Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

Spis treści

I. Łącza do Internetu. 2
II. Dostawa routerów. 3
III. Dostawa Firewalli. 4
IV. Wdrożenie. 9
V. Poziom świadczenia usługi. 10
VI. Szkolenia. 11

I. Łącza do Internetu.

Wykonawca dostarczy łącza internetowe zgodnie z poniższymi wymaganiami:

<table>
<tr><th>Ozn.</th><th>Opis</th></tr>
<tr><td>LI
01</td><td>Wykonawca dostarczy łącza do Internetu, spełniające wymagania przedstawione w poniższej tabeli:
Tabela 1. Wymagania w zakresie łączy do Internetu
<table>
<tr><th>Lokalizacja</th><th>Konfiguracja węzła</th><th>Łącze główne</th><th>Łącze zapasowe</th></tr>
<tr><td>Warszawa,
ul. Podleśna 61</td><td>2PE+2CE</td><td>1 Gb/s</td><td>1 Gb/s</td></tr>
</table>
Usługa będzie świadczona przez 48 miesięcy od dnia wskazanego w umowie.</td></tr>
<tr><td>LI
02</td><td>Wykonawca wspólnie z Zamawiającym uzgodnią w jaki sposób łącza internetowe będą się wzajemnie zastępowały. Zamawiający posiada 2 dodatkowe punkty styku z Internetem w Krakowie i Gdyni, przyznaną przestrzeń adresową Provider Independent (PI) oraz Autonomous System Number (ASN).</td></tr>
<tr><td>LI
03</td><td>Do adresacji łączy internetowych Wykonawca wykorzysta udostępnioną przez IMGW-PIB pulę 254 publicznych adresów IP. Pula adresowa należy do klasy Provider Independent (PI) przydzielonej przez RIPE NCC (Regional Internet Registry –Europa) dla potrzeb IMGW-PIB. Jeżeli podczas uruchamiania sieci pojawi się potrzeba przydzielenia dla któregoś z łączy internetowych dodatkowych adresów, Wykonawca przekaże do dyspozycji Zamawiającego odpowiednią dodatkową pulę adresów.</td></tr>
<tr><td>LI
04</td><td>Łącza do Internetu zostaną zrealizowane jako wydzielone fizyczne łącza, zakończone stykiem w technologii Gigabit Ethernet 1000BASE-T.</td></tr>
<tr><td>LI
05</td><td>Zostaną zainstalowane dwa łącza do Internetu o niezależnym przebiegu, do różnych punktów dostępowych (routerów szkieletowych) sieci Wykonawcy, zakończone routerami operatora zgodnie z wymaganiami opisanymi w punkcie II. Dostawa routerów.
Zamawiający wymaga, aby połączenia z Internetem w lokalizacjach:
• „Gdynia" łącze do operatora internetowego TASK,
• „Kraków" łącze do operatora Cyfronet,
były połączeniami zapasowymi dla połączeń do Internetu w Warszawie.
Zamawiający wymaga dodatkowo aby podstawowym wyjściem użytkowników do Internetu były w zależności od adresu sieci, w której są użytkownicy łącza w Krakowie, Gdyni lub Warszawie, a w przypadku awarii zastępowały się wzajemnie.</td></tr>
<tr><td>LI
06</td><td>Dla łączy w Warszawie, Wykonawca uruchomi usługę polegającą na Ochronie przed atakami DDoS w postaci:
• TCP SYN flood,
• UDP flood (w tym DNS reflection),
• HTTP GET flood,
• HTTP POST flood,</td></tr>
</table>

	• ICMP flood, • IGMP flood, • invalid packets, • IP fragments, • IP NULL • DNS flood • SIP request flood, • SSL negotiation. System musi zapewniać możliwość filtrowania ataków o wielkości przynajmniej 10Gbps i ochronę w warstwach ISO/OSI: od 3 do 7, przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Czas reakcji na zaistniałe zdarzenie lub zgłoszenie Zamawiającego maksymalnie 15 minut (SLA). Wymagane jest automatyczne tworzenie i przesyłanie raportów po każdej mityzacji/obronie dla ataku przekraczającego 100 Mbps i zbiorczy raport miesięczny dostarczany Zamawiającemu.

II. Dostawa routerów.

Wykonawca dostarczy 4 routery, które spełnią następujące wymagania:

Ozn.	Opis
RO 01	Routery będą wyposażone minimum w 2 porty Gigabit Ethernet 1000BASE-T.
RO 02	Urządzenia obsłużą ruch 1Gbps na łączu symetrycznym (strumień wejściowy 1Gbps i strumień wyjściowy 1Gbps).
RO 03	Routery będą w pełni wspierały protokoły OSPF w wersjach 2 i 3.
RO 04	Routery będą w pełni wspierały protokół BGP w wersji 4 z obsługą 4 bajtowych ASN.
RO 05	Routery muszą posiadać wsparcie dla funkcjonalności Policy Based Routing.
RO 06	Routery będą wspierały Vlany - 802.1Q.
RO 07	Routery będą wspierały protokół HSRP i/lub VRRP.
RO 08	Routery będą wspierały listy kontroli dostępu w oparciu o: • adresy IP źródłowe i docelowe, • protokoły IP,

	• porty TCP/UDP, • opcje IP, • flagi TCP, • wartości TTL.
RO 09	Routery będą wspierały obsługę NAT i PAT.
RO 10	Tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
RO 11	Obsługa protokołu GRE oraz mechanizmu honorowania IP Precendence dla ruchu tunelowanego.
RO 12	Obsługa mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+.
RO 13	Ilość pamięci pozwalającą na przechowywanie i aktualizowanie dwóch pełnych tablic BGP oraz ruchu wewnętrznego OSPF i 10 sesji GRE.
RO 14	Monitorowanie zdarzenia oraz generowanie akcji takich jak: • wykonanie komendy z poziomu linii poleceń urządzenia, • wygenerowanie SNMP trap.
RO 15	Obsługa protokołów SSH, Syslog, SNMP w wersji 2c i 3 oraz NetFlow/JFlow.
RO 16	Możliwość montażu w szafie RAC 19" (odpowiednie mocowania w zestawie).

III. Dostawa Firewalli.

Wykonawca dostarczy 4 firewalle o następujących funkcjonalnościach:

Ozn.	Opis
FW 01	System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów i użytkowników w sieci wewnętrznej.
FW 02	Firewalle muszą być dostarczone jako specjalizowane urządzenia zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość - sprzęt i oprogramowanie musi być dostarczone i wspierane przez jednego producenta.
FW 03	Firewalle muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer).

FW 04	Firewalle muszą posiadać przepływność z włączoną funkcją kontroli aplikacji, kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering): • 2 Gbit/s dla dwóch urządzeń zainstalowanych w Warszawie, • 1 Gbit/s dla urządzeń zainstalowanych w Krakowie i Gdyni.
FW 05	System zabezpieczeń firewall musi być wyposażony w co najmniej: • 6 portów 1000BASE-TX dla dwóch urządzeń zainstalowanych w Warszawie, • 4 porty 1000BASE-TX dla urządzeń zainstalowanych w Krakowie i Gdyni.
FW 06	Firewalle muszą 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.
FW 07	Firewalle zgodnie z ustaloną polityką muszą prowadzić kontrolę ruchu sieciowego pomiędzy strefami bezpieczeństwa na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
FW 08	Polityk zabezpieczeń dla firewalli będą uwzględniać co najmniej: • strefy bezpieczeństwa, • adresy IP klientów i serwerów, • protokoły i usługi sieciowe, • aplikacje, • kategorie URL, • użytkowników aplikacji, • reakcje zabezpieczeń, • rejestrowanie zdarzeń i alarmowanie, • zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne).
FW 09	Firewalle muszą 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.
FW 10	Firewalle muszą bezpośrednio realizować zadania kontroli aplikacji określone w politykach zabezpieczeń.
FW 11	System zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez firewalle.
FW 12	System zabezpieczeń musi umożliwiać 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 itp..
FW 13	System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. firewalle blokują (bezpośrednio) wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa są wskazane jako dozwolone.

FW 14	Firewalle muszą umożliwiać deszyfrowanie ruchu SSL w celu głębokiej inspekcji (tak samo jak dla ruchu nieszyfrowanego).
FW 15	Firewalle muszą umożliwiać wyłączenie deszyfrowania ruchu SSL na podstawie automatycznie aktualizowanej przez producenta listy adresów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nieuwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning").
FW 16	Firewalle muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
FW 17	System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, LDAP, serwerami Terminal Services oraz syslog). 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.
FW 18	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron http. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
FW 19	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
FW 20	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej. Baza sygnatur anty-wirus musi być regularnie aktualizowana w sposób automatyczny.
FW 21	System zabezpieczeń firewall musi posiadać moduł wykrywania i blokowania ataków exploit w warstwie 7 modelu OSI IPS/IDS. Baza sygnatur IPS/IDS musi być regularnie aktualizowana w sposób automatyczny.
FW 22	System zabezpieczeń firewall musi posiadać moduł inspekcji anty-spyware. Baza sygnatur anty-spyware musi być regularnie aktualizowana w sposób automatyczny.
FW 23	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
FW 24	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).
FW 25	System zabezpieczeń firewall musi posiadać możliwość tworzenia reguł na podstawie FQDN .
FW 26	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.

FW 27	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.
FW 28	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
FW 29	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.
FW 30	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
FW 31	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.
FW 32	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.
FW 33	System zabezpieczeń firewall musi umożliwiać inspekcję tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
FW 34	System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
FW 35	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.
FW 36	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla: • adresów IP, grup adresów IP i sieci, • poszczególnych użytkowników, • w zakresie oznaczania pakietów znacznikami DiffServ, • dla dowolnych aplikacji. W tym ustawienia priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 3 klas dla różnego rodzaju ruchu sieciowego.

FW 37	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.
FW 38	Firewalle będą wspierały protokoły SNMP, SNMP Trap, NetFlow/JFlow, Syslog.

Do dostarczonych firewalli Wykonawca dostarczy system do zarządzania i monitorowania o następujących funkcjonalnościach.

Ozn.	Opis
FZ 01	Interfejs zarządzania: • graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW, • linia poleceń (CLI).
FZ 02	Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie, zatwierdzania i cofania zmian konfiguracji, przeglądanie różnic, dostęp do historii zmian.
FZ 03	Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
FZ 04	Możliwość utworzenia wspólnych elementów konfiguracyjnych dla wszystkich zarządzanych firewalli, edycja jednego obiektu spowoduje zmianę na wszystkich firewallach.
FZ 05	Możliwość zdefiniowania wielu administratorów o różnych uprawnieniach.
FZ 06	Możliwość uwierzytelniania administratorów za pomocą: • bazy lokalnej, • serwera LDAP, • RADIUS, • TACACS+ • Kerberos.
FZ 07	Możliwość suwania logów i raportów przetrzymywanych na urządzeniu zgodnie z określonym harmonogramem.
FZ 08	Możliwość sprawdzenia wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
FZ 09	Możliwość wysyłania logów do różnych serwerów Syslog.

FZ 10	Możliwość tworzenia raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny zgodnie z ustalonym harmonogramem.

IV. Wdrożenie.

Ozn.	Opis
RW 01	W terminie 5 dni roboczych od podpisania umowy Wykonawca dostarczy harmonogram wdrożenia wraz z opisem realizacji z uwzględnieniem zastosowanych technologii, informacją o parametrach i zastosowanych mediach transmisyjnych. Proces uruchomienia łączy, instalacji i konfiguracji dostarczonych urządzeń będzie uzgadniany z wyprzedzeniem, pomiędzy przedstawicielami Wykonawcy oraz Zamawiającego. Wykonawca przeprowadzi wdrożenia w dni powszednie, w godzinach od 8 do 16. Wykonawca przedstawi do akceptacji Zamawiającego harmonogram migracji. Migracja od dnia rozpoczęcia do zakończenia nie będzie przekraczać 21dni (w przypadku przekroczenia zostaną naliczane kary umowne).
RW 02	Wykonawca skonfiguruje i uruchomi dostarczone routery (dokona migracji z obecnie wykorzystywanych urządzeń) do pracy w sieci i środowisku Zamawiającego: • 2 routery w Warszawie, • 1 router w Krakowie, • 1 router w Gdyni.
RW 03	Wykonawca skonfiguruje i uruchomi dostarczone Firewalle (dokona migracji z obecnie wykorzystywanych urządzeń – PaloAlto 3020 oraz ASA5540) do pracy w sieci i środowisku Zamawiającego: • 2 firewalle w Warszawie w konfiguracji klastra niezawodnościowego, • 1 firewall w Krakowie, • 1 firewall w Gdyni.
RW 04	Wykonawca skonfiguruje i uruchomi dostarczony system do zarządzania.
RW 05	Na czas migracji Wykonawca zapewni wsparcie inżyniera specjalistę w zakresie technologii routingu (BGP i OSPF), którego zadaniem będzie aktywny udział w rekonfiguracji urządzeń sieciowych Wykonawcy i Zamawiającego na potrzeby migracji.
RW 06	Na czas migracji Wykonawca zapewni wsparcie inżyniera specjalistę w zakresie dostarczonego systemu zabezpieczeń firewall, którego zadaniem będzie aktywny udział w rekonfiguracji urządzeń sieciowych Wykonawcy i Zamawiającego na potrzeby migracji.
RW 07	Wykonawca wykona dokumentację powdrożeniową, która będzie zawierała: • schematy logiczne wraz z opisami, • opis mechanizmu wyboru łącza internetowego, • opis mechanizmu przełączania miejsca rozgłaszania adresacji w BGP.

V. Poziom świadczenia usługi.

SI01	Dla dostarczonych urządzeń Wykonawca zapewni wsparcie serwisowe na poziomie Next Business Day.
SI02	Wykonawca zapewni dostępność usług łączy internetowych na poziome 99,7% w skali roku. Zamawiający będzie klasyfikował awarie łączy na: • **Awarie Krytyczne** – wszystkie awarie, które dotyczą obu łączy, • **Awarie Niekrytyczne** – pozostałe awarie. Wykonawca zapewni usuwanie awarii w czasie nie przekraczającym: • **Awarii Krytycznych – 8 godzin,** • **Awarii Niekrytycznych – 2 dni robocze.** Wykonawca może przez zastosowanie obejścia (np. wykreowanie łącza tymczasowego o parametrach nie gorszych niż łącze zapasowe w danej lokalizacji) sprowadzić awarię krytyczną do awarii niekrytycznej.
SI03	Usługa serwisu technicznego będzie obejmowała usuwanie problemów z siecią oraz dostarczonymi urządzeniami po ich zgłoszeniu przez Zamawiającego na specjalnie do tego celu wydzielony numer telefoniczny dostępny bez przerwy - 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Powyższy numer telefoniczny powinien być dostępny według standardowych stawek operatora lub bezpłatnie, niedopuszczalne jest zastosowanie numeru o podwyższonej płatności (np. 0-700).
SI04	Wykonawca zapłaci kary umowne z tytułu niedotrzymania parametrów SLA: a) Bonifikatę z tytułu niedotrzymania Gwarantowanego Czasu Usunięcia Awarii ustala się na podstawie poniższego wzoru: **Bonifikata za Awarię = (Ta - TG) * KA,** gdzie: • Ta – Czas usunięcia Awarii [h], zaokrąglony wzwyż do pełnej godziny, • TG – Gwarantowany czas usunięcia Awarii [h], • KA – bonifikata w wysokości 4 % miesięcznego abonamentu za łącze. b) Bonifikatę z tytułu niedotrzymania Gwarantowanej dostępności usług transmisji danych ustala się na podstawie poniższego wzoru: **Całkowita bonifikata = [TA – MA * (Tusługi / T)] * KD,** gdzie: • MA – maksymalna liczba godzin Awarii dopuszczalna dla danego Poziomu Usługi [h], • TA – suma czasów trwania wszystkich Awarii w danym roku kalendarzowym [h], • Tusługi – czas korzystania z Usługi Podstawowej w danym roku kalendarzowym [h], • T – liczba godzin w danym roku kalendarzowym [h], • KD – bonifikata w wysokości 4 % miesięcznego abonamentu za łącze. Wynik działania [TA – MA*(Tusługi/T)] –zaokrągla się wzwyż do pełnej godziny.
SI05	Wykonawca zapłaci kary umowne z tytułu opóźnienia w uruchomieniu łączy w stosunku do terminów zawartych w umowie na poziomie 300% miesięcznego abonamentu za łącze, za każdy kolejny rozpoczęty tydzień po terminie zawartym w umowie.

VI. Szkolenia.

a. Wykonawca dostarczy 4 vouchery ważne przez rok od dnia dostawy na szkolenia w języku polskim z dostarczonego systemu zabezpieczeń firewall. Szkolenia będą posiadały autoryzację producenta dostarczonego systemu zabezpieczeń.

- Zakres szkolenia - Konfiguracja i zarządzanie zaproponowanym systemem zabezpieczeń.
- Miejsce szkolenia – certyfikowane przez producenta systemu zabezpieczeń centrum szkoleniowe w Warszawie.
- Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy.

b. Wykonawca dostarczy 4 vouchery ważne przez rok od dnia dostawy na szkolenie z wdrażania i diagnostyki sieci LAN w oparciu o przełączniki sieciowe warstwy 2 (L2) i warstwy 3 (L3). Szkolenie zostanie przeprowadzone przez trenera certyfikowanego przez producenta dostarczonych routerów internetowych:

- Zakres szkolenia:
  - Podstawowe koncepcja oraz projektowanie sieci,
  - Architektur sieci kampusowych,
  - Implementacja „spanning tree",
  - Routing między sieciami VLAN,
  - Implementacja sieci wysokiej dostępności,
  - Implementacja „First Hop Redundancy",
  - Zabezpieczanie sieci kampusowych.
- Miejsce szkolenia – certyfikowane przez producenta dostarczonych routerów centrum szkoleniowe w Warszawie.
- Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy.

c. Wykonawca dostarczy 4 vouchery ważne przez rok od dnia dostawy na szkolenie z zakresu konfiguracji oraz optymalizacji protokołów routingu. Szkolenie zostanie przeprowadzone przez trenera certyfikowanego przez producenta dostarczonych routerów internetowych:

- Zakres szkolenia:
  - Zasady działania sieci i routerów,
  - Implementacja EIGRP,
  - Implementacja OSPF,
  - Konfiguracja i redystrybucja,
  - Implementacja kontroli tras,
  - Korporacyjna łączność internetowa,
  - Hardening routerów i protokołów rutowania.
- Miejsce szkolenia – certyfikowane przez producenta dostarczonych routerów centrum szkoleniowe w Warszawie.
- Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy.

d. Wykonawca dostarczy 4 vouchery ważne przez rok od dnia dostawy na szkolenie z zakresu konfiguracji oraz optymalizacji protokołu routingu BGP. Szkolenie zostanie przeprowadzone przez trenera certyfikowanego przez producenta dostarczonych routerów internetowych:

- Zakres szkolenia:
  - Wprowadzenie do protokołu BGP,
  - Tranzytowe systemy autonomiczne,
  - Atrybuty BGP (mechanizmy wyboru drogi),
  - Filtrowanie routingu i dobór tras w BGP,
  - Rozwiązania typu BGP route reflektor,
  - Rozwiązania typu BGP confederations,
  - Rozwiązania bazujące na Multi-Exit Discriminator,
  - Rozwiązania bazujące na AS-path prepending,
  - Rozwiązania bazujące na BGP communities,
  - Tłumienie niestabilnych ścieżek w BGP (route flap dampenin
  - Łączenie sieci klienckich do sieci Internet Service Provider za pomocą
  - Optymalizacja pracy BGP.
- Miejsce szkolenia - certyfikowane przez producenta dostarczonych routerów centrum szkoleniowe w Warszawie.
- Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy.