenie należy przedstawić ogólnodostępny link do strony producenta urządzenia z oficjalnym dokumentem np. certyfikat lub oświadczenie, potwierdzającym autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia tak aby Zamawiający mógł samodzielnie zweryfikować te informację W przypadku braku takiego linku lub ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski.   **Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy**  [długość gwarancji: pozacenowe kryterium oceny ofert] |

# Punkt dostępowy dla sieci WiFi

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.   1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:    1. Temperatura 0-45°C,    2. Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington. 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:    1. 2.4 GHz 802.11b/g/n/ax,    2. 5GHz 802.11a/n/ac/ax ze wsparciem dla kanałów 20/40/80/160MHz,    3. 2.4/5GHz dedykowany skaner spectrum. 4. Urządzenie musi być wyposażone w moduł radiowy Bluetooth/BLE. 5. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID. 6. Liczba interfejsów:    1. 2x Ethernet – 1 w standardzie 10/100/1000/2500 Base-TX, 1 w standardzie 10/100/1000 Base-TX    2. Port szeregowy RS-232 RJ-45 7. Urządzenie powinno być zasilane poprzez oba interfejsy ETH w standardzie 802.3af/at lub zewnętrzny zasilacz. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:    1. Tunnel,    2. Bridge,    3. Mesh. 9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). 10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:     1. MIMO – 4x4, 1x1 w przypadku radia pracującego jako dedykowany skaner     2. Transmit Beam Forming (TxBF),     3. Maksymalna przepustowość dla poszczególnych modułów radiowych:        1. 1140 Mbps;        2. 2400 Mbps;     4. Wymagana moc nadawania:        1. min. 24 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;        2. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;     5. Wsparcie dla 802.11n 20/40Mhz HT,     6. Wsparcie dla kanału 160 MHz dla 802.11ac,     7. Anteny – 5 wewnętrznych dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.     8. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,     9. Maksymalna deklarowana liczba klientów per moduł radiowy – 512 |
| Gwarancja oraz wsparcie | Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta tzw. LifeTime do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 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. |

# ETAP II – wdrożenie dostarczonych rozwiązań i usługa segmentacji sieci

# Segmentacja sieci

## Segmentacja sieci

1. Wykonawca przygotuje i omówi koncepcję instalacji i konfiguracji z administratorem sieci Zamawiającego.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogramy wdrożenia.
3. Wdrożenie nowych urządzeń musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu UTMy, przełączniki CORE, Active Directory) będących w posiadaniu Zamawiającego. Dodatkowo każda zmiana w koncepcji musi być każdorazowo uzgadniana z Administratorem sieci.
4. Prace, które będą powodować przerwy w segmentach sieci w dostępności do usług dla pracowników urzędu winny być wykonywane poza godzinami pracy urzędu. Możliwe jest również wykonywanie prac w dni wolne od pracy w urzędzie po wcześniejszym uzgodnieniu z Zamawiającym.
5. Wykonawca wykona prekonfigurację UTM i NAS w jednostkach organizacyjnych.

## Wdrożenie systemu NAC w ramach pkt.2 OPZ

1. Prace, które będą powodować przerwy w segmentach sieci w dostępności do usług dla pracowników urzędu winny być wykonywane poza godzinami pracy urzędu. Możliwe jest również wykonywanie prac w dni wolne od pracy w urzędzie po wcześniejszym uzgodnieniu z Zamawiającym.
2. Instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
3. Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
4. Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
5. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
6. Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
7. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
8. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
9. Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania systemu

## Wdrożenie narzędzi wspomagających zarządzanie ryzykami i uprawnieniami

1. Dokonanie oceny zabezpieczeń technicznych i organizacyjnych stosowanych przez Zamawiającego- forma zdalna
2. Identyfikacja ryzyk w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji, w tym ochrony danych osobowych -forma zdalna
3. Ocena i przygotowanie planów postępowania z ryzykiem- forma zdalna
4. Min. 6 – godzinne szkolenie dla osób wyznaczonych przez Zamawiającego z metodyki oraz pracy z wykorzystaniem narzędzia wspomagającego analizę ryzyka- forma zdalna
5. Wsparcie podczas instalacji i konfiguracji bazy danych