**Sprawa numer: DZ.210.598.2023.ZZ**

**UMOWA /wzór nr ………..**

zawarta pomiędzy:

**Instytutem Łączności – Państwowym Instytutem Badawczym,** z siedzibą w Warszawie pod adresem: ul. Szachowa 1, 04-894 Warszawa, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000023097, NIP: 5250009312 oraz REGON: 000132629, zwanym dalej **„Zamawiającym”,** reprezentowanym przez:

**dr. hab inż. Paweł Pławiak** – p.o. Dyrektora Instytutu Łączności – Państwowego Instytutu Badawczego,

**a**

**……………………………………………….,** z siedzibą w ……………………. pod adresem ul. ………………. ,**xx-xxx ……………………….,** wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla …... …………… w ………………, ……… Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: ……………….., NIP …………….., REGON …………….., o kapitale zakładowym: ………………, zwanym dalej „**Wykonawcą**”, reprezentowaną przez:

**……………………………………………………..**

Zamawiający i Wykonawca będą dalej łącznie zwani „**Stronami**” lub indywidualnie „**Stroną**”.

*W wyniku dokonania wyboru oferty Wykonawcy w postępowaniu o udzielenie zamówienia publicznego, prowadzonym z wyłączeniem stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w zw. z art. 2 ust. 1 pkt 1 tej ustawy, zawarto umowę (dalej: „****Umowa****”) o następującej treści:*

**§ 1.**

**Przedmiot Umowy**

1. Przedmiotem Umowy jest dostawa dwóch firewalli - urządzeń Palo Alto PA-440 wraz z licencjami PAN-PA-440-TP-5YR-HA2, PAN-SVC-BKLN-440-5YR dla ochrony sieci komputerowych w oddziałach Instytutu Łączność – PIB w Gdańsku i we Wrocławiu~~.~~
2. Parametry urządzeń są zawarte w Opisie Przedmiotu Zamówienia (dalej: ,,OPZ’’), który stanowi Załącznik nr 1 do Umowy.
3. Przedmiot umowy obejmuje w ramach zamówienia w szczególności:
   1. dostarczenie do Zamawiającego nowych, wolnych od wad i usterek Urządzeń, o jakości i parametrach określonych w OPZ, na koszt i ryzyko Wykonawcy;
   2. dostarczenie Urządzenia w opakowaniu posiadającym wyraźne oznaczenie (nazwa, liczba sztuk, producent);
   3. dostarczenie wszystkich niezbędnych akcesoriów i innych drobnych elementów wymaganych do poprawnego działania dostarczonych urządzeń;
   4. dostarczenie instrukcji obsługi w języku polskim;
   5. dostarczenie dokumentu gwarancji;
   6. dostarczenie zaleceń producenta dotyczących częstości wykonywania okresowych przeglądów serwisowych.

**§ 2.**

**Termin**

Umowa zostanie wykonana w terminie do 4 tygodni od podpisania Umowy

**§ 3.**

**Wynagrodzenie**

1. Z tytułu wykonania przedmiotu Umowy, określonego w § 1 Umowy, Zamawiający zapłaci Wykonawcy wynagrodzenie netto w kwocie …………………….. (słownie: ……………………….. ), tj. …….. …….. (słownie: ……………..)
2. Wartość umowy brutto (z podatkiem VAT) obejmuje wszelkie koszty Wykonawcy związane z realizacją przedmiotu Umowy.
3. Wynagrodzenie Wykonawcy płatne będzie na rachunek bankowy Wykonawcy, wskazany na fakturze VAT, w terminie 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT.
4. Faktura VAT, z załączonym zaakceptowanym przez Strony protokołem zdawczo-odbiorczym stanowić będzie podstawę do dokonania płatności.
5. Faktura zostanie wystawiona i przesłana na adres: Instytut Łączności – Państwowy Instytut Badawczy, ul. Szachowa 1, 04-894 Warszawa, w terminie 30 dni od dnia zaakceptowania protokołu zdawczo-odbiorczego przez Zamawiającego.
6. Zamawiający wyraża zgodę na przesłanie mu faktury VAT w formie elektronicznej na adres: [faktury@il-pib.pl](mailto:faktury@il-pib.pl).
7. Wykonawca może również, za pomocą platformy, o której mowa w art. 13 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym, wystawić Zamawiającemu ustrukturyzowane faktury elektroniczne, o których mowa w art. 4 ust. 1 tej ustawy, posługując się adresem Zamawiającego: <https://www.brokerinfinite.efaktura.gov.pl>.
8. Zamawiający dokona zapłaty wymaganej kwoty za realizację przedmiotu Umowy przelewem, z zastosowaniem mechanizmu podzielonej płatności, o ile będzie to wymagane przepisami prawa. Rachunek bankowy Wykonawcy powinien być ujawniony w wykazie prowadzonym na podstawie art. 96b ust 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tzw. „biała lista”) prowadzonym przez Szefa Krajowej Administracji Skarbowej. Jeżeli Zamawiający stwierdzi, że rachunek wskazany przez Wykonawcę na fakturze nie znajduje się na tzw. „białej liście podatników VAT”, wstrzyma się z dokonaniem zapłaty za prawidłową realizację przedmiotu Umowy do czasu wskazania innego rachunku przez Wykonawcę, który będzie umieszczony na przedmiotowej liście.
9. Za datę zapłaty uznaje się obciążenie rachunku bankowego Zamawiającego.
10. Zamawiający nie wyraża zgody na zmianę wierzyciela Wykonawcy.

**§ 4.**

**Oświadczenia**

1. Wykonawca zobowiązuje się realizować Umowę z należytą starannością, przy zachowaniu zasad współczesnej wiedzy i zgodnie z obowiązującymi w tym zakresie przepisami, zgodnie z najlepszą praktyką i wiedzą zawodową z zachowaniem należytej staranności.
2. Wykonawca zobowiązuje się do natychmiastowego informowania Zamawiającego o wszelkich zaistniałych problemach i trudnościach mających lub mogących mieć wpływ na terminową i bezusterkową realizację przedmiotu umowy oraz przedstawienia propozycji ich rozwiązania
3. Powierzenie przez Wykonawcę wykonania całości lub części przedmiotu Umowy osobom trzecim wymaga uprzedniej pisemnej zgody Zamawiającego.
4. W przypadku powierzenia wykonania całości lub części przedmiotu Umowy osobom trzecim, Wykonawca ponosi odpowiedzialność za ich działania lub zaniechania jak za działania i zaniechania własne.
5. Wykonawca oświadcza, że Urządzenia:
   1. spełniają wszystkie wymogi dotyczące bezpieczeństwa oraz zużycia energii określone w obowiązującym w Polsce prawie;
   2. są fabrycznie nowe, kompletne, nieużywane i bez oznak używania, nierefabrykowane i nieregenerowane, nienaprawiane, nie podlegały ponownej obróbce oraz w jednolitej konfiguracji;
   3. są wolne od jakichkolwiek wad fizycznych, prawnych, jak i ograniczających możliwość jego prawidłowego użytkowania;
   4. zostały dopuszczone do obrotu gospodarczego na terytorium Rzeczpospolitej Polskiej;
   5. są zgodne ze stosowanymi normami technicznymi;
   6. posiadają certyfikaty dopuszczające do stosowania w Unii Europejskiej;
   7. posiadają gwarancje producenta .
6. Korzystanie przez Wykonawcę z narzędzi koniecznych do wykonania Umowy, w szczególności, z praw autorskich, licencji, praw własności przemysłowej, intelektualnej nie narusza przepisów prawa, prawem chronionych dóbr osobistych lub majątkowych osób trzecich, w szczególności praw autorskich, praw pokrewnych, praw z rejestracji wzorów przemysłowych oraz praw ochronnych na znaki towarowe.
7. W razie powstania w trakcie wykonywania Umowy lub po jej wykonaniu jakichkolwiek roszczeń osób trzecich, Wykonawca przejmuje na siebie wyłączną odpowiedzialność za roszczenia osób trzecich z tytułu szkód majątkowych i niemajątkowych w mieniu i na osobie z tytułów, o których mowa w ust. 3, a wynikłych z wykonania, z nienależytego wykonania lub z braku wykonania Umowy przez Wykonawcę, jego zastępców, pracowników lub jakichkolwiek osób zaangażowanych do realizacji Umowy.

**§ 5.**

**Warunki realizacji Umowy, odbiór**

1. Wykonawca dostarczy urządzenia zgodne z wymaganiami zawartymi w Opisie Przedmiotu Zamówienie stanowiącego załącznik nr 1 do Umowy, do siedziby Zamawiającego w dni robocze, po wcześniejszym majlowym potwierdzeniu terminu dostawy przez Zamawiającego.
2. Za dni robocze, o których mowa w Umowie, uważa się dni od poniedziałku do piątku w godzinach od 9:00 do 16:00, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy u Zamawiającego.
3. Wykonawca dostarczy wsparcia producenta na okres 60 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjnych w trybie 24x7.
4. Koszt dostawy: załadunku, transportu do siedziby Zamawiającego oraz rozładunku i umieszczenia we wskazanych przez Zamawiającego pomieszczeniach lub miejscu ponosi Wykonawca.
5. Podczas odbioru Zamawiający dokona sprawdzenia zgodności dostarczonego przedmiotu Umowy, kompletności. Wzór protokołu zdawczo-odbiorczego stanowi Załącznik nr 2 do Umowy.
6. W przypadku stwierdzenia podczas dokonywania odbioru przedmiotu Umowy wad lub usterek, Wykonawca zobowiązuje się do ich niezwłocznego usunięcia lub wymiany przedmiotu Umowy na wolny od wad lub usterek. W przypadku, gdy Zamawiający uzna, że nie jest możliwe zapewnienie zgodności przedmiotu umowy z wymaganiami umownymi, może odstąpić od umowy z przyczyn leżących po stronie Wykonawcy.
7. Wykonawca udzieli gwarancji naprawy lub wymiany urządzenia w ciągu 48 godzin przez okres 60 miesięcy od daty podpisania protokołu zdawczo - odbiorczego
8. Zamawiający dokona odbioru przedmiotu Umowy bez wad lub usterek (lub po ich usunięciu).
9. Protokół zdawczo-odbiorczy podpisany obustronnie, bez zastrzeżeń, przez osoby upoważnione przez każdą ze Stron stanowi potwierdzenie należytego wykonania przedmiotu Umowy.
10. Protokół zdawczo-odbiorczy zostanie wystawiony i podpisany w dwóch egzemplarzach, po jednym dla każdej Strony.

**§ 6.**

**Koordynacja i nadzór wykonania Umowy**

1. Do współpracy i koordynacji realizacji przedmiotu Umowy, w tym do podpisania protokołu zdawczo- odbiorczego , upoważnione są osoby ze strony Zamawiającego:
2. ………………………………………………
3. Do współpracy i koordynacji realizacji przedmiotu Umowy, w tym do podpisania protokołu zdawczo-odbiorczego, upoważnione są osoby ze strony Wykonawcy:
4. ……………………………………………………………………………………………………………………
5. Korespondencja związana z wykonywaniem Umowy będzie dostarczana osobiście lub pocztą tradycyjną lub pocztą elektroniczną na adres:
6. do Zamawiającego: …………………………………………………………
7. do Wykonawcy: ……………………………………………………………………………………..
8. Oświadczenia w przedmiocie odstąpienia od Umowy, wypowiedzenia Umowy lub nałożenia kary umownej wymagają formy pisemnej lub elektronicznej pod rygorem nieważności.
9. Zmiana osób lub danych, o których mowa w ust. 1 - 3 nie stanowi zmiany Umowy. Zmiana taka nie wymaga zawarcia aneksu do Umowy. W przypadku wystąpienia takiej zmiany, Strony wzajemnie pisemnie informują się o zmianie takich danych lub o nowej osobie, upoważnionej do współpracy i koordynacji wykonania Umowy.

**§ 7.**

**Kary umowne**

1. Wykonawca zobowiązuje się do zapłaty Zamawiającemu kar umownych z następujących tytułów i w wysokości:
2. w przypadku opóźnienia Wykonawcy w terminie realizacji Umowy określonym w § 2 Umowy - w wysokości 0,5% całkowitego wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy za każdy rozpoczęty dzień opóźnienia,
3. w przypadku odstąpienia od Umowy przez Zamawiającego w całości lub części z przyczyn leżących po stronie Wykonawcy - w wysokości 20% całkowitego wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy.
4. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przekraczającego wysokość kar umownych zastrzeżonych w Umowie na zasadach ogólnych kodeksu cywilnego.
5. Wykonawca wyraża zgodę na potracenie kar umownych z przysługującego mu wynagrodzenia brutto, określonego w § 3 ust. 1 Umowy (potrącenie umowne). Strony zgodnie postanawiają, że w ramach tego kary umowne mogą być pokrywane lub potrącane z każdej należności Wykonawcy, w szczególności z wynagrodzenia Wykonawcy, nawet w przypadku nieprzedstawienia przez Wykonawcę faktury. Potrącenie kar umownych może być dokonane z wierzytelności niewymagalnych, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskania pisemnego potwierdzenia
6. Łączna wysokość kar umownych nie może przekroczyć 20% wynagrodzenia, o którym mowa w § 3 ust. 1 Umowy.
7. Kary umowne będą naliczane odrębnie za każdy przypadek naruszenia Umowy, uprawniający do naliczenia kar.

**§ 8.**

**Wypowiedzenie/Odstąpienie od Umowy**

1. Strony postanawiają, że Zamawiającemu przysługuje prawo do wypowiedzenia/odstąpienia od Umowy w całości lub w części, według własnego wyboru Zamawiającego w przypadku, gdy:
2. dotychczasowy przebieg prac związanych z wykonaniem Umowy wskazywać będzie, że zachodzą uzasadnione wątpliwości, iż Umowa zostanie należycie wykonana i w umówionym terminie;
3. gdy wysokość naliczonych kar umownych przekroczy 20% wartości maksymalnego wynagrodzenia Wykonawcy, o którym mowa w § 3 ust. 1 Umowy;
4. Wykonawca nienależycie wykonuje Umowę, a w szczególności nie przestrzega ustalonych terminów lub narusza inne postanowienia Umowy i w przypadku, gdy po upływie wyznaczonego przez Zamawiającego terminu, nie krótszego niż 3 dni, od wezwania przez Zamawiającego do zaniechania przez Wykonawcę naruszeń postanowień Umowy oraz usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania.
5. Postanowienia powyższe nie ograniczają prawa Zamawiającego do odstąpienia od Umowy w przypadkach wskazanych w przepisach obowiązującego prawa. W szczególności w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu lub powzięcia informacji o nieotrzymaniu środków budżetowych koniecznych do realizacji Umowy od dysponenta odpowiedniego stopnia lub braku środków w budżecie Zamawiającego, czego nie można było przewidzieć w chwili zawarcia Umowy.
6. W przypadku wypowiedzenia/odstąpienia od Umowy Wykonawcy przysługuje tylko prawo do części wynagrodzenia za zrealizowaną i odebraną przez Zamawiającego część Umowy na podstawie protokołu zdawczo-odbiorczego.
7. Prawo wykonania odstąpienia od Umowy, o którym mowa w niniejszym paragrafie Zamawiający może wykonać w terminie 30 dni liczonych od wystąpienia okoliczności uprawniających Zamawiającego do odstąpienia od Umowy jednak nie później niż w terminie 60 dni liczonych od terminu określonego w § 2 Umowy.

**§ 9.**

**Zmiany Umowy**

O ile Umowa nie stanowi inaczej wszelkie zmiany i uzupełnienia Umowy wymagają zachowania formy pisemnej lub elektronicznej pod rygorem nieważności.

**§ 10.**

**Gwarancja jakości i rękojmia**

1. Wykonawca udziela gwarancji jakości na dostarczone urządzenia (na jego wszystkie elementy), która biegnie od dnia podpisania protokołu zdawczo – odbiorczego bez uwag przez Strony i wynosi 5 lat NBD. Termin rękojmi za wady jest równy okresowi gwarancji, zgodnie z art. 558 kodeksu cywilnego.
2. Dla Zamawiającego gwarantem z tytułu gwarancji jakości, o której mowa w niniejszej Umowie jest Wykonawca. Nie zwalnia to jednak Wykonawcy od dostarczenia dokumentów gwarancyjnych oraz wsparcia technicznego producenta oferowanego przedmiotu zamówienia (jeśli jest inny niż Wykonawca), jeżeli takie są przez niego dostarczane wraz z tym przedmiotem zamówienia.
3. Wykonawca gwarantuje, że usługi gwarancyjne w ramach Umowy będą świadczone w sposób profesjonalny zgodnie ze standardami obowiązującymi w branży.
4. Realizacja obowiązków gwarancyjnych podlegać będzie dokumentowaniu przez Wykonawcę w Protokole gwarancyjnym, którego wzór stanowi Załącznik nr 3 do Umowy.
5. W przypadku utraty lub braku możliwości zapewnienia dostępu do serwisu, wszelkie działania organizacyjne i koszty z tym związane ponosi Wykonawca, w tym załatwienie wszelkich formalności związanych z ewentualną wymianą wadliwego elementu przedmiotu umowy, jego wysyłką do naprawy gwarancyjnej i odbiorem, dostarczeniem do Zamawiającego lub z importem części zamiennych.
6. W okresie gwarancji Wykonawca zobowiązuje się do naprawy lub wymiany przedmiotu umowy, który ulegnie uszkodzeniu. Wykonawca nie ponosi odpowiedzialności za uszkodzenia powstałe w czasie eksploatacji, jeśli są one spowodowane niestosowaniem się do dostarczonej instrukcji obsługi sprzętu.
7. Czas reakcji serwisu na zgłoszone wady (usterki) z tytułu gwarancji lub rękojmi oraz czas naprawy lub wymiany urządzenia nastąpi w terminie nie dłuższym niż w ciągu 48 godzin przez okres 60 miesięcy od podpisania protokołu zdawczo - odbiorczego.
8. Gwarancja obejmuje wszystkie usterki i wady oraz uszkodzenia powstałe w czasie, zgodnego z przeznaczeniem i instrukcjami użytkowania dostarczonego sprzętu.
9. Gwarancja musi być świadczona przez producenta lub autoryzowany przez niego serwis lub osoby na koszt Wykonawcy.
10. Wykonawca gwarantuje najwyższą jakość dostarczonego sprzętu zgodnie ze specyfikacją techniczną. Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady (usterki) powstałe z przyczyn tkwiących w przedmiocie umowy od momentu podpisania protokołu zdawczo – odbiorczego przez Zamawiającego jak i wszelkie inne wady fizyczne, powstałe z przyczyn, za które Wykonawca ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
11. Naprawa lub wymiana sprzętu na nowy musi mieć miejsce w siedzibach Zamawiającego.
12. Serwis gwarancyjny świadczony będzie co najmniej przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. Kontakt do serwisu: e-mail [………………](mailto:info@e-prime.pl) tel.: ……………………
13. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych telefonicznie w godz. 8.00 – 16.30 a przez całą dobę przez e-mail lub WWW.
14. W przypadku naprawy lub wymiany przedmiotu umowy w okresie gwarancyjnym, gwarancja ulega przedłużeniu o czas naprawy lub wymiany.
15. Dla uniknięcia wszelkich wątpliwości, Strony zgodnie postanawiają, że skorzystanie przez Zamawiającego z uprawnień z tytułu gwarancji nie wyłącza możliwości wykonania przez Zamawiającego przysługujących mu na mocy bezwzględnie obowiązujących przepisów prawa uprawnień z tytułu rękojmi i odwrotnie, wykonanie uprawnień z tytułu rękojmi nie wyłącza wykonania uprawnień z tytułu gwarancji.
16. W wypadku rozbieżności pomiędzy postanowieniami Umowy, a postanowieniami gwarancji producenta, pierwszeństwo mają postanowienia Umowy, chyba że postanowienia gwarancji producenta są dla Zamawiającego korzystniejsze.

**§ 11.**

**RODO**

1. Strony zobowiązują się przetwarzać dane osobowe – udostępnione na podstawie odpowiednich zgód lub innych podstaw prawnych – zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej: RODO) i innymi powszechnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych, stosując przy tym środki techniczne i organizacyjne wskazane w art. 32 RODO, zapewniające właściwą ochronę danych osobowych oraz zapewniając dostęp do danych osobowych wyłącznie osobom upoważnionym.
2. Strony zobowiązują się do zachowania w tajemnicy uzyskanych informacji podlegających ochronie.

**§ 12.**

**Postanowienia końcowe**

1. Ewentualne spory powstałe w trakcie realizacji Umowy podlegają rozpoznaniu przez sąd właściwy dla siedziby Zamawiającego.
2. Prawem właściwym dla oceny Umowy oraz wszelkich związanych z nią zdarzeń prawnych jest prawo polskie.
3. W sprawach nieuregulowanych Umową zastosowanie mają przepisy prawa polskiego,  
   w szczególności przepisy Kodeksu cywilnego.
4. Załączniki do Umowy stanowią jej integralną część.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego i jeden dla Wykonawcy.
6. Umowa została zawarta w dniu podpisania Umowy przez ostatnią ze Stron.

**Załącznik do Umowy:**

Załącznik nr 1 – OPZ   
Załącznik nr 2 – Wzór protokołu zdawczo-odbiorczego.  
Załącznik nr 3 – Wzór protokołu gwarancyjnego  
Załącznik nr 4 - Klauzula informacyjna RODO Zamawiającego  
Załącznik nr 5 – oferta Wykonawcy

|  |  |
| --- | --- |
| ……………………………………. | ………………………………………. |
| (data i podpis Zamawiającego) | (data i podpis Wykonawcy) |

Numer sprawy: DZ.210.598.2023.ZZ

Załącznik nr 1

do umowy nr ……

Opis przedmiotu zamówienia.

Dostawa dwóch firewalli - urządzeń Palo Alto PA-440 wraz z licencjami PAN-PA-440-TP-5YR-HA2 oraz PAN-SVC-BKLN-440-5YR dla ochrony sieci komputerowych w oddziałach Instytutu Łączność – PIB w Gdańsku i Wrocławiu.

Instytut Łączności posiada w oddziałach w Gdańsku i Wrocławiu Firewalle Palo Alto model PA-850, wraz z licencjami/wsparciem:

* PAN-SVC-BKLN-850-R - Partner enabled premium suport year 1
* PAN-PA-850-TP-HA2-R - Therat preventiuon subscriptionfor devic

które mają być zastąpione dwoma urządzeniami Palo Alto PA-440 wraz licencjami:

* PAN-SVC-BKLN-440-5YR - Partner enabled premium suport year 5
* PAN-PA-440-TP-5YR-HA2- Therat preventiuon subscriptionfor devic

spełniającymi następującymi wymaganiami:

|  |  |
| --- | --- |
| Lp. | **Wymagania podstawowe** |
| 1 | System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| 2 | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 2.2 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 700 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 190 000 jednoczesnych połączeń. |
| 3 | System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Ethernet 10/100/1000 oraz musi być wyposażone w uchwyty/szyny do montażu urządzeń w szafie RACK 19 lub jeśli ich nie posiada to należy dostarczyć półkę montażową zgodną z oferowanym urządzeniem. |
| 4 | System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| 5 | Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). |
| 6 | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. |
| 7 | System zabezpieczeń firewall musi obsługiwać nie mniej niż 3 wirtualne routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. |
| 8 | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| 9 | Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| 10 | System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| 11 | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. |
| 12 | Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 2,2 Gbit/s. |
| 13 | Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). |
| 14 | Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. |
| 15 | Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. |
| 16 | System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| 17 | System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 18 | System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| 19 | System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |
| 20 | System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |
| 21 | System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików. |
| 22 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| 23 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| 24 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. |
| 25 | System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. |
| 26 | System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |
|  | **Wymagania podstawowe identyfikacja użytkowników** |
| 27 | System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |
| 28 | System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. |
| 29 | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |
| 30 | Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
|  | **Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day** |
| 31 | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. |
| 32 | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 33 | System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| 34 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 35 | System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 36 | System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 37 | System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 38 | System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 39 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 40 | System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| 41 | System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| 42 | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 43 | System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| 44 | System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |
| 45 | System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| 46 | System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| 47 | System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany. |
| 48 | System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| 49 | System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 700 Mbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. |
| 50 | Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". |
| 51 | Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”. |
| 52 | System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. |
|  | **Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS** |
| 53 | System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| 54 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| 55 | System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| 56 | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |
| 57 | System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach. |
| 58 | System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0. |
| 59 | System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
| 60 | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. |
| 61 | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |
|  | **Wymagania dodatkowe środowisko wirtualne vmware** |
| 61 | System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |
|  | **Wymagania zarządzanie i raportowanie** |
| 62 | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| 63 | System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. |
| 64 | System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. |
| 65 | System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. |
| 66 | System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| 67 | Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| 68 | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. |
| 69 | System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). |
| 70 | System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |
| 71 | System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. |
| 72 | System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. |
| 73 | System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. |
| 74 | System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. |
| 75 | System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia. |
| 76 | System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. |
| 77 | System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. |
| 78 | System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. |
| 79 | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| 80 | Wykonawca musi zapewnić wsparcie w migracji konfiguracji z obecnego rozwiązania Zamawiającego na rozwiązanie zaoferowane. |
| 81 | Wymagana jest gwarancja naprawy lub wymiany urządzenia w ciągu 48 godzin przez okres 60 miesięcy od daty podpisania odbioru. |
| 82 | Wymagane jest dostarczenie wsparcia producenta na okres 60 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7. |
| 83 | Urządzenie należy dostarczyć w konfiguracji z dwoma zasilaczami. |
| 84 | Urządzenie należy wraz z zestawem montażowym do szafy 19 cali. Dopuszczalne jest dostarczenie półki, na której zostanie postawione urządzenie. |

Numer sprawy: DZ.210.598.2023.ZZ

Załącznik nr 2

do umowy nr ……

(wzór)

**PROTOKÓŁ ZDAWCZO – ODBIORCZY**

1. W dniu …………………… dokonano odbioru przedmiotu zamówienia realizowanego na podstawie umowy nr ……………………… z dnia ……………………, w tym:

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Przedmiot dostawy** | **Data realizacji** | **Zastrzeżenia/brak zastrzeżeń** |
|  |  |  |  |

1. *Zamawiający* stwierdza, że przedmiot umowy został dostarczony ……………………………………………………………………...….

…………………………………………………………………………………..

……………………………………………………………………………………

Protokół niniejszy stanowi podstawę do wystawienia faktury VAT.

**Zamawiający:** **Wykonawca:**

…………………………. …………………….

…………………………. …………………….

Nr sprawy: DZ.210.598.2023.ZZ

Załącznik nr 3

do umowy nr ……………………

**PROTOKÓŁ GWARANCYJNY Nr …**

Sporządzony w dniu ………. w związku ze zgłoszeniem reklamacji na podstawie Umowy nr ………………... z dnia …

Imię i nazwisko przedstawiciela Zamawiającego ...

Dokładny adres: …………………………………………………….

Nazwa Sprzętu ...

Nr seryjny ...

Producent ...

Transport : Wykonawcy ...

Dokładny opis wad ...

Żądanie Zamawiającego co do sposobu załatwienia reklamacji ...

Data i podpis osoby składającej reklamację po stronie Zamawiającego: ...

Data i podpis osoby przyjmującej reklamację po stronie Wykonawcy: ...

Opinia pracownika / rzeczoznawcy Wykonawcy...

Decyzja pracownika Wykonawcy ...

Sposób realizacji reklamacji …

Przedstawiciel Zamawiającego Przedstawiciel Wykonawcy

................................................... ..............................................

(data, czytelny podpis) (data, czytelny podpis)

Numer sprawy: DZ.210.598.2023.ZZ

Załącznik nr 4  
do umowy nr …………………….

Informacja o przetwarzaniu danych osobowych  
dla Wykonawców - postępowania prowadzone z wyłączeniem przepisów  
ustawy Prawo zamówień publicznych

1. Administrator danych:  
Administratorem danych osobowych jest Instytut Łączności – Państwowy Instytut Badawczy z  
siedzibą w Warszawie ( 04-894 ) przy ul. Szachowej 1, zwany dalej „ Instytutem ”.  
2. Inspektor ochrony danych:  
Nadzór nad przestrzeganiem przepisów o ochronie danych osobowych w Instytucie realizuje inspektor  
ochrony danych. Z inspektorem należy kontaktować się drogą mailową iod@itl.waw.pl lub w formie  
pisemnej na adres siedziby administratora.  
3. Cel i podstawy przetwarzania:  
Państwa dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b) RODO w celu związanym z zawarciem i realizacją Umowy …………………… dotyczącej …………………..oraz w oparciu o art. 6 ust. 1 lit. c) RODO - w celu  
wypełnienia obowiązków prawnych ciążących na administratorze i realizacją zawartych umów a także  
na podstawie art. 6 ust. 1 lit f) RODO – w celu zabezpieczenia i dochodzenia ewentualnych roszczeń z  
umowy jako prawnie uzasadnionych interesów realizowanych przez administratora i weryfikacji  
danych osobowych w publicznych rejestrach.  
4. Odbiorcy danych osobowych:  
Odbiorcami Pani/Pana danych osobowych będą podmioty i organy, upoważnione na podstawie  
powszechnie obowiązujących przepisów prawa, oraz podmioty, którym na podstawie stosownych  
umów powierzono dane osobowe w związku z realizacją usług gwarantujących należyte wykonanie  
niniejszej umowy.  
5. Okres przetwarzania danych osobowych:  
Pani / Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji warunków umowy oraz w zakresie wymaganym przez przepisy prawa powszechnie obowiązującego lub dla zabezpieczenia i dochodzenia ewentualnych roszczeń.  
6. Uprawnienia:  
Posiada Pani/Pan prawo do dostępu do treści swoich danych, ich sprostowania, ograniczenia  
przetwarzania, wniesienia sprzeciwu, żądania ich usunięcia – w przypadkach i na warunkach  
określonych w RODO.  
Nie przysługuje Pani/Panu prawo do usunięcia danych osobowych, prawo do przenoszenia danych  
osobowych, prawo sprzeciwu wobec przetwarzania danych osobowych, gdyż podstawą prawną  
przetwarzania Pani / Pana danych osobowych jest art. 6 ust. 1 lit. c RODO Skorzystanie przez

Panią/Pana z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o których mowa w  
art. 16 RODO, nie może skutkować zmianą umowy.  
Posiada Pani/Pan prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych  
osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie ( 00 - 193 ) przy  
ul. Stawki 2.  
W celu skorzystania z powyższych uprawnień należy skontaktować się z administratorem danych lub z Inspektorem ochrony danych osobowych.  
7. Obowiązek podania danych:  
Podanie danych osobowych jest obowiązkowe, gdyż jest niezbędne dla wykonania przedmiotu umowy i jego udokumentowania.