Zintegrowane urządzenie sieciowe typu UTM dla Uczelnianego Centrum Informatycznego

1. Komplet składający się z dwóch (2) urządzeń klasy wraz z subskrypcją zabezpieczeń, zgodną z opisem poniżej.
2. Zaoferowane rozwiązanie kompletu urządzeń klasy UTM ma być dostarczone, zainstalowane i skonfigurowane według zaleceń Zamawiającego w jego siedzibie w Częstochowie przy ul. Dąbrowskiego 69, w szczególności w zakresie pełnej migracji konfiguracji z obecnie używanego rozwiązania UTM Zamawiającego na system docelowy. Zamawiający posiada obecnie UTM marki Sophos model XG330 ver.2.
3. Wykonawca zobowiązuje się do przeprowadzenia na własny koszt szkolenia dla 3 administratorów w zakresie wdrożenia i zarządzania dostarczonymi urządzeniami w terminie ustalonym z Zamawiającym. Szkolenie musi trwać nie krócej aniżeli 16 godzin i być zakończone testem oraz uzyskaniem dokumentu ukończenia kursu administracyjnego. Zamawiający nie narzuca formy szkolenia i dopuszcza szkolenie on-line. Szkolenie musi odbywać się w formie praktycznych warsztatów. Niedopuszczalne jest przeprowadzenia szkolenia w formie odtworzenia nagranego szkolenia.

ARCHITEKTURA SYSTEMU
1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, złożonej z dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności typu Active-Passive, o specyfikacji opisanej poniżej 2. Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
1. Metalowa obudowa o wysokości max. 2U przeznaczona do montażu w szafie RACK 19'' 2. Obsługa nielimitowanej ilości hostów w sieci chronionej. 3. Rozwiązanie musi być wyposażone w wielordzeniowy procesor x86 wraz z dedykowanym procesorem do analizy ruchu dla warstwy aplikacji. 4. Minimalna liczba i typ interfejsów fizycznych: 8x GE (IEEE 1000Base-T), 8x 10GE (IEEE 10GBase-X), 2x 40GE (IEEE 40GBase-X), MGMT: 1 x RJ45lub 1 x COM Micro-USB, Modem USB: 1 x USB 3.0, 5. Zainstalowane moduły światłowodowe SFP+ jednomodowe LC Duplex: 4 szt. 6. Możliwość rozbudowy urządzenia o dodatkowe interfejsy: 8x 10GE (IEEE 10GBase-X) 7. Minimalna liczba nowych połączeń na sekundę: 400 000 8. Minimalna liczba jednoczesnych połączeń: 32 000 000 9. Minimalna przepustowość Firewall: 100 000 Mbps 10. Minimalna przepustowość IPS: 40 000 Mbps 11. Minimalna przepustowość Threat Protection: 12 000 Mbps 12. Minimalna przepustowość IPSec: 5 000 Mbps 13. Zintegrowane dwa dyski SSD do celów logowania i raportowania o pojemności nie mniejszej niż 480 GB każdy ze sprzętowym RAID-1 14. Zintegrowany wielofunkcyjny wyświetlacz LCD lub LED

15. Zainstalowany wewnętrzny redundantny zasilacz sieciowy 230V

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej: ping, traceroute, name lookup, route lookup 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych oraz wyświetlania tablicy ARP. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i możliwością wycofywania (rollback). 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, Dodawanie tego typu obiektów musi być możliwe bezpośrednio podczas tworzenia reguły zapory sieciowej. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. 10. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 11. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 12. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie oraz tygodniowo 13. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)

	14. System ochrony musi umożliwiać konfigurację jako klaster złożony z dwóch aktywnych urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active (po zakupie dodatkowej licencji i/lub subskrypcji)
Zapora sieciowa, konfiguracja sieciowa oraz routing	1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak sieć, użytkownik, grupa oraz strefy 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Rozwiązanie musi zapewniać możliwość tworzenia reguł w oparciu o relacje między strefami zapory sieciowej 5. Rozwiązanie musi oferować możliwość definiowania własnych stref zapory sieciowej. 6. Rozwiązanie musi pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. 7. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 8. System musi zapewniać ochrona przed skanowaniem portów (portscan blocking). 9. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 10. Rozwiązanie musi zapewniać obsługę routingu statycznego. 11. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF). 12. System musi oferować wsparcie dla IGMP snooping. 13. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą STP. 14. System musi oferować funkcjonalność serwera DHCP i DHCP Relay. 15. System musi oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. 16. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 17. Rozwiązanie musi umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. 18. Wymagane jest by rozwiązanie zapewniało obsługę modemów USB LTE jako zapasowe łącze awaryjne. 19. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 20. System musi zapewniać pełną obsługę usług DNS oraz NTP.
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.

	2. Rozwiązanie musi pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity muszą być przyznawane cykliczne lub niecykliczne. 3. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	1. Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. 2. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 3. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 4. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 5. Dodatkowo system musi umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego 6. System musi oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. 7. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 8. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników	1. Rozwiązanie musi udostępniać plik instalacyjny agenta do autentykacji w sieci. 2. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 3. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows, Mac OS X, Linux, iOS, Android 4. Rozwiązanie musi umożliwiać zmianę nazwy użytkownika oraz hasła. 5. Rozwiązanie musi oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 2. Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). 3. Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5 – tzw. Clientless VPN

OCHRONA SIECI	
IPS	1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 5000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur 5. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi zapewniać skanowanie plików w czasie rzeczywistym 4. Rozwiązanie musi oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów. 5. System musi oferować funkcję Web cache dla ograniczenia zużycia pasma. 6. System musi filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. 7. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 8. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 9. Rozwiązanie musi zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS. 10. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	1. Rozwiązanie musi oferować bazę danych opisująca co najmniej 2000 aplikacji. 2. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 3. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 4. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla kategorii stron lub aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/total. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.

	3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	1. Rozwiązanie musi oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub jako MTA 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 4. System musi umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego. 5. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 6. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 7. Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar. 8. System musi wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości. 9. Rozwiązanie musi oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora. 10. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 11. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów IP i adresów email. 12. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka. Dopuszcza się zastosowanie modułu wbudowanego w urządzenie lub poprzez dostarczenie dedykowanego urządzenia tego samego producenta.
OCHRONA SERWERÓW APLIKACYJNYCH WEB	
WAF	Rozwiązanie musi posiadać dodatkowy moduł ochrony klasy Web Application Firewall o poniższej funcjonalności: 1. Funkcjonalność oparta o mechanizm Reverse Proxy. 2. Rozwiązanie musi oferować mechanizm URL hardening 3. Rozwiązanie musi oferować mechanizm Form hardening. 4. Rozwiązanie musi oferować ochronę przed SQL injection. 5. System musi zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL). 6. System musi pozwalać na podpisywanie plików cookies. 7. Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych.

	8. Rozwiązanie musi oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing). 9. System musi umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych. 10. System musi umożliwiać stosowanie operatorów logicznych AND/OR.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	Rozwiązaniem musi posiadać dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll. 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie mus umożliwiać dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .7z, .cab. 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS. 6. System musi oferować ochronę ze średnim realnym czasem analizy kodu poniżej 180 sekund. 7. System musi oferować szczegółowe raporty wyników analizy.
LOGOWANIE I RAPORTOWANIE	
	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi umożliwiać wysyłanie raportów poprzez email. 6. Rozwiązanie musi generować raporty w PDF/HTML i XLS. 7. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 8. System musi zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym dla każdego z łącza 9. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację

	10. Rozwiązanie musi oferować możliwość zanonimizowania danych w raportach. 11. System musi pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.
POZOSTAŁE	
Certyfikaty	Urządzenie musi posiadać certyfikaty: CE, FCC Class A,

PODSTAWOWE WYMAGANIA

Zamawiający wymaga dostarczenia i montażu urządzeń we wskazanej lokalizacji (węzeł sieciowy przy ul. Dąbrowskiego 69 w Częstochowie).
Wykonawca będzie zobowiązany:
• wraz z urządzeniami należy dostarczyć:
  • 16 wkładek 10GE (IEEE 10GBase-X) niskiej mocy emisji,
  • 2 wkładki 40GE (IEEE 40GBase-X) niskiej mocy emisji,
  • 16 patchcordów światłowodowych 3m,
• przenieść obecnie używaną konfigurację na nowy komplet urządzeń,
• przeprowadzić testy funkcjonalne i wydajnościowe na środowisku testowym,
• aktywować wszystkie zakupione licencje,
• zaktualizować urządzenia i oprogramowanie do najnowszej wersji,
• zainstalować i skonfigurować oprogramowanie zarządzające,
• przeprowadzić przełączenie z nowych urządzeń na nowe (**ze względu na konieczność zachowania dostępności Uczelni z zewnątrz, dopuszczalna przerwa w dostępie do usług nie może być dłuższa niż 5 min!**) – **Składając ofertę, Wykonawcy oświadcza, że potwierdza zdolność techniczną i personalną do przeprowadzenia wymaganego przełączenia w wymaganym reżimie czasowym**,
• przeprowadzić testy funkcjonalne i wydajnościowe na środowisku produkcyjnym,
• przeprowadzić symulację awarii i przełączenia klastra z urządzenia na urządzenie,
• przeprowadzić co najmniej 16-godzinne szkolenie stanowiskowe dla 3 administratorów z podstawowej obsługi urządzeń i oprogramowania.

GWARANCJA I SERWIS
Wymagania ogólne dla dostarczanych rozwiązań :
• Dostarczone urządzenia musza być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji. • Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki, • Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, • Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień dostawy, • Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna, • Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Warunki gwarancji i serwisu :

- Na dostarczany sprzęt musi być udzielona **min. 60-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,
- Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu,
- Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych, diagnozę usterki i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki,
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (od poniedziałku do piątku, w godzinach 8-17), fax, e-mail lub WWW (przez całą dobę),
- Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań,
- W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki. Dostarczony sprzęt zastępczy musi zostać skonfigurowany w sposób umożliwiający mu podjęcie pracy zgodnie z poprzednią funkcją jaką pełnił w infrastrukturze zamawiającego,
- Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach 8-16. Gwarantowane min. 30h pomocy technicznej do wykorzystania w trakcie trwania gwarancji.

Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:

- bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji,
- dostęp do dokumentacji sprzętu i oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producenta.

Zamawiający w momencie odbioru otrzyma:

- subskrypcje obejmujące wszystkie wymagane moduły,
- możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania subskrypcji.