Załącznik nr 7 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**ETAP I**

1. **Klaster HA urządzeń UTM (1x klaster UTM, tj. 2 szt. UTM)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania** |
| Obsługa sieci | 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |
| Zapora korporacyjna (firewall) | 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.  2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.  3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).  4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.  5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów  wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.  6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.  7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie  konfigurowalnych, zestawów reguł firewall.  8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.  9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.  10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).  11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe |
| Intrusion prevention system (IPS) | 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.  2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.  3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.  4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.  5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.  6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.  7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.  8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.  9. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych. |
| Kształtowanie pasma (traffic shapping) | 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.  2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.  3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).  4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |
| Ochrona antywirusowa | 1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).  2. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.  3. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji. |
| Ochrona antyspam | 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).  2. Ochrona antyspam ma działać w oparciu o:  a. białe/czarne listy,  b. DNS RBL,  c. Skaner heurystyczny.  3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.  4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |
| Wirtualne sieci prywatne (VPN) | 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).  2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:  a. PPTP VPN,  b. IPSec VPN,  c. SSL VPN.  3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.  4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.  5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)  6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). |
| Filtr dostępu do stron www | 1. Urządzenie ma posiadać wbudowany filtr URL.  2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii  tematycznych stron internetowych.  3. Administrator ma mieć możliwość dodawania własnych kategorii URL.  4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:  a. blokowanie dostępu do adresu URL,  b. zezwolenie na dostęp do adresu URL,  c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej  przez administratora.  5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.  7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.  8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.  9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.  10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch |
| Uwierzytelnianie | 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:  a. lokalną bazę użytkowników (wewnętrzny LDAP),  b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),  c. usługę katalogową Microsoft Active Directory.  2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.  3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:  a. SSL,  b. Radius,  c. Kerberos.  4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.  5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.  6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.  7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).  8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).  9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneliSSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. |
| Administracja łączami do internetu (ISP) | 1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).  2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  a. równoważenie względem adresu źródłowego,  b. równoważenie względem połączenia.  3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.  4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza  podstawowego (tzw. Failover).  5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.  6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie  opóźnienia, jitter, wskaźnika utraty pakietów).  7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. |
| Routing (trasowanie) | 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.  2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania  statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza  podstawowego.  3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).  4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |
| Administracja urządzeniem | 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.  2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.  3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.  4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.  5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)  7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.  8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.  9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.  10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do  przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.  11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.  12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).  13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).  14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.  15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).  16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.  17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:  a. manualnego eksportu do pliku w dowolnym momencie czasu,  b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer  zarządzany przez administratora, z możliwością wyboru częstotliwości  18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.  19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.  20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. |
| Raportowanie | 1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.  2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.  3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.  4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.  5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.  6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.  7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.  8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.  9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). |
| Pozostałe usługi i funkcje | 1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.  2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).  3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.  4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci  skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie  określenia bramy, serwerów DNS, nazwy domeny).  5. Urządzenie ma posiadać usługę DNS Proxy.  6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.  7. Urządzenie musi mieć zaimplementowane Open API  8. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.  9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. |
| Gwarancja i serwis | 1. Do dnia 25.06.2026 roku urządzenie musi posiadać dostęp do aktualizacji FW+IPS, VPN, filtr URL, AV, AS, obsługa kart SD lub wbudowanego dysku twardego. 2. Do dnia 25.06.2026 roku należy zapewnić wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma być objęte 2-letnią gwarancją producenta. |
| Parametry sprzętowe | 1. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.  2. Urządzenie może być pozbawione dysku twardego, a oprogramowanie wewnętrzne może działać na wbudowanej pamięci flash.  3. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD lub dysk twardy do przechowywania logów.  4. Liczba portów Ethernet 2,5Gbps – min. 8.  5. Liczba portów światłowodowych 1Gbps – min. 1.  6. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.  7. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.  8. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.  9. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.  10. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.  11. Maksymalna liczba tuneli VPN IPSec – minimum 100.  12. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.  13. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100.  14. Obsługa interfejsów 802.11q (VLAN) – minimum 128  15. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.  16. Urządzenie nie ma limitu na liczbę użytkowników.  17. Liczba reguł filtrowania – minimum 8 192.  18. Liczba tras statycznego routingu – minimum 512.  19. Liczba tras dynamicznego routingu – minimum 10 000.  20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie  redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.  21. Urządzenie musi być wyposażone w moduł TPM.  **W urządzeniu należy zainstalować kartę pamięci microSD o pojemności 32GB lub dysk o pojemności 100GB.** |

1. Zakres instalacji i konfiguracji

* aktualizacja oprogramowania firmware do najnowszej wersji,
* przeniesienie konfiguracji z dotychczasowego urządzenia brzegowego do dostarczonego urządzenia,
* analiza aktualnej konfiguracji mechanizmów bezpieczeństwa oraz wprowadzenie zmian w konfiguracji urządzenia brzegowego mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego,
* wprowadzenie do konfiguracji urządzenia UTM zmian umożliwiających izolację serwerów od sieci produkcyjnej oraz identyfikacja usług (portów) niezbędnych do zachowania komunikacji ze stacjami roboczymi użytkowników (bez konieczności zmiany adresacji IP),
* analiza ruchu z serwerów aplikacyjnych oraz odseparowanie tych serwerów od sieci Internet; identyfikacja i przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,
* połączenie urządzeń w klaster wysokiej dostępności HA w trybie Active-Passive,
* przeprowadzenie testów funkcjonowania klastra UTM,
* przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

Wykonawca zagwarantuje, że zadania określone powyżej wykonywać będzie osoba posiadająca niezbędne umiejętności w tym aktualny certyfikat kompetencji wystawiony przez producenta urządzenia lub autoryzowane centrum szkoleniowe.

1. **Przełącznik zarządzalny, 8-portowy (4 szt.)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania** |
| Porty przełącznika | minimum 8x 10/100/1000Base-T RJ45 oraz minimum 2x 100/1000Base-X SFP |
| Port konsolowy | RJ45 (RS-232) |
| Szybkość przełączania | minimum 20Gb/s |
| Przepustowość | minimum 14Mp/s (dla pakietów 64Kb) |
| Bufor pakietów | minimum 0,5MB |
| Ramki Jumbo | minimum 10k |
| Tablica adresów MAC | minimum 8k |
| Tablica ACL | minimum 1200 |
| Tablica VLAN | minimum 4000 |
| Pamięć RAM | minimum 128MB |
| Zasilanie | zabudowany zasilacz 230V AC |
| Certyfikaty bezpieczeństwa | CE, RoHS |
| VLAN | Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Selective QinQ, Flexible QinQ |
| DHCP | IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82,Option 37/38, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server |
| Spanning tree | IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding |
| Agregacja łączy | IEEE 802.3ad (LACP), 8 groups per device / 8 ports per group |
| Bezpieczeństwo | Storm Control based on packets and bytes, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting Radius, TACACS+ |
| Multicast | IGMP v1/v2/v3 snooping, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication |
| Lista kontroli dostępu | IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL |
| Diagnostyka | VCT, DDM, Ping, Trace Route, RSPAN |
| Zarządzanie | TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, , SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, CPU Mirror, ULDP (like UDLD), LLDP/LLDP MED., auto provisioning |
| Oprogramowanie oraz wsparcie techniczne | oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług |
| Gwarancja | lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

1. Zakres instalacji i konfiguracji

* aktualizacja oprogramowania firmware do najnowszej wersji,
* konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych Zamawiającego.

1. **Przełącznik zarządzalny, 24-portowy (3 szt.)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania** |
| Porty przełącznika | minimum 4x COMBO (10/100/1000Base-T RJ45 lub 100/1000Base-X SFP), minimum 8x 100/1000Base-X SFP oraz minimum 4x 1/10GBase-X SFP+ |
| Port konsolowy | RJ45 (RS-232) |
| Port zarządzania | RJ45 (10/100Base-T RJ45) |
| Szybkość przełączania | minimum 110Gb/s |
| Przepustowość | minimum 70Mp/s (dla pakietów 64Kb) |
| Bufor pakietów | minimum 1,5MB |
| Ramki Jumbo | minimum 10k |
| Tablica adresów MAC | minimum 16k |
| Tablica ACL | minimum 1k |
| Tablica VLAN | minimum 4000 |
| Tablica routingu | minimum 1k dla IPv4, w tym IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1. |
| Pamięć Flash | minimum 128MB |
| Pamięć RAM | minimum 512MB |
| Certyfikaty bezpieczeństwa | CE, RoHS |
| Obsługa VLAN | Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN |
| DHCP | IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server |
| Drzewo rozpinające | IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, |
| Agregacja linków | IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance |
| Bezpieczeństwo | Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Guest VLAN and auto VLAN, |
| QoS | 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, |
| Lista Kontroli Dostępu | IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Standard and Expanded ACL based on IP Precedence, DSCP, ToS; Vlan Tag/Untag, Rules can be configured to port and VLAN |
| Zarządzanie | TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, |
| Oprogramowanie oraz wsparcie techniczne | oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług |
| Gwarancja | lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

Uwaga. Do każdego przełącznika należy dostarczyć:   
- 2 szt. wkładki SFP+ 10GbE RJ45 (łącznie 6 szt. dla trzech szt. przełączników),

- 2 szt. moduł optyczny SFP+ 10Gb (łącznie 6 szt. dla trzech szt. przełączników),

- patchcord światłowodowy do wykonania stack-a przełączników (łącznie 4 szt. dla trzech szt. przełączników).

1. Zakres instalacji i konfiguracji

* aktualizacja oprogramowania firmware do najnowszej wersji,
* połączenie przełączników w stack oraz przeprowadzenie testów konfiguracji,
* konfiguracja grup portów,
* konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.

1. **Dysk sieciowy NAS (1 szt.) z dyskami twardymi**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania** |
| Typ urządzenia | Serwer NAS |
| Obudowa | Rack 1U |
| Procesor | Min. czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2022 co najmniej 4 580 punktów |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 8 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA. |
| Dyski twarde | Sprzęt powinien być wyposażony w 4 dyski (producenta urządzenia sieciowego) dedykowane do pracy w NAS o pojemności min. 4 TB 3,5” HDD o prędkości obrotowej 5400 rpm |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 * 1 port eSATA (jako gniazdo rozszerzenia) |
| Porty sieciowe | Minimum:   * 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |
| Funkcja Wake on LAN/WAN | Tak |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:   * Wewnętrzny: Btrfs, ext4 * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu: 108 TB * Minimalny liczba wewnętrznych wolumenów: 64 * Minimalny liczba obiektów iSCSI Target: 128 * Minimalny liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| Uprawnienia | Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji |
| Wirtualizacja | Obsługa VMware vSphere with VAAI, Microsoft Hyper-V, Citrix, OpenStack |
| Usługa katalogowa | Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane przeglądarki | Google Chrome, Firefox, Microsoft Edge, Safari 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach |
| Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC 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 współdzielonych * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów * 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 a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| Gwarancja | * 3 lata na urządzenia główne oraz 3 lata na dyski twarde |

1. Zakres instalacji i konfiguracji

* w urządzeniu należy zainstalować dyski twarde oraz wykonać ich konfigurację (RAID-5),
* urządzenie należy zainstalować w szafie RACK Zamawiającego.

1. **Dysk twardy do serwera archiwum (4 szt.)**
2. Informacje o dyskach i serwerze docelowym

* 4x dysk SAS 900GB z ramką do mocowania do serwera DELL PowerEdge R450 (ST: 6H321S3)

1. Zakres instalacji i konfiguracji

* Dyski twarde należy zainstalować w serwerze wskazanym przez Zamawiającego.

1. **Zakup oprogramowania antywirusowego -zmiana wersji na program z obsługą Firewall i SANDBOX**

**Dane aktualnej licencji:**

Rodzaj: ESET PROTECT Essential ON-PREM

Liczba licencji: 39

Data ważności: 29.04.2025 r.

**Dane nowej licencji:**

Rodzaj: ESET PROTECT Advanced lub inna zawierająca moduły Firewall oraz Sandboxing w chmurze

Liczba licencji: 45

Data rozpoczęcia abonamentu: 7 dni od podpisania umowy na realizację niniejszego zadania

Data ważności: 25.06.2026

Konsola zarządzająca: w chmurze ESET

1. **Wsparcie techniczne do serwera Zabbix + GrayLog**
2. Okres wsparcia technicznego i częstotliwość wykonywania czynności serwisowych

* okres wsparcia technicznego: od dnia podpisania umowy wynikającej z niniejszego postępowania do dnia 25.06.2026 roku,
* minimalna częstotliwość wykonywania czynności serwisowych w okresie wsparcia technicznego: jeden raz na 3 miesiące.

1. Zakres pierwszej instalacji/konfiguracji

* kontrola zajętości dysków wirtualnych z bazami Zabbix i Graylog;
* aktualizacja języka php do wersji 8.3, ustawienie nowej wersji jako domyślnej i odinstalowanie języka php w wersjach starszych,
* aktualizacja komponentów systemu Debian 11,
* zmiana listy źródeł z wersji Bullseye na Bookworm,
* aktualizacja systemu operacyjnego, a następnie aktualizacja aplikacji,
* aktualizacja repozytorium oprogramowania Zabbix, zastąpienie instancji starej instalacji Zabbix (6.4) nową wersją Zabbix 7.0 dostosowaną do systemu operacyjnego Debian 12, kontrola aktualizacji wersji bazy danych Mariadb, modyfikacja wartości NextID w tabelach,
* aktualizacja repozytorium oprogramowania Graylog, zastąpienie starej instancji Graylog 5.2, aplikacją Graylog Open 6.0,
* analiza logów aplikacji w celu wychwycenie potencjalnych błędów aktualizacji oprogramowania,
* weryfikacja i dostosowanie ustawień firewall-a UFW maszyny wirtualnej,
* konfiguracja nowego Input w systemie Graylog w celu odseparowania logów urządzenia brzegowego, dodania znacznika do logów otrzymywanych z urządzenia brzegowego,
* wprowadzenie nowych reguł przetwarzania logów w systemie Graylog dla wiadomości przesyłanych przez urządzenie brzegowe w celu ekstrakcji wartości poszczególnych kolumn,
* analiza dostępności hostów w systemie Zabbix, ostatniego czasu odczytu danych przez SNMP lub agenta Zabbix, sprawdzenie ilości i przyczyn niewspieranych obiektów („Not Supported Items”).

1. Czynności serwisowe wykonywane w okresie wsparcia technicznego

* kontrola sprawności mechanizmu archiwizacji maszyny wirtualnej,
* kontrola zajętości dysków wirtualnych z bazami Zabbix i Graylog,
* aktualizacja języka php,
* aktualizacja komponentów systemu Debian,
* aktualizacja oprogramowania Zabbix,
* aktualizacja oprogramowania Graylog,
* analiza logów aplikacji w celu wychwycenie potencjalnych błędów aktualizacji oprogramowania,
* weryfikacja, czy kluczowe hosty w ciągu ostatniego miesiąca wysyłały logi na serwer Graylog (na podstawie dostarczonej przez administratora systemu informatycznego listy kluczowych urządzeń) oraz analiza przyczyn braku takiej komunikacji,
* analiza logów serwera Zabbix w poszukiwaniu prób rejestrowania hostów przez Zabbix Agent Active,
* konfiguracja SNMP lub instalacja agenta Zabbix na urządzeniach, które do tej pory nie były monitorowane przez system Zabbix (na podstawie dostarczonej przez administratora systemów informatycznych listy kluczowych urządzeń); dodanie nowych hostów w systemie Zabbix wraz z poświadczeniami wymaganymi do komunikacji oraz dobranie odpowiednich szablonów,
* utworzenie szablonów do monitorowania hostów kluczowych, które do tej pory były monitorowane tylko pod względem dostępności w sieci (testy ICMP), analiza możliwości monitorowania parametrów na podstawie plików MIB producenta i przygotowania reguł Discovery w celu zbierania danych o kluczowych do funkcjonowania urządzenia parametrach,
* analiza raportu najpopularniejszych triggerów w systemie Zabbix i dostosowanie stopnia powiadomień lub wartości granicznych w celu optymalizacji alertów wysyłanych do administratorów.

1. **UTM (2 szt.)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Obsługa sieci | 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie  konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |
| Zapora korporacyjna (firewall) | 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.  2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.  3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).  4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.  5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.  6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.  7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie  konfigurowalnych, zestawów reguł firewall.  8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.  9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.  10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).  11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe. |
| Intrusion prevention system (IPS) | 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.  2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.  3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.  4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.  5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.  6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.  7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.  8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.  9. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych. |
| Kształtowanie pasma (traffic shapping) | 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.  2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.  3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).  4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |
| Ochrona antywirusowa | 1. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).  2. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.  3. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji. |
| Ochrona antyspam | 1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).  2. Ochrona antyspam ma działać w oparciu o:  a. białe/czarne listy,  b. DNS RBL,  c. Skaner heurystyczny.  3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.  4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |
| Wirtualne sieci prywatne (VPN) | 1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).  2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:  a. PPTP VPN,  b. IPSec VPN,  c. SSL VPN.  3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.  4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.  5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)  6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).  7. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. |
| Filtr dostępu do stron www | 1. Urządzenie ma posiadać wbudowany filtr URL.  2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii  tematycznych stron internetowych.  3. Administrator ma mieć możliwość dodawania własnych kategorii URL.  4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:  a. blokowanie dostępu do adresu URL,  b. zezwolenie na dostęp do adresu URL,  c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej  przez administratora.  5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.  7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.  8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.  9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.  10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch |
| Uwierzytelnianie | 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:  a. lokalną bazę użytkowników (wewnętrzny LDAP),  b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),  c. usługę katalogową Microsoft Active Directory.  2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.  3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:  a. SSL,  b. Radius,  c. Kerberos.  4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.  5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.  6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.  7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).  8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).  9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneliSSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. |
| Administracja łączami do internetu (ISP) | 1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).  2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  a. równoważenie względem adresu źródłowego,  b. równoważenie względem połączenia.  3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.  4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza  podstawowego (tzw. Failover).  5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.  6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).  7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. |
| Routing (trasowanie) | 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.  2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania  statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza  podstawowego.  3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).  4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |
| Administracja urządzeniem | 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.  2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.  3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.  4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.  5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)  7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.  8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.  9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.  10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.  11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.  12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).  13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).  14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.  15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).  16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.  17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:  a. manualnego eksportu do pliku w dowolnym momencie czasu,  b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer  zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz  dziennie, raz w tygodniu, raz w miesiącu  18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.  19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.  20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. |
| Raportowanie | 1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.  2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.  3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.  4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.  5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.  6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.  7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i  tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.  8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.  9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH). |
| Pozostałe usługi i funkcje | 1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.  2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).  3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.  4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci  skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie  określenia bramy, serwerów DNS, nazwy domeny).  5. Urządzenie ma posiadać usługę DNS Proxy.  6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.  7. Urządzenie musi mieć zaimplementowane Open API  8. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. |
| Gwarancja i serwis | 1. Do dnia 31.05.2026 roku urządzenie musi posiadać dostęp do aktualizacji FW+IPS, VPN, filtr URL, AV, AS, obsługa kart SD lub wbudowanego dysku. 2. Do dnia 31.05.2026 roku należy zapewnić wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Urządzenie ma być objęte 2-letnią gwarancją producenta. |
| Parametry sprzętowe | 1. Urządzenie może być pozbawione dysku twardego, a oprogramowanie wewnętrzne może działać na wbudowanej pamięci flash.  2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD lub dysk twardy do przechowywania logów.  3. Liczba portów Ethernet 2,5Gbps – min.4.  4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.  5. Przepustowość Firewall (1518 bajtów UDP) – minimum 3Gbps.  6. Przepustowość Firewall wraz z włączonym systemem IPS (1400 bajtów UDP) – minimum 1Gbps.  7. Przepustowość filtrowania Antywirusowego – minimum 300Mbps.  8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.  9. Maksymalna liczba tuneli VPN IPSec – minimum 50.  10. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.  11. Obsługa interfejsów 802.11q (VLAN) – minimum 100  12. Liczba równoczesnych sesji – minimum 100 000 i nie mniej niż 10 000 nowych sesji/sekundę.  13. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.  14. Urządzenie nie ma limitu na liczbę użytkowników.  15. Liczba reguł filtrowania – minimum 1024.  16. Liczba tras statycznego routingu – minimum 200.  17. Liczba tras dynamicznego routingu – minimum 10 000.  18. Urządzenie musi posiadać pasywny system chłodzenia.  **W urządzeniu należy zainstalować kartę pamięci microSD o pojemności 32GB lub dysk twardy o pojemności min.100GB.** |

1. Zakres instalacji i konfiguracji

* instalacja w jednostkach: SP Raciborowice, GOPS Warta Bolesławiecka,
* aktualizacja oprogramowania firmware do najnowszej wersji,
* przeniesienie konfiguracji z dotychczasowego routera do dostarczonego urządzenia,
* analiza aktualnej konfiguracji mechanizmów bezpieczeństwa oraz wprowadzenie zmian w konfiguracji urządzenia brzegowego mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego,
* konfiguracja sieci VLAN oraz ograniczeń firewall-a,
* izolacja ruchu w celu wykonywania przez jednostki organizacyjne kopii odmiejscowionej,
* analiza ruchu z serwerów aplikacyjnych oraz odseparowanie tych serwerów od sieci Internet; identyfikacja i przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,
* wydzielenie sieci VLAN dedykowanej dla serwera archiwum, przygotowanie reguł firewall-a ograniczających ruch z sieci LAN do serwera archiwum,
* utworzenie harmonogramu dostępności serwera archiwum,
* przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

Wykonawca zagwarantuje, że zadania określone powyżej wykonywać będzie osoba posiadająca niezbędne umiejętności w tym aktualny certyfikat kompetencji wystawiony przez producenta urządzenia lub autoryzowane centrum szkoleniowe.

1. **Odnowienie licencji dla UTM Stormshield SN 310**
2. Parametry aktualnej licencji

* Rodzaj licencji: podstawowa
* Data końca licencji: 04.02.2026 r.

1. Parametry nowej licencji

* Rodzaj licencji: podstawowa
* Data zakończenia licencji: 25.06.2026 r.

1. **Przełączniki zarządzalne do jednostek organizacyjnych (5 szt.)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Porty przełącznika | minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 100/1000Base-X SFP |
| Port konsolowy | RJ45 (RS-232) |
| Szybkość przełączania | minimum 56Gb/s |
| Przepustowość | minimum 41Mp/s (dla pakietów 64Kb) |
| Bufor pakietów | minimum 1,5MB |
| Ramki Jumbo | minimum 12k |
| Tablica adresów MAC | minimum 16k |
| Tablica ACL | minimum 500 |
| Tablica VLAN | minimum 4000 |
| Pamięć RAM | minimum 256MB |
| Zasilanie | zabudowany zasilacz 230V AC |
| Certyfikaty bezpieczeństwa | CE, RoHS |
| VLAN | Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ |
| DHCP | IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82,Option 37/38, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server |
| Spanning tree | IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, |
| Agregacja łączy | IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group |
| Bezpieczeństwo | Storm Control based on bytes, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting Radius, TACACS+ |
| Multicast | IGMP v1/v2/v3 snooping, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication |
| Lista kontroli dostępu | IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL |
| Diagnostyka | VCT, DDM, Ping, Trace Route, RSPAN, Dying GASP, sFlow |
| Zarządzanie | TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, , SNTP/NTP (IPv4/IPv6), Multiple Configuration Files, Port Mirror, CPU Mirror, ULDP (like UDLD), LLDP/LLDP MED., auto provisioning |
| Oprogramowanie oraz wsparcie techniczne | oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług |
| Gwarancja | lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

1. Zakres instalacji i konfiguracji

* instalacja w jednostkach organizacyjnych Zamawiającego,
* przeniesienie konfiguracji ze starych przełączników nieposiadających wsparcia technicznego producenta,
* aktualizacja oprogramowania firmware do najnowszej wersji,
* konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych,
* przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

1. **Dyski sieciowe NAS do jednostek organizacyjnych (5 szt.)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| Typ urządzenia | Serwer NAS |
| Obudowa | Tower |
| Procesor | Czterordzeniowy procesor o taktowaniu 2.0 GHz (maksymalnie  2,7 GHz z przyspieszeniem) osiągający w teście PassMark na luty 2024 co najmniej 2 960 punktów |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB |
| Możliwości rozbudowy | Sprzęt powinien być wyposażony w min. 2 kieszenie na dyski twarde typu hot-swap. Obsługiwane dyski 3.5” oraz 2.5”. |
| Dyski twarde | Sprzęt powinien być wyposażony w 2 dyski (producenta urządzenia sieciowego) dedykowane do pracy w NAS o pojemności min. 4 TB 3,5” HDD o prędkości obrotowej 5400 rpm |
| Porty zewnętrzne | Minimum:   * 2 porty USB 3.2.1 |
| Porty sieciowe | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |
| Funkcja Wake on LAN/WAN | Tak |
| Gniazdo rozszerzeń PCIe 2.0 | Min. 1x 4-liniowe gniazdo x8 gen. 3 |
| Wentylator obudowy | Min. 1 wentylator |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS  Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:   * Wewnętrzny: Btrfs, ext4, * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | * Maksymalny rozmiar pojedynczego wolumenu: 108 TB * Minimalny liczba wewnętrznych wolumenów: 64 * Minimalny liczba obiektów iSCSI Target: 128 * Minimalny liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0,  RAID 1 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows  (ACL) |
| Usługa katalogowa | Integracja z usługami Windows AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane przeglądarki | Google Chrome, Firefox, Microsoft Edge, Safari 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android 11.0 i nowsze) na tabletach |
| Obsługiwane systemy klienckie | Windows 7 i nowsze, macOS 10.12 i nowsze |
| Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni   dyskowej w oparciu o nowoczesny system plików, który  będzie zapewniał obsługę migawek, generowania sum  kontrolnych CRC 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   * Oprogramowanie zarządzające serwerem NAS musi   zapewnić darmowe, kompleksowe rozwiązanie do  tworzenia kopii zapasowych przeznaczone dla  heterogenicznych środowisk IT, umożliwiające zdalne  zarządzanie i monitorowanie ochrony komputerów,  serwerów i maszyn wirtualnych na jednym, centralnym,  przyjaznym dla administratora interfejsie. Ponadto  gromadzone dane na urządzeniu mają mieć możliwość  replikacji jako lokalne kopie zapasowe, sieciowe kopie  zapasowe i kopie zapasowe danych w chmurach  publicznych przy użyciu darmowego narzędzia  instalowanego z Centrum Pakietów   * 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 a także  wspierać algorytm Intelliversioning. Ponadto omawiana  usługa powinna umożliwiać pracę z dokumentami  biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz  slajdów) i wpierać wersjonowanie oraz edycję tworzonych  plików office w czasie rzeczywistym. |
| Gwarancja | 2 lata na urządzenia główne z możliwością przedłużenia do 4  lat za pomocą dodatkowego pakietu gwarancyjnego oraz 2 lata na dyski twarde |

1. Zakres instalacji i konfiguracji

* instalacja w jednostkach organizacyjnych Zamawiającego,
* w urządzeniu należy zainstalować dyski twarde oraz wykonać ich konfigurację (RAID-1),
* urządzenie należy zainstalować w miejscach wskazanych przez Zamawiającego.

1. **Zakup systemu do wykonywania testów i badań bezpieczeństwa, kampanii phishingowych oraz testów podatności**
2. Wymagania ogólne
3. System musi posiadać wsparcie techniczne (licencję) do dnia 25.06.2026 r. na niżej opisane funkcjonalności.
4. System musi umożliwiać wielokrotne przeprowadzenie kampanii phishingowych dla 20 kont poczty elektronicznej.
5. System musi umożliwiać wielokrotne przeprowadzenie testów podatności 2 (dwóch) stron internetowych.
6. System musi umożliwiać wielokrotne przeprowadzenie skanowania sieci komputerowej w celu identyfikacji/rozpoznania podłączonych urządzeń.
7. System musi umożliwiać wielokrotne przeprowadzenie skanowania podatności urządzeń w sieci komputerowej (serwery, przełączniki, dyski NAS, stacje robocze) w ilości 20 szt.
8. Rozwiązanie typu manager/konsola ma musi być dostępne w chmurowej (SaaS).
9. Rozwiązanie musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej.
10. Rozwiązanie musi oferować możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX.
11. Sonda skanująca musi wymagać rejestracji, w konsoli centralnej Security Center, przy użyciu wygenerowanego przez administratora sześcioznakowego tokena lub innego mechanizmu uwierzytelniania.
12. Konsola centralna musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
13. Administrator w konsoli centralnej musi posiadać możliwość dodania dodatkowych użytkowników zarządzających.
14. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.
15. Zarządzanie zestawami
16. Rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń i aplikacji webowych do skanowania.
17. Rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV.
18. Dodanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską.
19. Dodanie aplikacji webowej musi pozwalać na dodanie rodzaju autentykacji, białej i czarnej listy adresów URL oraz rozszerzeń do skanowania.
20. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z 4 poziomów: Neutralny, Niski, Średni i Wysoki (nazewnictwo przykładowe).
21. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru znaczników (tagów).
22. Administrator musi posiadać możliwość dodania znaczników (tagów) dynamicznych, które będą przypisywane do urządzeń po spełnieniu jednego z warunków: nazwy zestawu urządzeń, adresu IP z podanego zakresu, otwartych portów lub systemu operacyjnego.
23. Skanowanie sieciowe
24. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail.
25. Rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
26. Usługa skanowania sieci musi obsługiwać IPv6.
27. Rozwiązanie musi posiadać możliwość dodawania różnych profili skanowania sieciowego.
28. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
29. Funkcja wykrywania urządzeń w profilu skanowania, musi pozwalać na wybór domyślnych portów, dodanie dodatkowych portów, wybór rodzaju połączenia TCP SYN lub TCP SYN ACK oraz możliwość wyłączenia lub włączenia wysłania ICMP PING.
30. Rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
31. Rozwiązanie musi umożliwiać włączenia skanowania drukarek.
32. Rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach.
33. Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.
34. Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
35. Profil skanowania sieciowego musi posiadać możliwość wyboru intensywność skanowania.
36. Profil skanowanie sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
37. Rozwiązanie musi posiadać co najmniej 100 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
38. Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta.
39. Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
40. Urządzenia znalezione podczas zadania skanowania muszą zostać automatycznie dodane do listy urządzeń wraz z odpowiednimi znacznikami (tagami), przypisanymi na podstawie wykrytych portów usług oraz systemu operacyjnego.
41. Podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.
42. Skanowanie aplikacji webowych
43. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania aplikacji webowych.
44. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania aplikacji webowych.
45. Rozwiązanie musi posiadać możliwość skanowania aplikacji internetowych (skanowanie stron internetowych).
46. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail.
47. Rozwiązanie musi posiadać możliwość zapewnienia konfigurowalnych ustawień skanowania, takich jak ustawienia indeksowania do metody formularza: Post i Get, Post, Get.
48. Podczas tworzenia zadania skanowania aplikacji webowych, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie lub sondy zewnętrznej hostowanej w chmurze producenta.
49. Podczas tworzenia profilu skanowania aplikacji webowych administrator musi posiadać możliwość włączenia i wyłączenia wykonania testów „łamania” haseł typu brute force.
50. Rozwiązanie musi posiadać możliwość wyboru intensywności skanowania wydajności (wstępnie ustawiona na niską, średnią i wysoką) przez system.
51. Rozwiązanie musi posiadać możliwość włączenia pełnego zestawu kategorii wykrywania podatności, a także dostosowania kategorii wykrywania podatności do skanowania, a także listy wykluczeń.
52. Rozwiązanie musi posiadać możliwość wyboru opcji skanowania wrażliwych treści, numerów kart kredytowych i zezwalania na wprowadzanie niestandardowych treści.
53. Administrator musi posiadać możliwość uruchomienia zadania skanowania aplikacji webowej jednorazowo lub z harmonogramem.
54. Podatności wykryte podczas skanowania aplikacji webowych muszą automatycznie być umieszczane w menedżerze podatności.
55. Skanowanie agentowe
56. Rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przesyłać do konsoli centralnej listę zainstalowanych aplikacji.
57. Systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową.
58. Wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności.
59. Pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .msi.
60. Aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej, tokenu lub innej informacji uwierzytelniającej.
61. Zarządzanie aktywami
62. Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami:
    1. Oznaczanie (lista grupowania)
    2. Nazwa zasobu
    3. Liczba wykrytych podatności w zabezpieczeniach
    4. Najwyższa wykryta podatność
    5. Krytyczność/istotność dla Zamawiającego
    6. Informacje o systemie operacyjnym
    7. Data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu
63. Rozwiązanie musi posiadać możliwość przeglądania informacji o aktywach, takich jak:
    1. Sieć: Stan podatności - Aktywne, Ignorowane i Wyłączone.
    2. Sieć : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona
    3. Sieć: lista otwartych portów powiązanych z zasobem
    4. Sieć: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i przedziału czasu.
    5. Aplikacja internetowa : Stan podatności - Aktywne, Ignorowane i Wyłączone.
    6. Aplikacja internetowa : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona
    7. Aplikacja internetowa : Lista przeskanowanych i wykrytych map witryn
    8. Aplikacja webowa: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i interwału.
64. Potrafi zapewnić możliwość edycji informacji o aktywach, takich jak:
    1. Sieć: Aby podać nazwę zasobu (jeśli nie jest dostępny DNS).
    2. Sieć: aby podać etykietę wpływu biznesowego
    3. Sieć: Aby podać kolumnę wejściową dla opisu zasobu
    4. Sieć: możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO
    5. Aplikacja internetowa: Aby podać nazwę zasobu
    6. Aplikacja internetowa: Aby podać etykietę wpływu biznesowego
    7. Aplikacja internetowa: Aby zapewnić kolumnę wejściową dla opisu zasobu
    8. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO
    9. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość zapewnienia funkcji skanowania REST API
    10. Aplikacja internetowa: Może zapewnić zakres indeksowania, taki jak nazwa hosta adresu URL i podkatalog adresu URL. A także w stanie jawnie określić inne adresy URL
    11. Aplikacja webowa: Możliwość podawania nagłówków i plików cookie
    12. Aplikacja internetowa: może zapewnić uwierzytelnione skanowanie, takie jak HTTP Basic i HTTP Form
    13. Aplikacja internetowa: Może zapewnić elastyczność w utrzymywaniu listy wykluczających adresów URL, takich jak biała i czarna lista.
    14. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych luk w zabezpieczeniach powiązanych z zasobami aplikacji internetowej.
65. Rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych.
66. Rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii Network IP
67. Moduł kampanii phishingowych
68. Rozwiązanie musi posiadać możliwość utworzenia kampanii phishingowej i edukacyjnej.
69. Administrator musi posiadać możliwość utworzenia własnych profili phishingowych lub importu predefiniowanych przez producenta.
70. Profile kampanii phishingowych utworzone przez producenta muszą być dostępne w języku polskim.
71. Profil kampanii phishingowej powinien zawierać szablon wiadomości email lub wiadomości email i strony internetowej.
72. Rozwiązanie musi posiadać możliwość przypisania do profilu kampanii phishingowej kategorii domen, z których wysyłane będą wiadomości.
73. Kampanie phishingowe muszą posiadać możliwość wyboru czasu rozpoczęcia kampanii oraz czy wiadomości mają być wysyłane jednorazowo do wszystkich odbiorców, w grupach lub losowo w określonym zakresie czasu.
74. Platforma musi posiadać co najmniej 5 predefiniowanych szablonów kampanii:
    1. Polski: Wiadomości phishingowe - oszustwo związane z kontem e-mail
    2. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kontami e-mail
    3. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kartami kredytowymi
    4. Polski: Pobieranie plików - Office 365
    5. Polski: Phishing - Office 365
75. Administrator musi posiadać możliwość przypisania do kampanii phishingowej, kampanii edukacyjnej przeprowadzanej poprzez wysłanie wiadomości email i/lub strony internetowej.
76. Administrator musi posiadać możliwość utworzenia własnych profili edukacyjnych lub importu predefiniowanych przez producenta.
77. Profile kampanii edukacyjnych utworzone przez producenta muszą być dostępne w języku polskim i angielskim.
78. Rozwiązanie musi posiadać możliwość wyboru treści wiadomości edukacyjnej w zależności od podjętej przez odbiorcę czynności: otwarcia wiadomości, odpowiedzi na wiadomość, kliknięcia w link oraz wypełnienia formularza na stronie phishingowej.
79. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru treści prezentacji edukacyjnej w formie strony internetowej na której można zamieszczać treści edukacyjne w postaci tekstu, grafiki oraz wideo.
80. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru testu sprawdzającego wiedzę w formie strony internetowej na której można zamieszczać pytania i odpowiedzi w formie jednokrotnego i wielokrotnego wyboru.
81. Rozwiązanie musi posiadać możliwość anonimizacji danych odbiorców i podjętych przez nich czynności.
82. Menadżer podatności
83. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami:
    1. Wyniki skanowania podatności sieci według ważności (z opcjami wykresów)
    2. Wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresów)
    3. Otwarte zgłoszenia według ważności (z opcjami wykresów)
    4. Top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP / tagów)
    5. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety)
    6. Zgodność z OWASP (z opcjami wykresów : Słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych)
    7. Ostatnie skanowania
    8. Nadchodzące skanowania
    9. Ostatnie 10 raportów
    10. Liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji Ips / Web / tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał)
    11. Ocena wyników kampanii phishingowych
    12. Ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień)
84. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności
    1. Możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów:
    2. Według stanu : Wszystkie, Nie ignorowane/wyłączone i ignorowane/wyłączone.
    3. Według typu: Host i aplikacja internetowa
    4. Według statusu : Nowy, Aktywny, Ponownie otwarty, Naprawiony
    5. Według ważności : Informacja, Niski, Średni, Wysoki, Krytyczny
    6. Według tagów (opcja uwzględnienia/wykluczenia tagu)
    7. Według pierwszego i ostatniego wykrycia
    8. Według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych
    9. Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych / hosta.
    10. Możliwość tworzenia raportów bezpośrednio z Menedżera podatności poprzez wybranie jednej lub więcej podatności.
    11. Możliwość dalszego administrowania / zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji:
    12. Co ignorować: Wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i Ignoruj tę podatność.
    13. Powód ignorowania : Fałszywie dodatni, Ryzyko zaakceptowane, Nieistotne
    14. Opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności
    15. Możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu
    16. Możliwość tworzenia czatu konwersacyjnego do celów współpracy między użytkownikami
    17. Opcja wyświetlania następujących informacji na temat podatności -

i. Wpływ

ii. Rozwiązanie

iii. Podsumowanie

iv. Wgląd

v. Wykrywanie

vi. Odniesienie

vii. Łatki

viii. Możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach

ix. Środki zaradcze

1. Możliwość dostarczania informacji o zgłoszeniach, takich jak:
   1. Numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej.
   2. Możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak : Otwarte, Zamknięte lub Rozwiązane
   3. Możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami
   4. Możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia
   5. Możliwość przypisania do wyznaczonego właściciela i terminu płatności
   6. Możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami:
   7. Status
   8. Typ zasobu
   9. Kategoria usługi
   10. Tagi
   11. Termin płatności
   12. Kategoria skanowania sieci i aplikacji internetowych
   13. Istotność
   14. System operacyjny
   15. Porty
   16. Właściciel
   17. Potrafi zapewnić proaktywną obsługę zgłoszeń opartą na zasadach
2. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.
3. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.
4. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.
5. System raportujący

System raportujący musi zawierać następujące raporty:

1. Skanowanie sieci
2. Aplikacja sieciowa
3. Łatki
4. Środki zaradcze
5. Ocena phishingu e-mail
6. Porównanie (raport Delta)
7. Zgodność
8. Raporty zgodności: Musi być w stanie wygenerować następujący typ zgodności:
   1. Ustawa o ochronie danych osobowych
   2. ISO / IEC 27001
   3. Ogólne rozporządzenie o ochronie danych
   4. Bezpieczeństwo sieci i informacji
9. System powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez rząd, gdy ma to zastosowanie.
10. Rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami:
    1. Raport oparty na określonym czasie skanowania
    2. Raport oparty na wszystkich bieżących informacjach o podatnościach
    3. Raport trendów z historią podatności
    4. Zawartość raportu : Szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu do 500 znaków.
    5. Sposób prezentacji raportu: Podatności według ważności w czasie, Podatności według statusu, Podatności według ważności, 5 najbardziej narażonych kategorii
    6. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności
11. Potrafi utworzyć i dostosować szablon raportu aplikacji internetowej z następującymi opcjami:
12. Raport oparty na określonym czasie skanowania
13. Raport oparty na wszystkich bieżących informacjach o podatnościach
14. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności
15. Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty mają byc dostarczane kanałem e-mail.

**ETAP II**

1. **Most bezprzewodowy do archiwum odmiejscowionego (1 szt., tj. 2 szt. anten z uchwytami)**
2. Minimalne parametry techniczne urządzenia

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania** |
| Interfejs sieciowy | 2 porty RJ45 GbE |
| Zasilanie | PoE |
| Zasilacz | Dołączony |
| Maksymalne zużycie mocy | 8,5W |
| Moc | 19 dBi |
| Polaryzacja | Podwójna liniowa |
| Częstotliwość pracy | 5 MHZ |
| Przepustowość | 450+ Mbps |
| Zasięg | 5 km |
| Zarządzanie | Indywidualne (bez konieczności stosowania kontrolera) |
| Gwarancja | 24 miesiące |

1. Zakres instalacji i konfiguracji

* urządzenie należy rozpakować i uruchomić w siedzibie Zamawiającego,
* do urządzeń należy dołączyć niezbędne zasilacze, przewody oraz uchwyty,
* urządzenia należy zamontować w miejscach (lokalizacjach) wskazanych przez Zamawiającego,
* należy dokonać wstępnej konfiguracji połączenia, sieci VLAN oraz sieci zarządzającej zgodnie z wytycznymi służb informatycznych Zamawiającego.

1. **Oprogramowanie NAC (Network Access Control)**
2. Minimalna funkcjonalność

**Podstawowa funkcjonalność 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 99 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 300 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
    * 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, 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, 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, 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 obsługi 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 wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
38. System musi posiadać funkcję personalizacji strony gościnnej.
39. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
40. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
41. 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.
42. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
43. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
45. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
46. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
47. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
48. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
49. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
50. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
51. 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.
52. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
53. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
54. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
55. 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.
56. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
57. 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.
58. 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
59. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
60. System musi współpracować z serwerem tokenów.
61. 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
62. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
63. 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 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, MicroTik, Ubiquiti Networks, DCN.
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).

**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.
4. Zakres instalacji i konfiguracji

* Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku Zamawiającego.
* Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
* Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
* Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
* Integracja urządzeń sieciowych (switche, AP itp.) z systemem NAC (jeżeli urządzenia te wspierają niezbędne funkcjonalności).
* Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy (jeżeli urządzenia te wspierają niezbędne funkcjonalności).
* Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
* Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.
* Wykonawca zapewni 8-godzinne warsztaty w zakresie użytkowania i administrowania wdrożonym systemem NAC.
* Warsztaty mogą się odbyć w formie zdalnej.
* Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
* Szczegółowy plan, zakres i termin warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.
* Wraz dożywotnią licencją systemu NAC Wykonawca dostarczy licencję na wsparcie obowiązującą do dnia 25.06.2026 roku, w ramach której Wykonawca zapewni:
* 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.

**DOTYCZY ETAPU I i II**

**Prace konfiguracyjne i wdrożeniowe oraz pozostałe wymagania**

1. Wszystkie dostarczane przez Wykonawcę urządzenia klasy UTM muszą pochodzić od jednego producenta.
2. W przypadku gdy podłączenie urządzeń w miejscu wskazanym przez Zamawiającego będzie niemożliwe ze względu na brak gniazd zasilających Wykonawca zobowiązany jest dostarczyć listwę zasilającą RACK lub zwykłą (w zależności od potrzeb).
3. Zakres prac obejmuje w szczególności:
4. dostawę kompletnego sprzętu wraz niezbędnym do jego działania oprogramowaniem oraz przewodami,
5. przygotowanie dokumentacji powykonawczej wdrożenia,
6. zapewnienie wsparcia technicznego dla Zamawiającego z zakresu eksploatacji i konfiguracji urządzeń przez okres wskazany w ofercie (minimum 1 miesiąc).
7. Zamawiający wymaga aby czynności związane z konfiguracją przełączników zarządzalnych i urządzeń UTM oraz testami bezpieczeństwa wykonywane były przez lokalnego Administratora Systemu Informatycznego pod nadzorem osoby realizującej wdrożenie ze strony Wykonawcy.
8. Sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, **wyprodukowany** **nie wcześniej niż w 2024 roku**, dostarczony w oryginalnym opakowaniu (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Zamawiający nie dopuszcza zastosowania urządzeń tzw. „refurbished”.
9. Dostarczone oprogramowanie ma być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych.
10. Oprogramowanie wszystkich urządzeń musi być zaktualizowane do najnowszej dostępnej wersji a jego licencja musi umożliwiać dostęp do bezpłatnych aktualizacji w okresie do dnia 25.06.2026 roku**.**
11. Zamawiający zastrzega możliwość przeprowadzenia weryfikacji oryginalności dostarczonego sprzętu i oprogramowania u producenta w przypadku wystąpienia wątpliwości co do jego legalności.
12. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dokumentację powykonawczą (powdrożeniową, użytkową) zawierającą m.in. opis systemu, funkcjonalności, zależność pomiędzy wszystkimi jego elementami, opis sposobu konfiguracji wraz z wykazem niezbędnych licencji. Dodatkowo do dokumentacji należy dołączyć, o ile zajdzie taka konieczność, rejestr dostępu w czasie prac do miejsc ograniczonego dostępu.