Załącznik 6.3. do SIWZ

SP.ZP.272.49.2018.II.FR

Opis Przedmiotu Zamówienia

Zadanie 3 – Dostawa i wdrożenie infrastruktury sieciowej – aktywnej i pasywnej dla Gminy Kąty Wrocławskie

Zamówienie realizowane w ramach projektu pn**.** „Zwiększenie dostępności i jakości elektronicznych usług publicznych dla mieszkańców i podmiotów gospodarczych Powiatu Wrocławskiego oraz 8 Gmin: Czernicy, Długołęki, Jordanowa Śląskiego, Kątów Wrocławskich, Kobierzyc, Mietkowa, Siechnic i Żórawiny”. współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020; Oś Priorytetowa 2 Technologie Informacyjno - Komunikacyjne; Działanie 2.1 E-usługi publiczne, Poddziałanie 2.1.1 E-usługi publiczne – konkurs horyzontalny.

1. **Zestawienie zbiorcze sprzętu - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Dostawa infrastruktury sieciowej – aktywnej i pasywnej		Gmina Kąty Wrocławskie
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Przełącznik dostępowy	3
2.	UTM	3

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

   W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

   - Dostawę, instalację, konfigurację i uruchomienie zgodnie ze wskazaniem Zamawiającego urządzeń wymienionych w poz. 1 i 2 powyższej tabeli.

   Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

   3.1. ***Urządzenie UTM Typ 1 – 2 szt.***

   Dostarczony system bezpieczeństwa (dostarczane urządzenie wraz z niezbędnym oprogramowaniem), musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

   Dla elementów systemu bezpieczeństwa obsługujących niniejszy podmiot, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
   2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   3. Monitoring stanu realizowanych połączeń VPN.
   4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
   5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX
   6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   7. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę
   8. Przepustowość Firewall'a: nie mniej niż 7 Gbps

9. Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 480 GB. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
    - Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,5 Gbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 250Mbps
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.

21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla pakietów obejmujących: Kontrolę aplikacji, IPS, Antywirus, Antyspam, Web Filtering, Sandbox, ochrona systemów mobilnych , upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres min: 36 miesięcy.
31. Gwarancja oraz wsparcie

1) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5.

   Oferent winien przedłożyć dokumenty:

   - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
   - oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
   - certyfikat ISO 9001 podmiotu serwisującego

3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

32. Instalacja, konfiguracja i wdrożenie w siedzibie Zamawiającego na podstawie wytycznych i polityk przekazanych przez przedstawicieli Zamawiającego

33. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenie do analizy ruchu sieciowego firmy Fortinet, które będzie wykorzystywane z dostarczanymi urządzeniami UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenie do analizy ruchu sieciowego na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów.**

3.2. Urządzenie UTM Typ 2 – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących niniejszy podmiot, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX
6. System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 28 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 3 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 1600 Mbps
10. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)

- Możliwość analizy ruchu szyfrowanego protokołem SSL
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1200 Mbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 180 Mbps
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych

- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla pakietów obejmujących: Kontrolę aplikacji, IPS, Antywirus, Antyspam, Web Filtering, Sandbox, ochrona systemów mobilnych , upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres min: 36 miesięcy.
31. Gwarancja oraz wsparcie

1) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5.

   Oferent winien przedłożyć dokumenty:
   - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
   - oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
   - certyfikat ISO 9001 podmiotu serwisującego
3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami,

technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

32. Instalacja, konfiguracja i wdrożenie w siedzibie Zamawiającego na podstawie wytycznych i polityk przekazanych przez przedstawicieli Zamawiającego.

33. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenie do analizy ruchu sieciowego firmy Fortinet, które będzie wykorzystywane z dostarczanymi urządzeniami UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenie do analizy ruchu sieciowego na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów.**

3.3. Przełącznik sieciowy – switch – 3 szt.

L.p.	**Opis przedmiotu/funkcji/parametrów**	**Opis parametrów oferowanego towaru**
1.	Przełącznik musi posiadać architekturę umożliwiającą przełączanie w warstwie 2 ethernet i 3 ipv4 oraz ipv6.	
2.	Przełącznik musi być wyposażony w poniższe porty	
2.1	co najmniej 48 portów dostępowych Ethernet 10/100/1000Base-T IEEE 802.3z Auto-MDI/MDIX	
2.2	co najmniej 4 porty uplink 10 Gigabit Ethernet SFP+, obsługujące co najmniej moduły SFP TX, SX, LX/LH, LH/ZX, zgodne ze standardem IEEE 802.3z, oraz SFP+ LR,SR.	
2.3	Każdy przełącznik musi być wyposażony w: 3 moduły SFP+ LR 10km w pełni kompatybilny z modułami oferowanymi przez producenta przełącznika wraz z obsługą funkcjonalności DOM (pomiar temperatury, prądu i mocy sygnału optycznego; 1 moduł SFP+ 10-Gigabit Ethernet Direct Attach do długości min 3m; 2 kabele krosowe FO SC-LC o długości 5m; 1 kabel krosowy FO LC-LC o długości 5m	
2.4	Wszystkie porty muszą pracować z pełną prędkością interfejsów (wire-speed) dla pakietów dowolnej wielkości, czyli przełącznik musi mieć wydajność ponad 100 Mpps (130 Mpps łącznie z portami stackującymi).	
3.	Przełącznik jest dedykowanym urządzeniem sieciowym o wysokości 1U, przystosowanym do montażu w szafie rack 19'' oraz posiada oprzyrządowanie niezbędne do zamocowania w takiej szafie.	
4.	Przełącznik musi być wyposażony w minimum jeden zasilacz AC, przystosowany do zasilania z sieci 230V/50Hz.	

5.	Przełączniki muszą posiadać możliwość łączenia w stos, tak że 10 przełączników jest widocznych w sieci jako jedno urządzenie bez utraty wymaganych funkcjonalności. Każdy switch musi posiadać co najmniej 2 porty stackujące o przepustowości nie mniejszej niż 10 Gb/s każdy, jednocześnie w obie strony; oraz co najmniej jeden kabel stackujący o długości nie mniejszej niż 50 cm.	
6.	Przełącznik obsługuje co najmniej 16000 adresów MAC, w tym co najmniej 1000 adresów MAC opisanych statycznie w konfiguracji.	
7.	Przełącznik obsługuje sieci VLAN zgodnie z IEEE 802.1Q w ilości nie mniejszej niż 1000 z zakresu 1-4090 VLAN ID oraz protokół MVRP.	
8.	Urządzenie obsługuje agregowanie połączeń zgodnie z IEEE 802.3AD, nie mniej niz 6 grup LACP do 8 portów każda. Przy wysyłaniu pakietu IP przez interfejs LACP do wyznaczenia fizycznego portu na który pakiet będzie wysłany jest brany pod uwagę co najmniej adres IP źródłowy i docelowy tego pakietu, w przypadku protokołów TCP i UDP również numery portów, a dla innych protokołów co najmniej adres źródłowy i docelowy, lub źródłowe i docelowe adresy MAC.	
9.	Urządzenie obsługuje filtrowanie ruchu wejściowego i wyjściowego co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4 IPv4 (pole TTL protokołu IP może być obsługiwane tylko przy filtrowaniu ruchu wejściowego na interfejsach warstwy 3). Urządzenie realizuje sprzętowo nie mniej niż 500 reguł filtrowania ruchu. Jest dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.	
10.	Przełącznik obsługuje ramki jumbo (9216 bajtów) na wszystkich interfejsach.	
11.	Przełącznik jest przystosowany do pracy ciągłej przy temperaturze otoczenia z zakresu 0 – 45^{o}C.	
12.	Przełącznik jest wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania	
13.	Przełącznik umożliwia wgranie systemu operacyjnego z zewnętrznego nośnika danych poprzez łącze szeregowe RS-232, USB lub dedykowany port ethernetowy. Musi istnieć możliwość ustawienia restartu urządzenia w zadanym terminie.	
14.	Zarządzanie urządzeniem musi być możliwe za pośrednictwem interfejsu linii komend (CLI) przez port konsoli oraz zdalnie przez telnet lub ssh przy użyciu zarówno protokołu IPv4 jak i IPv6.	
15.	Urządzenie umożliwia zapisanie aktualnej konfiguracji w postaci tekstowej (może być skompresowana jeśli istnieje niezależny, bezpłatny program do jej rozpakowania) w wewnętrznej pamięci nieulotnej oraz na urządzeniach zewnętrznych przy pomocy protokołu tftp, ftp lub scp. Istnieje możliwość modyfikowania konfiguracji poza urządzeniem i ponownego jej wczytania do urządzenia.	
16.	Przełącznik generuje logi dotyczące zdarzeń na nim zachodzących.	

	Użytkownik ma dostęp do dokumentacji producenta urządzenia z wyjaśnieniami znaczenia poszczególnych wpisów w logach. Logi te są dostępne lokalnie na urządzeniu oraz przesyłane do innych urządzeń z użyciem protokołu syslog (przy użyciu protokołu ipv4 lub ipv6, zależnie od konfiguracji dokonanej przez użytkownika). Istnieje możliwość uszczegóławiania logów (tryb debug) dotyczących konkretnych usług (np. STP, 802.1x itp.)	
17.	Przełącznik umożliwia ustawienie limitów pakietów akceptowanych na wskazanych portach w jednostce czasu (tzw. rate-limit). Przełącznik odrzuca pakiety przekraczające limit. Istnieje możliwość ustawiania limitów pakietów indywidualnie dla każdego interfejsu.	
18.	Przełącznik umożliwia ustawienie limitów pakietów typu broadcast oraz unknown unicast w jednostce czasu indywidualnie na każdym interfejsie. Przełącznik odrzuca pakiety przekraczające zadany limit.	
19.	Urządzenie umożliwia dynamiczne przyporządkowywanie komputerów do VLANu na podstawie adresu MAC (tzw. dynamic vlans lub MAC based vlans).	
20.	Urządzenie obsługuje Private VLANs (across switches).	
21.	Urządzenie obsługuje protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9.	
22.	Urządzenie udostępnia za pomocą protokołu SNMP i interfejsu CLI co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych portach. Ponadto istnieje możliwość obsługi liczników odebranych ramek zawierających błędy na poszczególnych interfejsach oraz liczniki ramek których nie udało się wysłać lub wystąpiły błędy podczas ich wysyłania.	
23.	Dostępna jest funkcja kopiowania (mirroring) ruchu dla pakietów spełniających warunki określone w odpowiednim filtrze.	
24.	Urządzenie posiada możliwość diagnostyki kabla, TDR (Time Domain Reflectometer) na wszystkich portach 10/100/1000BASE-T. Urządzenie pozwala na konfigurowanie maksymalnej, rozgłaszanej w czasie autonegocjacji, prędkości portu w standardzie 10/100/1000BASE-T.	
25.	Przełącznik umożliwia zdefiniowanie czasu po jakim będzie próbował aktywować porty wyłączone automatycznie ze względu na nieprawidłowości występujące w przyłączonych do nich częściach sieci (errdisable recovery).	
26.	Przełącznik posiada funkcjonalność netFlow, netflow lite lub równoważną (np. RFC3176 sFlow) umożliwiającą monitorowanie ruchu w warstwach 3 do 4 modelu OSI dla pakietów IPv4.	
27.	Przełącznik obsługuje protokół Spanning Tree i Rapid Spannig Tree, a także Multiple Spanning Tree (nie mniej niż 16 instancji MSTP) oraz VLAN Spanning Tree Protocol (lub równoważny) dla co najmniej 128 vlan-ów.	

28.	Przełącznik posiada możliwość wyłączenia Spanning Tree oraz filtrowania (ignorowania) ramek BPDU na wskazanych portach.	
29.	Przełącznik udostępnia informacje dla każdej instancji SPT, kiedy przyszedł ostatni pakiet TCN (Topology Change Notification) oraz liczniki pakietów TCN dla każdej instancji SPT lub informację z którego interfejsu przyszedł ostatni pakiet TCN.	
30.	Switch posiada opcję definiowania zapasowego portu dla portu podstawowego, tzn. tylko jeden z dwóch interfejsów jest aktywny w danej chwili	
31.	Przełącznik obsługuje protokół LLDP i LLDP-MED, w tym przydział numeru VLANu i klasy QOS dla telefonów VoIP.	
32.	Urządzenie posiada mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu może odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie obsługuje sprzętowo nie mniej niż 8 kolejek na port fizyczny, w tym możliwość zdefiniowania co najmniej jednej kolejki jako kolejki priorytetowej (strict priority) oraz co najmniej jedna kolejka umożliwia pracę w trybie shaping (wygładzania ruchu).	
33.	Przełącznik obsługuje IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie, autoryzowanych każdy indywidualnie. Przełącznik przypisuje ustawienia dla użytkownika na podstawie atrybutów (co najmniej VLAN oraz reguła filtrowania ruchu) zwracanych przez serwer RADIUS, dostępny zarówno przez ipv4 jak i ipv6. Istnieje możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik wspiera co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.	
34.	Przełącznik umożliwia określanie maksymalnej liczby adresów MAC dopuszczalnych na wskazanym porcie. Po przekroczeniu limitu dopuszczalnych adresów MAC pakiety z adresami źródłowymi MAC nie znajdującymi się w zbudowanej tablicy MAC będą ignorowane.	
35.	Przełącznik obsługuje protokół MVR (Multicast VLAN Registration).	
36.	Przełącznik obsługuje sprzętowo takie mechanizmy bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, IP Source Guard, DHCP Snooping (wraz z obsługą opcji 82), dla protokołu ipv4 i ich odpowiedniki w protokole ipv6, tzn. Negihbor Discover Inspection oraz filtruje Router Advertisements na niezaufanych portach.	
37.	Przełącznik posiada funkcjonalność IGMP (v2, v3) oraz MLD (v1 i v2) snooping i wysyła ramki multicastowe tylko do nasłuchujących klientów. Funkcjonalność ta nie zakłóca poprawnej pracy multicastów IPv6, w tym standardu Neighbor Discovery.	

38.	Przełącznik musi obsługiwać co najmniej 500 tras routingu unicast ipv4 i 500 tras unicast ipv6 jednocześnie, co najmniej 200 pozycji ARP i 500 tras multicast ipv4/IGMP groups i ipv6. Przełącznik potrafi pracować w trybie proxy ARP oraz wykonywać DHCP relay na zadanych interfejsach.	
39.	Urządzenia muszą być nieużywane, fabrycznie nowe, tzn. nie starsze niż 6 miesięcy i nie przewidziane do wycofania z produkcji, pochodzić z legalnych kanałów dystrybucji producenta sprzętu. Urządzenia muszą posiadać dożywotnią gwarancję producenta (tzn. co najmniej 3 lat od momentu ogłoszenia terminu zakończenia produkcji). Pomoc techniczna oraz szkolenia z produktu muszą być świadczone w języku polskim. Nowe krytyczne aktualizacje wersji firmware muszą być ogólnodostępne lub Zamawiający musi mieć zapewniony dostęp do nowych wersji oprogramowania przez co najmniej 5 lat od podpisania protokołu odbioru. Zamawiający musi mieć zapewniony dostęp do wszystkich instrukcji użytkownika opublikowanych przez producenta urządzenia oraz dokumentacji do modułów i oprogramowania dostarczonego w ramach realizacji zamówienia. Zamawiający musi mieć możliwość zgłaszania Producentowi błędów w działaniu oprogramowania urządzenia oraz możliwość pobierania poprawek poprzez oficjalne kanały wsparcia.	
40.	Dopuszcza się aby wymagane standardy były obsługiwane w wersjach nowszych niż wymienione powyżej.	
41.	**Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy JUNIPER. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami JUNIPER zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.). W wypadku dostarczenia innych urządzeń niż urządzenia marki JUNIPER wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, w ośrodku szkoleniowym na terenie Dolnego Śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. W wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.**	

4. **Wymagania dotyczące gwarancji**

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.