ZAŁĄCZNIK NR 2 DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

**„ZAKUP SYSTEMU ZABEZPIECZEŃ SIECIOWYCH– 2 ZADANIA”**

(nr postępowania ZP/3/IX/2022)

# Spis treści

[1 Spis treści 2](#_Toc115184358)

[2 Słownik i skróty 3](#_Toc115184359)

[3 Przedmiot zamówienia 5](#_Toc115184360)

[4 Opis wymagań 5](#_Toc115184361)

[4.1 Wymagania dotyczące NAC (ZADANIE NR 1) 5](#_Toc115184362)

[4.2 Load Balancer wraz z funkcjonalnością WAF (ZADANIE NR 2) 16](#_Toc115184363)

[5 Wymagania dodatkowe – godziny inżyniera (dotyczy ZADANIA NR 1) 27](#_Toc115184364)

[6 Wymagania dodatkowe (dotyczy ZADANIA NR 1 i ZADANIA NR 2) 28](#_Toc115184365)

[7 Świadczenie serwisu gwarancyjnego i gwarancji. 28](#_Toc115184366)

[8 Zasady odbioru przedmiotu zamówienia (dotyczy ZADANIA NR 1 i ZADANIA NR 2) 29](#_Toc115184367)

# Słownik i skróty

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

| **Skrót/pojęcie** | **Definicja** |
| --- | --- |
| **Awaria** | Oznacza Awaria Krytyczna i/lub Awaria Niekrytyczna i/lub Awaria Zwykła. |
| **Awaria Krytyczna** | Oznacza brak działania środowiska produkcyjnego zakupionych rozwiązań NAC i WAF, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Awarie Krytyczne mają jedną lub więcej z poniższych cech: 1. dane biznesowe zostały uszkodzone;
2. System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji;
3. wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na:
4. uwierzytelnianie,
5. niezaprzeczalność,
6. poufność,
7. integralność,
8. dostępność,
9. rozliczalność;

wszelkie awarie związane z bezpieczeństwem dostępu do rozwiązania (w tym nieautoryzowanym dostępem do danych). |
| **Awaria Zwykła** | Utrudnia działanie rozwiązania w środowisku produkcyjnym w zakresie Funkcjonalności Krytycznej i uniemożliwia działanie rozwiązania w zakresie pozostałych funkcjonalności. W tym kontekście „utrudnia” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez Wykonawcę procedury tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji, (co może mieć wpływ na wygodę w użytkowaniu rozwiązania lub wymagać procedur ręcznych). „Uniemożliwia” oznacza brak możliwości jego obejścia. |
| **Dokumentacja**  | Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności wykaz ilościowo-cenowy. |
| **Zlecenie** | Zapotrzebowanie na prace inżyniera przekazane Wykonawcy przez Zamawiającego |
| **SLA** | Poziom dostępności usług (*Service Level Agreement).* |
| **Umowa** | Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia. |
| **Usługa Wsparcia technicznego** | Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania zakupionego w ramach postępowania rozwiązania oraz jego poszczególnych komponentów wraz dostępem do usługi wsparcia technicznego realizowanego przez producenta Oprogramowania oraz dostępem do aktualizacji dla Oprogramowania. |
| **Użytkownik** | Zamawiający oraz jego pracownicy. |
| **Wykonawca** | Podmiot realizujący zamówienie. |
| **Zamawiający/LPR** | Lotnicze Pogotowie Ratunkowe. |

# Przedmiot zamówienia

Przedmiotem zamówienia jest zakup licencji Oprogramowania na:

* ZADANIE NR 1: Network Access Control (NAC) umożliwiające uwierzytelnienie oraz autoryzacje urządzeń w sieci LAN, a także uwierzytelnienie i autoryzację administratorów urządzeń – rozwiązanie złożone z 2 urządzeń w wersji wirtualnej obsługujący 800 sesji urządzeń końcowych oraz 2 urządzeń dla uwierzytelniania administratorów;
* ZADANIE NR 2: Load Balancer z funkcją Web Access Firewall (WAF) w celu rozbudowy mechanizmów zabezpieczeń obecnie posiadanej infrastruktury – rozwiązanie złożone z 1 urządzenia w wersji wirtualnej obsługującej do 200Mbps ruchu z funkcją loadbalansera;
* ZADANIE NR 1 I 2: Dedykowane szkolenia z administrowania przedmiotem Zamówienia dla min. 2 pracowników Zamawiającego

Oprogramowanie będzie objęte gwarancją i wsparciem technicznym przez okres 3 lat od dnia podpisania protokołu ilościowo-jakościowego dostawy.

Wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Zamawiający wymaga, aby Wykonawca posiadał aktualny certyfikat Systemu Zarządzania Jakością ISO 9001 (lub równoważny odpowiednik) na projektowanie, produkcję, instalowanie i serwis systemów teleinformatycznych, informatycznych, telekomunikacyjnych lub wdrożył standardy lub normy zarządzania jakością w oparciu o standard ISO lub równoważny odpowiednik.

# Opis wymagań

## Wymagania dotyczące NAC (ZADANIE NR 1)

Rozwiązanie zapewni:

1. pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu;
2. wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń;
3. kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń;
4. uwierzytelnienie oraz autoryzację oraz rozliczalność działań administratorów w infrastrukturze sieciowej;

Tabela 1 Specyfikacja pojedynczego kompletu

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Numer produktu** | **Opis** | **Ilość** |
| 2 | ISE-A-LIC | Cisco Identity Service Engine Advantage Subscription | 800 |
| 4 | **L-ISE-TACACS-ND=** | Cisco ISE Device Admin Node License | 2 |
| 5 | **R-ISE-VMC-K9=** | Cisco ISE Virtual Machine Common PID | 2 |

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Tabela 2 Wymagania dla rozwiązania równoważnego

| **Kod wymagania** | **Opis wymagań** |
| --- | --- |
| **Podstawowe cechy rozwiązania** |
|  | Rozwiązanie umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych |
|  | Rozwiązanie umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych |
|  | Rozwiązanie umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń |
|  | W scenariuszu, w którym wszystkie komponenty rozwiązania znajdują się na pojedynczym serwerze jest on w stanie obsłużyć następującą liczbę jednoczesnych sesji: 800 sesji |
|  | Rozwiązanie umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym na systemach:* VMware wersji 7 dla ESXi 6.7 lub wyższej
* WMware Cloud w AWS
* Azure VMware Solution
* hypervisorze KVM na Red Hat Enterprise Linux (RHEL)
* Microsoft Hyper-V
* AWS EC2
* serwerach fizycznych wspieranych przez producenta
 |
|  | Rozwiązanie umożliwia wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:* Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji rozwiązania oraz jego monitorowanie
* Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
* przełączników dostępowych
* sesji uwierzytelniania 802.1X
* zdarzeń kontroli dostępu (autoryzacji)
* zdarzeń związanych z błędami
* zdarzeń związanych z alarmami systemowymi
* Wydzielenie serwerów usługowych realizujących funkcje:
* serwera RADIUS dla infrastruktury sieciowej
* serwera polityk uwierzytelniania i kontroli dostępu 802.1X
* serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
* serwera profilowania stacji końcowych
 |
|  | Rozwiązanie m umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym:* zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
* zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
 |
|  | Rozwiązanie umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS. |
|  | Rozwiązanie umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback). |
|  | Rozwiązanie umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled). |
|  | Rozwiązanie umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników. |
|  | Rozwiązanie umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0. |
|  | Rozwiązanie umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. Rozwiązanie wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni |
|  | Rozwiązanie umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:* dostęp do interfejsu konfiguracji usług tożsamości 802.1X
* dostęp do interfejsu konfiguracji urządzeń sieciowych
* dostęp do interfejsu konfiguracji polityk
* dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
* dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
 |
|  | Rozwiązanie umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP. |
|  | Rozwiązanie posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520. |
|  | Rozwiązanie wspiera REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych.  |
|  | Rozwiązanie wspiera REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych. |
|  | Rozwiązanie wspiera REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików. |
| **Mechanizmy uwierzytelniania 802.1x** |
|  | Rozwiązanie wspiera następujące protokoły uwierzytelniania i standardy:* RADIUS, zgodnie z dokumentami:
* RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
* RFC 2139 — RADIUS Accounting
* RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
* RFC 2866 — RADIUS Accounting
* RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
* RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
* RFC 2869 — RADIUS Extensions
 |
|  | RADIUS Proxy dla zewnętrznego serwera RADIUS |
|  | Rozwiązanie wspiera protokół Windows Active Directory, w tym następujące repozytoria AD:* Microsoft Windows Active Directory 2012 R2
* Microsoft Windows Active Directory 2016
* Microsoft Windows Active Directory 2019
 |
|  | Rozwiązanie wspiera protokół Lightweight Directory Access Protocol (LDAP) |
|  | Rozwiązanie wspiera protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO). |
|  | Rozwiązanie wspiera integrację z Azure Active Directory z użyciem technologii Oauth ROPC w celu uwierzytelnienia klientów 802.1x. |
|  | Rozwiązanie wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865 |
|  | Rozwiązanie wspiera następujące protokoły uwierzytelniania:* PAP/ASCII
* CHAP
* MS-CHAPv1
* MS-CHAPv2
* EAP-MD5
* LEAP
* EAP-TLS
* EAP-TTLS
* Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
* EAP-MS-CHAPv2
* EAP-GTC
* EAP-TLS
* Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi:
* EAP-MS-CHAPv2
* EAP-TLS
 |
|  | Rozwiązanie umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect |
|  | Rozwiązanie wspiera implementację 802.1X z przynajmniej następującymi suplikantami:* wbudowanym klientem 802.1X dla Windows 10
* wbudowanym klientem 802.1X dla Windows 7
* wbudowanym klientem 802.1X dla Windows 8 i 8.1
* Apple Mac OS X Supplicant
* Apple iOS Supplicant
* Google Android Supplicant
 |
|  | Rozwiązanie umożliwia tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based). |
|  | Rozwiązanie umożliwia uwierzytelnianie 802.1X maszyn i użytkowników. |
|  | Rozwiązanie umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły. |
|  | Rozwiązanie posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym) |
|  | Rozwiązanie posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.  |
|  | Rozwiązanie wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC |
|  | Rozwiązanie wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD – Network Access Devices), w tym:* tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port,
* tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia,
* tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden host w domenie danych (Data VLAN) na jednym porcie fizycznym,
* tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym,
* mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny,
* mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym,
* mechanizm umożliwiający wysłanie informacji o restarcie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA,
* mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X,
* mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X,
* obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki,
* mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLAN’ie (Guest VLAN) dla użytkowników gościnnych,
* mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny,
* przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLAN’ów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
* uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLAN’ie głosowym,
* współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN,
* możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web,
* możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznik.
 |
|  | Rozwiązanie wspiera uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X) |
| **Realizacja dostępu gościnnego** |
|  | Rozwiązanie umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:* Microsoft Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7,
* Apple Mac OS X 10.x oraz 11.x,
* Apple iOS 11.x, 12.x, 13.x i nowszych,
* Google Android dla wersji 7.x i nowszych,
* Linux.
 |
|  | Rozwiązanie umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor). |
|  | Rozwiązanie zapewnia uwierzytelnienie sponsora, które musi odbywać sekwencyjnie w oparciu o:* wewnętrzną bazę użytkowników,
* zewnętrzne repozytorium użytkowników.
 |
|  | Rozwiązanie umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:* logowania się do rozwiązania,
* tworzenia pojedynczego konta gościnnego,
* tworzenia wielu kont gościnnych,
* importowania kont gościnnych z pliku CSV,
* wysyłania wiadomości email po utworzeniu konta gościnnego,
* wysyłania wiadomości SMS po utworzeniu konta gościnnego,
* wyświetlenia hasła konta gościnnego,
* wydrukowania danych konta gościnnego,
* wyświetlenia danych stworzonych kont gościnnych,
* zawieszenia (suspend) i reinicjacji kont gościnnych.
 |
|  | Rozwiązanie umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:* zmianę logo strony logowania,
* zmianę obrazu tła strony logowania,
* zmianę logo bannera,
* zmianę obrazu tła bannera,
* zmianę koloru tła strony z treścią.
 |
|  | Rozwiązanie umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS |
|  | Rozwiązanie umożliwia zmianę adresu URL i FQDN strony sponsora. |
|  | Rozwiązanie umożliwia automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. Rozwiązanie umożliwia wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych |
|  | Rozwiązanie posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim |
|  | Rozwiązanie umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim. |
|  | Rozwiązanie umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:* Imienia,
* Nazwiska,
* Firmy,
* adresu e-mail,
* numeru telefonu,
* danych opcjonalnych (nie mniej niż 5 dodatkowych pól).
 |
|  | Rozwiązanie umożliwia konfigurację dla użytkowników gościnnych:* wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP),
* zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,
* samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora.
 |
|  | Rozwiązanie umożliwia honorowanie ustawień local przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego. |
|  | Rozwiązanie umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego. |
|  | Rozwiązanie umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 20 urządzeń per konto gościnne. |
|  | Rozwiązanie umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach. |
|  | Rozwiązanie umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny |
|  | Rozwiązanie umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych: |
|  | Rozwiązanie umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika |
|  | Rozwiązanie umożliwia tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu. |
|  | Rozwiązanie umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN. |
|  | Rozwiązanie umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS,  |
|  | Rozwiązanie umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora. |
|  | Rozwiązanie wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych. |
| **Profilowanie urządzeń** |
|  | Rozwiązanie umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu. |
|  | Rozwiązanie umożliwia wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności zapewnia możliwość stworzenia polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc. |
|  | Rozwiązanie umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:* DHCP,
* DHCP SPAN,
* http,
* RADIUS,
* DNS,
* SNMP,
* Network Scan (NMAP lub inne narzędzie profilowania aktywnego).
 |
|  | Rozwiązanie umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji. |
|  | Rozwiązanie umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy. |
|  | Rozwiązanie posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:* Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
* Urządzeń mobilnych: Android, Apple, Blackberry,
* Telefonów IP,
* Drukarek sieciowych,
* Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych,
* Routerów,
* Punktów dostępu bezprzewodowego.
 |
|  | Rozwiązanie umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:* reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci,
* reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt>.
 |
|  | Rozwiązanie umożliwia włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie. |
|  | Rozwiązanie wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta. |
| **Wymiana informacji kontekstowych oraz automatyzacji odpowiedzi** |
|  | Rozwiązanie umożliwia wymianę informacji kontekstowych dotyczących sesji użytkowników oraz urządzeń. Wymiana ta może występować w obu kierunkach –NAC może zarówno udostępniać informacje jak i przyjmować je z zewnętrznych systemów producenta oraz firm trzecich.  |
|  | Wymiana informacji realizowana jest z użyciem dedykowanej szyny wymiany informacji w architekturze Consumer-Provider, opartej o technologie REST oraz Websocket. NAC pełni rolę serwera wymiany informacji.  |
|  | Wymiana informacji może zostać skonfigurowana z kilkudziesięcioma rodzajami systemów klasy enterprise, m.in.: next-generation firewall, network detection and response (NDR)/flow monitoring, Security Information Event Management (SIEM), IoT Security, DNS, DHCP and IP (DDI) management, skanowania/zarządzania podatnościami.  |
|  | Rozwiązanie umożliwia zmianę autoryzacji stacji w oparciu o dyspozycje otrzymane poprzez szynę wymiany informacji. Zmiana autoryzacji może spowodować m.in. przeniesienie stacji do VLAN’u kwarantanny o ograniczonym dostępie do sieci lub dezaktywację portu, do którego podłączona jest stacja w celu odcięcia jej dostępu do sieci.  |
| **Obsługa serwerów certyfikatów CA** |
|  | Rozwiązanie posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.  |
|  | Funkcja CA umożliwia wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy protokołu EAP-TLS. |
|  | Rozwiązanie wspiera hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów. |
|  | Funkcja CA zapewnia przynajmniej następujące funkcjonalności:* Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS,
* Key Management: generacja i bezpieczne przechowywanie kluczy, i certyfikatów w modelu rozproszonym,
* Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji,
* Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA.
 |
| **Raportowanie** |
|  | Rozwiązanie umożliwia generowanie m.in. następujących raportów:* raportów dla protokołów AAA:
* diagnostyki protokołów AAA
* trendów uwierzytelnienia 802.1X
* accountingu RADIUS
* uwierzytelniania RADIUS
* raportów dozwolonych protokołów
* sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
* uwierzytelnień pomyślnych
* uwierzytelnień nieudanych
* „N” największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
* uwierzytelnień pomyślnych
* uwierzytelnień nieudanych
* raportów dla poszczególnych instancji serwerów składających się na kupowane Rozwiązanie, w tym:
* uwierzytelnień RADIUS per serwer
* Top „N” uwierzytelnień per serwer
* monitorowania Online Certificate Status Protocol (OCSP)
* administratorów systemu i ich uprawnień
* logowania administratorów do systemu
* zmian konfiguracji serwera dokonanych przez administratorów
* stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
* zmian operacyjnych serwera dokonanych przez administratorów
* zmian haseł przez użytkowników
* raportów dla stacji końcowych, w tym:
* uwierzytelnień typu MAC Authentication
* Top „N” uwierzytelnień per adres MAC stacji
* Top „N” uwierzytelnień per maszyna
* Top „N” uwierzytelnień per RADIUS Calling Station ID
* działań podsystemu profilera per adres MAC
* czasu wymaganego na sprofilowanie stacji per adres MAC
* raportów dla błędów, w tym:
* błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
* sumarycznych przyczyn nieudanych uwierzytelnień
* Top „N” uwierzytelnień per rodzaj błędu
* raportów dla urządzeń sieciowych:
* sumarycznych uwierzytelnień dla urządzeń sieciowych
* Top „N” uwierzytelnień per urządzenie sieciowe
* niedostępności serwera AAA dla urządzenia sieciowego
* wiadomości logowanych przez urządzenia sieciowe
* stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
* raportów użytkowników:
* sumarycznych uwierzytelnień użytkowników
* Top „N” uwierzytelnień per użytkownik
* sesji użytkowników gościnnych
* aktywności użytkowników gościnnych
* sumarycznych uwierzytelnień sponsorów dostępu gościnnego
* uwierzytelnień per unikalny użytkownik
* raportów katalogu sesji
* aktywnych sesji RADIUS
* historii sesji RADIUS
* za terminowanych sesji RADIUS
 |
| **Alarmy i diagnostyka** |
|  | Rozwiązanie umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:* wiadomości e-mail,
* syslog.
 |
|  | Alarmy mogą być generowane w następujących sytuacjach:* ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu,
* opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego,
* status krytycznych procesów będzie niepożądany, w tym status:
* procesu wewnętrznej bazy danych systemu,
* serwera aplikacyjnego systemu,
* bazy danych sesji,
* kolektora i procesora wiadomości log,
* błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej),
* stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
* obciążenie systemu (load),
* zajętość pamięci.
 |
|  | Rozwiązanie posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:* badanie łączności IP za pomocą ping, nslookup, traceroute,
* 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,
* ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
* definicji serwerów AAA,
* protokołu RADIUS,
* odkrywania urządzeń,
* logowania,
* uwierzytelniania Web,
* konfiguracji trybu 802.1X,
* wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu.
 |
| **Wsparcie dla protokołu IPv6** |
|  | Rozwiązanie posiada wsparcie dla SSH IPv6 |
|  | Rozwiązanie pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6 |
|  | Rozwiązanie pozwala na konfigurację NTP IPv6 |
|  | Rozwiązanie umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6 |
|  | Rozwiązanie umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6 |
|  | Rozwiązanie umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6 |
|  | Rozwiązanie umożliwia integrację z Active Directory w oparciu o IPv6 |
|  | Rozwiązanie umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6 |
| **Administrowanie urządzeniami sieciowymi** |
|  | Rozwiązanie umożliwia aktywację serwera TACACS+ na wszystkich lub wybranych maszynach (wirtualnych bądź fizyczych) będących jego częścią. |
|  | Serwer TACACS+ umożliwia uwierzytelnienie administratorów urządzeń sieciowych (np. przełączników oraz ruterów) oraz autoryzację zgodną ze skonfigurowaną na rozwiązaniu NAC polityką. |
|  | Polityki TACACS+ umożliwiają m.in. określenie czy określony w polityce administrator bądź grupa administratorów, dla określonych urządzeń, otrzyma pełne przywileje operacyjne i konfiguracyjne czy też ich ograniczony zakres (np. możliwość wykonywania tylko określonych komend). |
| **Dobre praktyki realizacji rozwiązań** (rozwiązanie spełnia następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci) |
|  | Rozwiązanie może występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.  |
|  | W przypadku zastosowania rozwiązania złożonego z kilku komponentów rozwiązanie zapewnia pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN.  |
|  | Niezależnie od tego czy NAC występuje w formie pojedynczego rozwiązania, czy jest złożony z kilku komponentów, może on być serwisowany jako jedno rozwiązaniew ramach pojedynczej usługi wsparcia |

## Load Balancer wraz z funkcjonalnością WAF (ZADANIE NR 2)

Tabela 3 Specyfikacja pojedynczego kompletu

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Numer produktu** | **Opis** |
| 1 | F5-BIG-LTM-VE200MV18 | BIG-IP Virtual Edition Local Traffic Manager 200 Mbps (v12.1.x – v18.x) |
| 2 | F5-ADD-BIG-AWFVE200M | BIG-IP Virtual Edition Advanced Web Application Firewall Add-on License 200 Mbps |
| 3 | F5-SVC-BIG-VE-STDL13 | Level 1-3 Standard Service for BIG-IP Virtual Edition (10x5) |

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Tabela 4 Wymagania na system równoważny

| **Kod wymagania** | **Opis wymagań** |
| --- | --- |
| **Podstawowe cechy rozwiązania loadbalanser** |
|  | Rozwiązanie musi realizować co najmniej następujące funkcjonalności:* Rozkład ruchu pomiędzy serwerami aplikacji Web,
* Selektywny http caching,
* Selektywna kompresja danych,
* Terminowanie sesji SSL,
* Optymalizacja i akceleracja aplikacji,
* Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http,
* Ukrywanie zasobów,
* Zmiana odpowiedzi serwera,
* Przepisywanie odpowiedzi (response rewriting),
* Ochrona przed atakami typu SYN Flood
* Multipleksowanie połączeń http
 |
|  | Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia |
|  | Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej |
|  | Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:* Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów,
* Obsługa (parsowanie, modyfikacja, kreowanie odpowiedzi) protokołów: http, http2, WebSocket, DNS, rtsp, sip, RADIUS, DIAMETER,
* Język skryptowy musi umożliwiać dynamiczne przypisanie polityki bezpieczeństwa aplikacyjnego w oparciu o dowolną kombinację atrybutów http, SSL/TLS.Parsowanie parametrów komunikacji TLS/SSL, w szczególności odczyt certyfikatów X.509 i wstrzykiwanie odczytanych parametrów w formie nagłówków http,
* Możliwość zdefiniowania reakcji na zagrożenie wykryte przez Web Application Firewall na podstawie danych dostarczonych przez WAF, odczytanych w komunikacji http, SSL, WebSocket oraz historycznych atrybutów konfiguracji (kontekstu)
 |
|  | Rozwiązanie musi pracować w trybie pełnego proxy. |
|  | Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania. |
| **Funkcjonalność lokalnego równoważenia obciążenia** |
|  | Rozwiązanie musi posiadać co najmniej następujące metody równoważenia obciążenia:* cykliczna
* ważona
* najmniejsza liczba połączeń
* najszybsza odpowiedź serwera
* najmniejsza liczba połączeń i najszybsza odpowiedź serwera
* najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie
* dynamicznie ważona oparta na SNMP/WMI
* definiowana na podstawie grupy priorytetów dla serwerów
* musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego
 |
|  | Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera |
|  | Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP TCP echo, TCP (możliwość zdefiniowania payloadu wysyłanego/odbieranego), TCP half-open, UDP (możliwość zdefiniowania payloadu wysyłanego/odbieranego), http/https, http2, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, LDAP, DNS, MQTT, SIP, POP3, IMAP, SMB, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług |
|  | Określanie stanu serwera na podstawie pasywnej obserwacji odpowiedzi na requesty produkcyjne |
|  | Rozwiązanie musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów:* cookie (hash, rewrite, custom, insert, passive), w tym możliwość bazowania na ciastku aplikacji lub jego części
* system powinien szyfrować cookie generowane w celu zachowania przywiązania sesji
* adres źródła
* SIP call ID
* identyfikator sesji SSL
* Microsoft Terminal Services (RDP) – nazwa użytkownika
* adres docelowy
* tworzone przez administratora systemu przy wykorzystaniu języka skryptowego
 |
|  | Wsparcie dla usług warstw 4 – 7: * inspekcja warstwy 7
* wstrzykiwanie nagłówków http
* ukrywanie zasobów
* zmiana odpowiedzi serwera
* zaszyfrowane cookies
* kierowania żądań do odpowiedniej pooli zasobów, adresów IP/portów
* przepisywanie odpowiedzi (response rewriting)
* ochrona SYN Flood
* multipleksacja zapytań HTTP
* kompresja i cache’owanie http
 |
|  | Wsparcie dla HTTP/2, w tym wsparcie dla kompresji nagłówków |
|  | Rozwiązanie musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer. |
|  | Rozwiązanie musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS. |
| **Optymalizacja i akceleracja aplikacji** |
|  | Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci:* LAN
* WAN
* Urządzenia mobilne
 |
|  | Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta. |
|  | Urządzenie musi mieć możliwość strojenia profili połączeń TCP, w tym co najmniej:* Ustawienia timeout idle
* keep alive interval
* zero window timeout
* Initial Receive Window Size
* Wyboru algorytmu wykrywania natłoku.
* Wsparcia hybrydowych algorytmów wykrywania natłoku, opartych o stratę pakietów i round-trip-time
* Mechanizmu rate pacing
* określenia maksymalnej wielkości bufora per połączenie TCP celem ochron przed wysyceniem pamięci
* określenia maksymalnego bofora wysyłania i odbioru (send/receive buffer)
 |
|  | Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control) |
|  | Urządzenie musi umożliwiać selektywne cachowanie zwracanego kontentu a cachowanie powinno być zależne od:* Listy URN-ów i prefixów URN-ów, z których zwracany jest kontent,
* Maksymalnej wielkości zwracanego obiektu,
* Minimalnej wielkości zwracanego obiektu.
 |
|  | Powinna istnieć możliwość ograniczania wielkości cachu, ilości cachowanych obiektów celem ochrony pamięci urządzenia przed przepełnieniem. |
|  | Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP |
|  | Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:* Listy dozwolonych URI,
* Listy wykluczonych URI,
* Listy kompresowalnych Content-Type,
* Listy wykluczonych Content-Type,
* Minimalnej wielkości zwracanego obiektu.
 |
| **Kierowanie ruchu do odpowiedniej pool’i zasbów** |
|  | Urządzenie powinno realizować mechanizm kierowania żądań od użytkowników końcowych do pool (grup) zasobów serwerowych na podstawie następujących atrybutów:* Wartości http hostname, początku/końca nagłówka hostname, ciąg znaków znajdujący się w nagłówku hostname,
* Port,
* metody http,
* nazwy cookie, ciągu znaków na początku/końcu nazwy cookie, ciągu znaku zawartego w nazwie cookie,
* URN-a, oraz ciągu znaków występujących na początku/końcu lub zawartych w URN-ie,
* User agent,
* Dowolnego nagłówka lub kombinacji nagłówków,
* Wykorzystania cipherów w TLS,
* Common Name Klienta, oraz ciągu znaków występujących na początku/końcu lub zawartych w Common Name.
 |
|  | Reguły kierowania żądań powinny wymuszać co najmniej następujące akcje:* Wybór pooli zasobów (grupy IP adresów i portów)
* Kierowania żądania do konkretnego adresu IP
* redyrekcji
 |
|  | Rozwiązanie musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów. |
|  | Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy.  |
|  | Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów. |
|  | Wsparcie dla protokołu TLS 1.3. |
|  | Rozwiązanie musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów |
|  | Rozwiązanie musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL |
|  | Rozwiązanie musi obsługiwać sieci VLAN w standardzie 802.1q |
|  | Rozwiązanie musi obsługiwać agregację linków w standardzie 802.3ad (LACP) |
|  | Rozwiązanie musi obsługiwać Jumbo Frames |
|  | Rozwiązanie musi posiadać funkcjonalność bramy VXLAN oraz NVGRE |
| **Podstawowe cechy** Rozwiązanie **WAF** |
|  | WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:* wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a,
* typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT),
* przejścia pomiędzy URL-ami (servletami),
* dopuszczalne metody http,
* dopuszczalne cookie,
* dopuszczalne parametry w polityce,
* parametry dynamiczne,
* typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany),
* oraz dopuszczalne parametry w danym servlecie,
* długość zapytań,
* nazwy hosta,
* wystąpień i długość parametrów (per każdy parametr),
* wystąpień i długości nagłówków,
* wystąpień i długości cookies,
* oczekiwanych typów znaków per każdy parametr,
* typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku,
* URL-i podatnych na CSRF.
 |
|  | Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego |
|  | WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej |
|  | Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń) |
|  | Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego:* W szczególności na podstawie publicznego ruchu produkcyjnego,
* Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać nadużycia w procesie nauki.
 |
|  | Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa. |
|  | Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr |
|  | Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa |
|  | Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http |
|  | WAF musi automatycznie wykrywać błędne wyniki dodatnie (false positive) i wyłączać odpowiadające nim sygnatury dla danego parametru |
|  | WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force. |
|  | WAF musi posiadać mechanizmy ochrony przed atakami: * SQL Injection,
* Cross-Site Scripting,
* Cross-Site Request Forgery,
* Session hijacking,
* Command Injection,
* Cookie/Session Poisoning,
* Parameter/Form Tampering,
* Forceful Browsing,
* Brute Force Login,
* Web Scraping,
* Cookie manipulation/poisoning,
* Dynamic Parameter tampering,
* Buffer Overflow,
* Stealth Commanding,
* Unused HTTP Methods,
* Malicious File Uploads,
* Hidden Field Manipulation.
 |
|  | Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji. |
|  | Dodatkowo WAF powinien chronić przed kradzieżą sesji poprzez porównywanie „odciusku palca” (fingerprint) przeglądarki z sesją użytkownika. |
|  | Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta). |
|  | Wstrzykiwanie przez WAF dodatkowych informacji (cookie, tokeny, JavaScript), nie powinno powodować degradacji wydajności oferowanego urządzenia. |
|  | Rozwiązanie musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie:* Host
* URN
* Nagłówków
* Cookie
 |
|  | Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do:* Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2, CouchDB, Elasticsearch, MongoDB, SQLite, Sybase/ASE,
* System Operacyjny: Windows, Linux, UNIX,
* Język aplikacji, frameworki, biblioteki: ASP, ASP.NET, PHP, Java Servlets, JavaScript, AngualrJS, Backbone.js, CodeIgniter, Django, Java Server Faces, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Lotus Domino, Macromedia ColdFusion, Outlook Web Access, SSI, WebDAV, jQuery, SSI, Apache Struts, ef.js, Ember.js, Express.js, GraphQL, Handlebars, JavaServer Faces, Laravel, MooTools, Moustache, Python, React, RequireJS, Ruby, Spring Boot, UIKit, Underscore.js, Vue.js, WebDAV, Zend, ZURB Fundation,
* Serwer WWW, silniki: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy, Jenkins, Jetty, Joomla, Macromedia JRun, Nginx, Node.js, Oracle Application Server, Oracle Identity Manager, Redis, Typo3 CMS.
 |
|  | WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http) |
|  | WAF musi blokować ataki typu Slow Loris |
|  | WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:* Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania,
* Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser,
* Sygnatur botów,
* Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).
 |
|  | Rozwiązanie powinno umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub brute force. |
|  | Rozwiązanie powinno kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.  |
|  | Moduł ochrony przed DDoS powinien wykrywać ataki per:* Source IP,
* Urządzenie, na bazie „odcisku palca” urządzenia,
* Obszar geolokacyjny,
* URL,
* Globalnie – website.
 |
|  | Rozwiązanie powinno wykrywać i chronić przed atakami DDoS na tzw. ciężkie servlety, czyli servlety wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych.* Wykrycie ataku na ciężkie servlety powinno opierać się przynajmniej o ilość zapytań (TPS) oraz czas odpowiedzi,
* System powinien umożliwiać definicję maksymalnego czasu próbki ruchu,
* Maksymalnej pojemności próbki ruchu,
* Interwału czasowego pomiędzy pobieraniem próbki ruchu.
 |
|  | Rozwiązanie powinno umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS. |
|  | Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia |
|  | WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania określonej liczby incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika. |
|  | WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a. |
|  | WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem |
|  | WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a |
|  | W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP |
|  | WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON. |
|  | WAF powinien wyświetlać stronę blokowania (błędu) w technologiach AJAX i JSON |
|  | WAF musi posiadać wsparcie dla Google Web Toolkit |
|  | WAF musi posiadać możliwość ochrony komunikacji XML poprzez: * walidację Schema/WSDL,
* wybór dozwolonych metod SOAP,
* szyfrację /deszyfrację fragmentów wiadomości SOAP,
* wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie),
* definiowanie możliwości użycia załączników wiadomości SOAP,
* włączanie/wyłączanie podążania za odnośnikami do schematów SOAP,
* walidację SOAP Action Header,
* włączanie/wyłączanie możliwości użycia DTD
* włączanie/wyłączanie możliwości użycia zewnętrznych referencji
* włączanie/wyłączanie możliwości użycia początkowych białych znaków
* włączanie/wyłączanie możliwości użycia numerycznych nazw
* włączanie/wyłączanie możliwości użycia Processing Instructions
* włączanie/wyłączanie możliwości użycia CDATA
* ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace,
* ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów,
* definicję dopuszczalnych znaków,
* definicję sygnatur.
 |
|  | Funkcja sprawdzania reputacji adresów IP dostających się do chronionych aplikacji – funkcjonalność nie wymagana w ramach zamówienia. |
|  | Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania. |
|  | Subskrypcja na sygnatury kontekstowe powiązane z konkretną kampanią ataków. |
|  | Serwis reputacyjny musi realizować co najmniej następujące funkcje – funkcjonalność nie wymagana w ramach zamówienia:* Automatyczna aktualizacja informacji o zagrożeniach nie rzadziej niż co 5 minut
* Rozpoznawać i blokować komunikację dla minimum poniższych:
* Anonimowych proxy,
* Sieci Botnet,
* Aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy,
* Źródeł ataków DDoS/DoS,
* Źródeł Exit Node sieci Tor
* Adresów IP zainfekowanych przez malware
* Adresów IP świadczących usługi hostingowe dla phishingu lub fraudów.
* Źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force
* Źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen
* Weryfikacja adresu źródłowego na podstawie X-Forwarded-For (XFF)
 |
|  | Serwis sygnatur z aktualnymi kampaniami musi realizować następujące funkcje i informacje – funkcjonalność nie wymagana w ramach zamówienia:* Natychmiastowa aktualizacja sygnatur z aktualnymi kampaniami
* Musi dostarczać informacji o:
* powiązaniu z konkretnym aktorem stojącym za atakami,
* wektorem ataku lub wykorzystanej technice,
* intencji ataku,
* datach dotyczących pierwszej obserwacji ataku, ostatnio widzianego ataku,
* statusu kampanii,
* analizą wykorzystanego payloadu,
* informacji o dodatkowych szkodach.
 |
|  | WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia. |
|  | WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców (przynajmniej trzech) np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel. |
|  | WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać:* Directory traversal,
* Kodowanie typu %u,
* Kodowanie typu IIS backslash,
* IIS Unicode codepoints,
* Bare byte decoding,
* Apache whitespace,
* Bad unescape,
* Wstrzykiwanie komentarzy (np. <!-- -->).
 |
|  | Mechanizm normalizacji powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania. |
|  | Urządzenie musi wspierać następujące tryby pracy:* Tryb wykrywania, logowania i blokowania ataków,
* Tryb wykrywania i logowania ataków bez blokowania,
* Tryb uczenia się bez blokowania,
* Tryb uczenia się z blokowaniem i logowaniem.
 |
|  | WAF w trybie nauki, musi umożliwiać automatyczne, stopniowe przełączanie polityki bezpieczeństwa w tryb blokowania, np. servlety/parametry, dla których został zaobserwowany wystarczający ruch dla algorytmu nauki, zostaną przełączone w tryb blokowania, podczas gdy pozostałe pozostaną w trybie transparentnym. |
|  | WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach. |
|  | WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression. |
|  | WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6 |
| **Podstawowe cechy zarządzania systemem** |
|  | Rozwiązanie musi posiadać co najmniej następujące interfejsy administracyjne:* GUI przy wykorzystaniu protokołu https,
* Zarządzanie poprzez SSH,
* Zarządzanie poprzez API REST.
 |
|  | Autoryzacja administratorów systemu musi bazować na rolach użytkowników |
|  | Rozwiązanie musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody) |
|  | Rozwiązanie musi posiadać następujące funkcje zarządzania siecią:* Obsługa protokołu SNMP v1/v2c/v3,
* Możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID,
* Zewnętrzny syslog,
* Zbieranie danych i ich wyświetlanie,
* Zbieranie danych zgodnie z ustawieniami administratora,
* Osobna brama domyślna dla interfejsu zarządzającego,
* Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot),
* Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy),
* Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
 |
|  | Rozwiązanie musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS. |
|  | Rozwiązanie musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.  |
|  | Rozwiązanie musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:* Czas odpowiedzi per serwer,
* Czas odpowiedzi per URI,
* Ilość sesji użytkownika,
* Przepustowość,
* Adres źródła,
* Kraj,
* User Agent (wykorzystywana przez klienta aplikacja),
* Metoda dostępu
 |
|  | Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji. |
|  | Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP. |
|  | Rozwiązanie musi wspierać pracę w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active – active oraz rozbudowy do klastra N+1. |
|  | W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych. |
|  | Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu. |
|  | Klaster wysokiej dostępności musi zapewniać synchronizację:* Konfiguracji,
* Stanu połączeń,
* Przywiązywania sesji (Session persistence).
 |
|  | Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod:* Weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover)
* Weryfikacji stanu pracy urządzenia poprzez interfejs szeregowy (serial failover)
 |
|  | Wymagana jest 3 letnia gwarancja producenta. W obrębie gwarancji zawarte musi być:* Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta,
* Sposób obsługi zgłoszeń gwarancyjnych w trybie 7x24,
 |

# Wymagania dodatkowe – godziny inżyniera (dotyczy ZADANIA NR 1)

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WD1.01 | Zapewnienie przez wykonawcę 90 godzin inżyniera posiadającego certyfikację na poziomie Ekspert producenta rozwiązań Cisco do końca 2022 roku, do wykorzystania na konsultacje, prace w zakresie konsultacji architektonicznych, realizacji szkoleń, konsultacji modernizacyjnych a także warsztatów technicznych z powiązanych technologii NAC. Godziny zostaną wykorzystane w powyższym okresie na realizację czynności w zależności od występujących potrzeb Zamawiającego oraz w związku z powiązaniem z innymi projektami prowadzonymi przez Zamawiającego. Zamawiający zastrzega sobie możliwość niewykorzystania wszystkich godzin Inżyniera we wskazanym okresie. Prace będą realizowane w siedzibie Zamawiającego lub poza nią po wcześniejszych uzgodnieniach. W przypadku, kiedy Wykonawca zidentyfikuje zagrożenia wynikające z realizacji zleconych prac poinformuje Zamawiającego o zagrożeniach. Zamawiający informuje, iż płatności będą realizowane z dołu, czyli po realizacji zleceń przez Wykonawcę oraz podpisaniu protokołu odbioru Zlecenia. Szczegółowa procedura udzielenia i odbioru Zleceń przez Zamawiającego opisana została w Umowie. Wszelkie zmiany realizowane w ramach architekturze wymagające zmian w dokumentacji należy nanieś na posiadaną przez Zamawiającego dokumentację lub dostarczyć nowo utworzoną. |

# Wymagania dodatkowe (dotyczy ZADANIA NR 1 i ZADANIA NR 2)

Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia, po wygaśnięciu zawartej umowy serwisowej, usługi wsparcia producenta bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla Licencji będących przedmiotem zamówienia

# Świadczenie serwisu gwarancyjnego i gwarancji.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis funkcjonalności** |
| **WUS.01** | Na dostarczone rozwiązanie Wykonawca zapewni wsparcie producenta wraz gwarancją liczoną od daty podpisania protokołu odbioru produktu na okres 36 miesięcy opartego na świadczeniach serwisowych producenta. |
| **WUS.02** | Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: * prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru;
* możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania;
* dostęp do pomocy technicznej producenta;
* nieograniczona liczba zgłoszeń serwisowych;
* dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania/urządzeń;
* dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji;
* dostęp do portalu www producenta Oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania;
* dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania/urządzeń).
 |
| **WUS.03** | Wykonawca wraz z dostawą licencji na Oprogramowanie przekaże warunki gwarancyjne i serwisowe, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie elektronicznej edytowalnej. |
| **WUS.04** | Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego. |
| **WUS.05** | Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu |
| **WUS.06** | Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzed wystąpienia awarii albo zaproponowanie procedury obejścia zaistniałych awarii bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę. |
| **WUS.07** | Wykonawca dokona usunięcia Awarii Krytycznej w terminie nie dłuższym niż 8 godzin od momentu zgłoszenia. |
| **WUS.08** | Wykonawca dokona usunięcia Awarii Niekrytycznej w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia.  |
| **WUS.09** | Wykonawca dokona usunięcia Awarii Zwykłej w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia.  |
| **WUS.11** | Wykonawca najpóźniej w 1 Dzień Roboczy, po rozwiązaniu każdego Incydentu serwisowego przedstawi raport z tego Incydentu serwisowego (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Incydencie serwisowym oraz rozwiązania Incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu serwisowego). |
| **WUS.15** | Wszystkie działania związane z usunięciem awarii oraz aktualizacji muszą być wykonywane przez autoryzowany przez Wykonawcę personel. |
| **WUS.16** | Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania awarii przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.  |
| **WUS.17** | W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.  |
| WUS.18 | Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów. |
| WUS.19 | Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.  |
| WUS.20 | Dla oprogramowania obowiązują prawa gwarancyjne producenta. |
| WUS.21 | Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady. |

# Zasady odbioru przedmiotu zamówienia (dotyczy ZADANIA NR 1 i ZADANIA NR 2)

1. **Zasady Ogólne**
2. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
3. Przedmiot Umowy podlegać będzie odbiorowi.
4. Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Księżycowej 5, w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35.
5. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu odbioru ilościowo – jakościowego, którego wzór stanowi załącznik nr 3 do Umowy oraz protokołu odbioru Zleceń, którego wzór stanowi załącznik nr 4 do Umowy
6. **Odbiór**
	1. Celem czynności kontrolnych prowadzonych w ramach odbioru jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności z zakresem określonym w Umowie lub w przekazanych Zleceniach jak również sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
	2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.
	3. Podstawą dokonania odbioru jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach Umowy wraz z wymaganymi licencjami lub też poprawności wykonanej pracy inżyniera.
	4. Pozytywny wynik odbioru zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego lub protokołu odbioru Zlecenia.