Załącznik nr 2a do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - DLA CZĘŚCI 2 (SOPZ)

1. Przedmiotem zamówienia jest **dostawa sprzętu informatycznego dla Miejskiego Centrum Oświaty w Tychach**

Część 2: Dostawa urządzeń infrastruktury sieciowej wraz z modułami i okablowaniem

Adres dostawy przedmiotu zamówienia: Miejskie Centrum Oświaty w Tychach, Al. Piłsudskiego 12 (II piętro bez windy), 43-100 Tychy

2. Wykonawca zobowiązuje się do wykonania przedmiotu zamówienia terminowo, z dochowaniem należytej staranności, na najwyższym poziomie, zgodnie z obowiązującymi zasadami najlepszej praktyki zawodowej, wiedzą techniczną oraz obowiązującymi przepisami prawa, normami oraz z uwzględnieniem profesjonalnego charakteru prowadzonej przez niego działalności.
3. Wszystkie czynności związane z dostawą przedmiotu zamówienia spoczywają na Wykonawcy, który zapewni, na swój koszt transport, rozładunek, wniesienie, ustawienie i montaż w pomieszczeniach wskazanych przez Zamawiającego przy użyciu własnej siły roboczej, narzędzi i materiałów montażowych.
4. Przedmiot zamówienia podczas transportu do miejsca przeznaczenia powinien być opakowany i zabezpieczony w taki sposób, aby zapobiec jego zdekompletowaniu, zniszczeniu lub obniżeniu jego jakości.
5. Odpowiedzialność za szkody powstałe w czasie transportu ponosi Wykonawca.
6. Wykonawca oświadcza, iż dostarczony przedmiot zamówienia jest w pełni zgodny z wymogami Specyfikacji Warunków Zamówienia oraz Szczegółowym Opisem Przedmiotu Zamówienia, a ponadto:
    a. jest fabrycznie nowy, nieuszkodzony, kompletny i nieużywany przed dniem dostarczenia (za wyjątkiem wykonania testów sprawnościowych towaru), bezpieczny i gotowy do pracy,
    b. pochodzi z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej oraz posiada stosowne atesty i certyfikaty zgodne z obowiązującymi przepisami prawa (odpowiednie dla danego przedmiotu zamówienia) dopuszczające go do sprzedaży. Zamawiający ma prawo to zweryfikować, a Wykonawca ma obowiązek udostępnić na wezwanie Zamawiającemu niezbędne dokumenty w celu potwierdzenia powyższego,
    c. istnieje w dacie składania oferty oraz jest oferowany na stronie internetowej producenta,
7. Wykonawca zobowiązany jest przedstawić dokumentację techniczną producenta w języku polskim lub angielskim każdego z elementów przedmiotu zamówienia, potwierdzającą w sposób jednoznaczny zgodność parametrów zaoferowanych sprzętów z zapisami OPZ. Jeżeli dokumentacja producenta nie potwierdza jednoznacznie zgodności ze wszystkimi wymaganymi parametrami opisanymi w OPZ, Wykonawca zobowiązany jest przedstawić stosowne oświadczenie.
8. Oferowane sprzęty muszą mieć pełne wsparcie techniczne producenta. Strona www producenta sprzętu powinna być w języku polskim i zawierać niezbędne sterowniki oraz oprogramowanie narzędziowe dla dostarczonego sprzętu wraz ze wskazaniem ogólnopolskiego numeru infolinii producenta umożliwiającego zgłoszenie awarii sprzętu lub uzyskanie pomocy technicznej.
9. Wykonawca ponosi odpowiedzialność cywilną za szkody i następstwa nieszczęśliwych wypadków powstałe z jego winy, dotyczące pracowników własnych i osób trzecich, powstałe w związku z czynnościami prowadzonymi podczas realizacji przedmiotu zamówienia.
10. Obowiązkiem Wykonawcy jest utrzymanie bieżącego porządku w trakcie dostawy oraz naprawa szkód powstałych w trakcie realizacji przedmiotu zamówienia, w tym uszkodzeń mechanicznych budynku wewnątrz i na zewnątrz. Wszelkie opakowania, wypełniacze oraz inne odpady wniesione

na teren Lokalizacji w ramach dostawy zostaną zutylizowane przez Wykonawcę, chyba że Zamawiający zadecyduje inaczej.

11. Do zakresu przedmiotu zamówienia należy także udzielenie gwarancji i wykonywanie świadczeń wynikających z udzielonej gwarancji.
12. Zamawiający na każdym etapie postępowania i realizacji zamówienia może żądać potwierdzenia aktualnych certyfikatów i atestów dopuszczających produkt do użytkowania i obrotu na rynku polskim.
13. Wykonawca zobowiązany jest niezwłocznie na piśmie poinformować Zamawiającego o wszelkich okolicznościach, które mogą mieć wpływ na realizację postanowień umowy w szczególności o przewidywanym opóźnieniu w dostawie.
14. Na Wykonawcy ciąży odpowiedzialność z tytułu uszkodzenia lub utraty przedmiotu zamówienia aż do chwili jego wydania Zamawiającemu potwierdzonego protokołem odbioru.
    Za dzień wydania uważa się dzień, w którym **wszystkie** elementy przedmiotu zamówienia zostały odebrane przez Zamawiającego.
15. Wykonawca umożliwi Zamawiającemu sprawdzenie dostarczonego przedmiotu zamówienia w celu jego odbioru w miejscu dostawy. Sprawdzenie będzie polegało na upewnieniu się, że przedmiot zamówienia jest wolny od widocznych wad fizycznych, a w szczególności, że odpowiada on wymogom określonym w Szczegółowym Opisie Przedmiotu Zamówienia. Zamawiający w terminie do 10 dni roboczych od daty dostawy towaru, z powyższej czynności sporządzi protokół, który zostanie udostępniony Wykonawcy po wcześniejszym ustaleniu.
16. Wykonawca **dostarczy** przedmiot zamówienia w oryginalnych opakowaniach producenta **i dokona montażu** we wskazanych pomieszczeniach w terminie **do 30 dni kalendarzowych od dnia podpisania umowy w godzinach 8.00 – 15.00 do siedziby Zamawiającego**, własnym transportem, własną siłą roboczą i na własny koszt. Najpóźniej na trzy dni przed terminem dostarczenia przedmiotu zamówienia Wykonawca powiadomi Zamawiającego o terminie dostawy.
17. Po podpisaniu umowy Zamawiający zaleca przeprowadzić wizję lokalną w placówce w celu potwierdzenia lokalizacji montażu, z uwzględnieniem specyfiki pomieszczenia.
18. W budynku znajduje się winda, która dojeżdża jedynie do 4. piętra, w związku z czym konieczne będzie wniesienie przedmiotu zamówienia po schodach.

Dostawa sprzętu sieciowego wraz z montażem i konfiguracją w środowisku informatycznym.

Urządzenie firewall - 2 szt.
Architektura urządzenia, obudowa, interfejsy

1) Urządzenie musi stanowić dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań typu serwerowego bazującego na ogólnodostępnych podzespołach PC ogólnego przeznaczenia.
2) Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3) Urządzenie musi być wyposażone w 8 portów miedzianych Gigabit Ethernet oraz minimum 2 porty 10Gigabit Ethernet definiowane przy pomocy wkładek/twinax.
4) Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych.
5) Urządzenie musi być wyposażone w dedykowany port konsoli/port USB co najmniej 3.0 oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6) Urządzenie musi być wyposażone w dodatkowy port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia,
7) Urządzenie musi mieć możliwość montażu w szafie rack 19” oraz posiadać w zestawie dołączone niezbędne elementy montażowe. Jeśli urządzenie nie jest przystosowane do montażu w szafie rack, należy dostarczyć dedykowany uchwyt od producenta sprzętu.
8) Wysokość urządzenia typu rack nie może przekraczać rozmiaru 1U.

Parametry wydajnościowe

9) Wymagana przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji (AVC) - na poziomie 8,5 Gb/s, a dla modułów AVC oraz systemu IPS - na poziomie 8,5 Gb/s
10) Maksymalna liczba sesji (z kontrolą aplikacji) nie może być mniejsza niż 290 000 z możliwością zestawiania co najmniej 50 000 nowych połączeń na sekundę.
11) Urządzenie musi zapewniać wsparcie dla VPN IPSec na poziomie co najmniej 9 Gb/s.

Funkcjonalność urządzenia

12) Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
13) Urządzenie musi mieć możliwość uruchomienia w trybie firewalla L3, jak i w trybie transparentnym.
14) Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).
15) Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
16) Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT).
17) Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
18) Urządzenie musi zapewniać funkcjonalność tzw. Firewall’a Next-Generation w zakresie:
    a) systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
    b) systemu IPS (Intrusion Prevention System).
19) System musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System musi tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a) Wiedza o użytkownikach – uwierzytelnienie,
    b) Wiedza o urządzeniach – pasywne skanowanie ruchu,
    c) Wiedza o urządzeniach mobilnych,
    d) Wiedza o aplikacjach wykorzystywanych po stronie klienta,
    e) Wiedza o podatnościach,
    f) Wiedza o bieżących zagrożeniach,
    g) baza danych URL.
20) System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM (Security Information and Event Management).
21) Urządzenie musi umożliwiać konfiguracją IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN System

musi umożliwić stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruchu jak i również tzw. „split tunelingu” (funkcja ta musi mieć możliwość konfiguracji per grupa VPN RA).

22) Moduł wykrywania aplikacji (AVC) musi zapewniać:
   a) możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji,
   b) możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług,
   c) wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,
   d) współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez moduł AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
23) Moduł IPS (Intrusion Prevention System) musi zapewniać:
   a) możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez moduł),
   b) możliwość pracy w trybie pasywnym (IDS),
   c) możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
      i. złośliwe oprogramowanie,
      ii. skanowanie sieci,
      iii. ataki na usługę VoIP,
      iv. próby przepełnienia bufora,
      v. ataki na aplikacje P2P,
      vi. zagrożenia dnia zerowego, itp.
   d) możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna),
   e) wiele sposobów wykrywania zagrożeń w tym:
      i. sygnatury ataków opartych na exploitach,
      ii. reguły oparte na zagrożeniach,
      iii. mechanizm wykrywania anomalii w protokołach,
      iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,
   f) możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
   g) mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives),
   h) możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń,
   i) wiele możliwości reakcji na zdarzenia w tym takie, jak:
      i. tylko monitorowanie,
      ii. blokowanie ruchu zawierającego zagrożenia,
      iii. zastąpienie zawartości pakietów,
      iv. zapisywanie pakietów,
   j) możliwość detekcji ataków i zagrożeń opartych na protokole IPv6,
   k) możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
      i. systemach operacyjnych,
      ii. serwisach,
      iii. otwartych portach, aplikacjach,
      iv. zagrożeniach,
   l) możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,
   m) możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.,

n) możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,
o) możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,
p) mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,
q) możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie,
r) obsługę reguł Snort,
s) możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS,
t) mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise),
u) mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa,

24) Moduł filtracji URL musi zapewniać:
a) kategoryzację stron – w co najmniej 70 kategoriach,
b) bazę URL o wielkości nie mniejszej niż 250 mln URL,
25) Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu co najmniej następujących kategorii plików w ruchu sieciowym:
a) pliki systemowe,
b) pliki graficzne,
c) pliki PDF,
d) pliki wykonywalne,
e) pliki multimedialne,
f) pliki pakietu Office,
g) pliki skompresowane.
26) Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w co najmniej następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
27) Urządzenie musi posiadać wbudowany podsystem wykrywania złośliwego oprogramowania (malware) i jego propagacji w strefie chronionej poprzez:
a) sprawdzenie reputacji plików w systemie globalnym,
b) sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze),
c) statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
28) Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
a) pliki wolne od złośliwego kodu,
b) pliki zawierające złośliwy kod,
c) pliki podejrzane,
d) pliki o własnej, zdefiniowanej przez użytkownika kategorii.
29) Podsystem wykrywania oprogramowania złośliwego musi zawierać narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).

Pozostałe wymagania

30) Urządzenie musi być objęte **co najmniej 36-miesięcznym** serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do:
a) wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia,
b) wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia,
c) aktualizacji oprogramowania urządzenia,
d) dostępu do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych.
31) W zakres dostawy wchodzą także licencje dla połączeń VPN zdalnego dostępu:
a) co najmniej **25 szt. licencji** pozwalających na autoryzację komputerów/telefonów
b) wsparcie na licencję również powinno być świadczone w okresie **co najmniej 36 miesięcy**.

System zarządzania oraz składowania logów dla firewall typu 1 - ilość: 1 sztuka

Specyfikacja

1. Wraz z urządzeniem zostanie dostarczona dedykowana platforma zarządzająca oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca może mieć formę maszyny fizycznej lub wirtualnej pracującej pod kontrolę VMware ESXi/KVM i spełnia następujące wymagania:

a) umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym

b) jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego

c) zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria

d) ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm

e) ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami

f) zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany

g) zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe,
uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS

h) zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją

i) ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci

j) daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną prioretyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta

k) ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora

l) zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS

m) ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej

n) zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania

o) zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu

p) zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP

q) zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze

r) zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika

s) zapewnia informowanie o zagrożeniach poprzez

a. wysłanie e-maila,

b. wysłanie trap SNMP,

c. przesłanie informacji do serwera Syslog,

d. uruchomienie skryptu użytkownika

e. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane połączenie

t) posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy

a. aktualnego stanu danego urządzenia,

b. podglądu historii dostępnych zasobów,

c. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)

u) ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym

v) ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
a. dozwolone porty i protokoły
b. dozwolone aplikacje według różnych kategorii
c. dozwolone kategorie stron internetowych (URL filtering)
d. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
e. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne
w) w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia
x) pozwala na łatwą nawigację pomiędzy obiektami. Pozwala podejrzeć, w którym innym obiekcie jest on zagnieżdżony lub w której polityce jest użyty
y) posiada narzędzie do monitorowania połączeń, które zostały sklasyfikowane do odpowiedniej reguły („hit count"). Narzędzie pozwala na monitorowanie jak dużo połączeń zachodzi dla konkretnych reguł w określonej jednostce czasu oraz pozwala na szybkie wyszukanie reguł niepotrzebnych, do których przez zadany okres nie trafił żaden ruch.
z) pozwala na wysłanie na sensor tylko wybranych elementów modyfikowanej konfiguracji
aa) określa przewidywany czas implementacji polityki na sensor przed implementacją
bb) pozwala przed rekonfiguracją na przegląd implementowanych zmian w porównaniu do aktualnych ustawień urządzenia zarządzanego
2. Wsparcie na maszynę wirtualną powinno być dostarczone na okres min. 36 miesięcy.

Przełącznik sieciowy typ 1- 2 szt.

1. Typ przełącznika i minimalna liczba portów:
    a. Typ i liczba portów - 4x 10Gigabit Ethernet copper RJ45/SFP+, 20x 10Gigabit Ethernet SFP+,
    b. 1x port GE do zarządzania OOB,
    c. Zasilanie przez wbudowany zasilacz AC 230 V,
    d. Obudowa 1U, rackmount, z kompletem uchwytów montażowych,
    e. Możliwość stackowania przełączników – do 8 przełączników i do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym: Quality of Service (QoS), sieci VLAN, Link Aggregation (LAG) i port mirroring.
2. Wsparcie wkładek SFP w portach SFP 1G, co najmniej:
    a. Gigabit Ethernet 1000Base-SX zasięg do 500 metrów,
    b. Gigabit Ethernet 1000Base-LX/LH zasięg do 10 km,
    c. Gigabit Ethernet 1000Base-EX zasięg do 40 km,
    d. Gigabit Ethernet 1000Base-ZX zasięg do 70 km,
    e. Wkładka z interfejsem miedzianym 1G RJ-45.
3. Wsparcie wkładek SFP+ w portach SFP+ 10G, co najmniej:
    a. 10Gigabit Ethernet 10GBase-SR,
    b. 10Gigabit Ethernet 10GBase-LR,
    c. 10Gigabit Ethernet 10GBase-ER,
    d. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
    e. Wkładka z interfejsem miedzianym 10G RJ45.
4. Zarządzenie energią:
    a. Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az),
    b. Możliwość wyłączenia diod LED w celu oszczędzania energii.
5. Minimalne parametry wydajnościowe:
    a. Przepustowość przełącznika (Switching capacity): 480 Gbps,
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 357 Mpps,

c. Pamięć DRAM – 1 GB,
d. Pamięć Flash – 512 MB,
e. Obsługa 4000 VLAN,
f. 16000 adresów MA,
g. Wire-speed IPv4 routing – 990 tras statycznych, 128 interfejsów IP,
h. Obsługa ramek jumbo – do 9000 bajtów,
i. 2000 IGMP group,
j. 8 połączeń zagregowanych typu „port channel" per grupa, obsługa 8 grup,
k. Ilość wpisów w listach kontroli dostępu Security ACL – 1000.

Przełącznik sieciowy typ 2- 7 szt.

1. Typ przełącznika i minimalna liczba portów:
   a. Typ i liczba portów – 32x 10/100/1000 POE+ RJ45, 16x 10/100/1000/2500 POE+ RJ45, 4x 10Gigabit Ethernet SFP+,
   b. Budżet mocy dla POE – 740 W,
   c. Zasilanie przez wbudowany zasilacz AC 230 V,
   d. Obudowa 1U, rackmount, z kompletem uchwytów montażowych,
   e. Możliwość stackowania przełączników – do 8 przełączników i do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym: Quality of Service (QoS), sieci VLAN, Link Aggregation (LAG) i port mirroring.
2. Wsparcie wkładek SFP w portach SFP 1G, co najmniej:
   a. Gigabit Ethernet 1000Base-SX zasięg do 500 metrów,
   b. Gigabit Ethernet 1000Base-LX/LH zasięg do 10 km,
   c. Gigabit Ethernet 1000Base-EX zasięg do 40 km,
   d. Gigabit Ethernet 1000Base-ZX zasięg do 70 km,
   e. Wkładka z interfejsem miedzianym 1G RJ45.
3. Wsparcie wkładek SFP+ w portach SFP+ 10G, co najmniej:
   a. 10Gigabit Ethernet 10Gbase-SR,
   b. 10Gigabit Ethernet 10Gbase-LR,
   c. 10Gigabit Ethernet 10Gbase-ER,
   d. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
   e. Wkładka z interfejsem miedzianym 10G RJ-45.
4. Zarządzenie energią:
   a. Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii,
   b. Zapewnia zasilanie PoE podczas restartu urządzenia,
   c. Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az),
   d. Możliwość wyłączenia diod LED w celu oszczędzania energii.
5. Minimalne parametry wydajnościowe:
   a. Przepustowość przełącznika (Switching capacity): 223 Gbps,
   b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 165 Mpps,
   c. Pamięć DRAM – 1 GB,
   d. Pamięć Flash – 512 MB,
   e. Obsługa 4000 VLAN,
   f. 16000 adresów MAC,
   g. Wire-speed Ipv4 routing – 990 tras statycznych, 128 interfejsów IP,
   h. Obsługa ramek jumbo – do 9000 bajtów,
   i. 2000 IGMP group,
   j. 8 połączeń zagregowanych typu „port channel" per grupa, obsługa 8 grup,
   k. Ilość wpisów w listach kontroli dostępu Security ACL – 1000.

Przełącznik sieciowy typ 3 - 6 szt.

1. Typ przełącznika i minimalna liczba portów:
    a. Typ i liczba portów – 8x 10/100/1000 POE+ RJ45, 2x Gigabit copper/SFP combo,
    b. Budżet mocy dla POE – 67W,
    c. Zasilanie przez zewnętrzny zasilacz AC 230V,
    d. Obudowa 1U, desktop,
    e. Urządzenie chłodzone pasywnie, bez wentylatorów.
2. Wsparcie wkładek SFP w portach SFP 1G (dla urządzeń wyposażonych w takie porty), co najmniej:
    a. Gigabit Ethernet 1000Base-SX zasięg do 500 metrów,
    b. Gigabit Ethernet 1000Base-LX/LH zasięg do 10 km,
    c. Gigabit Ethernet 1000Base-EX zasięg do 40 km,
    d. Gigabit Ethernet 1000Base-ZX zasięg do 70 km,
    e. Wkładka z interfejsem miedzianym 1G RJ-45.
3. Zarządzenie energią:
    a. Zasilanie PoE można włączać i wyłączać w oparciu o harmonogram zdefiniowany przez użytkownika w celu oszczędzania energii,
    b. Zapewnia zasilanie PoE podczas restartu urządzenia,
    c. Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az),
    d. Możliwość wyłączenia diod LED w celu oszczędzania energii.
4. Minimalne parametry wydajnościowe:
    a. Przepustowość przełącznika (Switching capacity): 20 Gbps,
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 14 Mpps,
    c. Pamięć DRAM – 1 GB,
    d. Pamięć Flash – 512 MB,
    e. Obsługa 4000 VLAN,
    f. 16000 adresów MAC,
    g. Wire-speed Ipv4 routing – 990 tras statycznych, 128 interfejsów IP,
    h. Obsługa ramek jumbo – do 9000 bajtów,
    i. 2000 IGMP group,
    j. 8 połączeń zagregowanych typu „port channel” per grupa, obsługa 8 grup,
    k. Ilość wpisów w listach kontroli dostępu Security ACL – 1000.

Wymagania wspólne dla przełączników od typ 1 do typ 4

1. Obsługa protokołu SNTP.
2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
3. Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2.
4. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree,
    b. IEEE 802.1s Multi-Instance Spanning Tree - obsługa 8 instancji,
    c. Per-VLAN Rapid Spanning Tree (PVRST+) - obsługa 126 instancji.
5. Obsługa protokołu LLDP i LLDP-MED.
6. Obsługa translacji sieci VLAN 1:1 (mapowanie 1 do 1 z translacją identyfikatora sieci klienckiej VLAN (C-VLAN) na interfejsie brzegowym na identyfikator sieci VLAN używanej w sieci operatora (S-VLAN)).
7. Obsługa Q-in-Q oraz Selective Q-in-Q.
8. Urządzenie musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad (LACP).
9. Urządzenie musi realizować funkcję UDLD w celu wykrywania jednokierunkowych połączeń spowodowanych uszkodzeniami linków.
10. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
11. Urządzenie musi mieć możliwość uruchomienia funkcji serwera DHCP wraz z obsługą wielu puli adresowych i zakresów adresowych.
12. Obsługa opcji DHCP: opcje 12, 59, 60, 66, 67, 82, 125, 129 oraz 150.

13. Realizacja funkcji DHCP Relay wraz z obsługą funkcji DHCP opcja 82.
14. Urządzenie musi mieć możliwość konfiguracji interfejsów Layer 3 dla:
    a. Portów fizycznych przełącznika,
    b. Interfejsów zagregowanych przy pomocy Link Aggregation (LAG),
    c. Interfejsów VLAN,
    d. Interfejsów loopback.
15. Obsługa UDP Relay (User Datagram Protocol Relay).
16. Obsługa funkcjonalności umożliwiającej powiadomienie przez przełącznik, z wykorzystaniem notyfikacji SYSLOG lub SNMP, nadrzędnego systemu monitorowania o wykryciu zaniku zasilania. Funkcjonalność umożliwia wysłanie komunikatu o zaniku zasilania przed całkowitą utratą zasilania przez urządzenie.
17. Mechanizmy związane z bezpieczeństwem sieci:
    a. Trzy poziomy dostępu administracyjnego poprzez konsolę (3 poziomy uprawnień),
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    c. Obsługa różnych trybów uwierzytelniania 802.1x na porcie:
        i. Tryb pojedynczego hosta, w którym tylko jeden host może być podłączony do portu;
        ii. Tryb wielu hostów, w którym port jest uwierzytelniony wówczas, gdy podłączony jest do niego co najmniej jeden uwierzytelniony klient;
        iii. Tryb wielu sesji, w którym status uwierzytelnienia nie jest przypisany do portu a wyłącznie do każdego z klientów podłączonych do portu;
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    g. Realizacja funkcji Change of Authorization (CoA) realizującej dynamiczną zmianę uwierzytelnienia dla sesji użytkownika podłączonego do danego portu,
    h. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    i. Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard,
    j. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    k. Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community,
    l. Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL,
    m. Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC],
    n. Bezpieczny proces bootowania urządzenia,
    o. Suplikant 802.1X - przełącznik musi mieć możliwość takiej konfiguracji, aby działał jako suplikant do innego przełącznika.

18. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    b. Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek,
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
f. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP,
h. Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu.

19. Urządzenie musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN
20. Urządzenie musi obsługiwać funkcję port mirroring polegającej na kopiowaniu ruchu z danego portu i przesłanie go do innego portu. Obsługa do co najmniej 8 portów źródłowych kopiujących swój ruch do jednego portu docelowego (monitorującego).
21. Obsługa funkcji VLAN mirroring polegającej na kopiowaniu ruchu z danej sieci VLAN i przesłanie go do innego portu. Obsługa do co najmniej 8 źródłowych sieci VLAN kopiujących swój ruch do jednego portu docelowego (monitorującego).
22. Urządzenie musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
23. Obsługa protokołu sFlow.
24. Obsługa standardów:
    - IEEE 802.3 10BASE-T Ethernet,
    - IEEE 802.3u 100BASE-TX Fast Ethernet,
    - IEEE 802.3ab 1000BASE-T Gigabit Ethernet,
    - IEEE 802.3ad Link Aggregation Control Protocol,
    - IEEE 802.3z Gigabit Ethernet,
    - IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN,
    - IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable,
    - IEEE 802.3x Flow Control,
    - IEEE 802.1D (STP, GARP, and GVRP),
    - IEEE 802.1Q/p VLAN,
    - IEEE 802.1w Rapid STP,
    - IEEE 802.1s Multiple STP,
    - IEEE 802.1X Port Access Authentication,
    - IEEE 802.3af,
    - IEEE 802.3at,
    - IEEE 802.1AB Link Layer Discovery Protocol,
    - IEEE 802.3az Energy Efficient Ethernet,
    - RFC 768,
    - RFC 783,
    - RFC 791,
    - RFC 792,
    - RFC 793,
    - RFC 813,
    - RFC 826,
    - RFC 879,
    - RFC 896,
    - RFC 854,

- RFC 855,
- RFC 856,
- RFC 858,
- RFC 894,
- RFC 919,
- RFC 920,
- RFC 922,
- RFC 950,
- RFC 951,
- RFC 1042,
- RFC 1071,
- RFC 1123,
- RFC 1141,
- RFC 1155,
- RFC 1157,
- RFC 1213,
- RFC 1215,
- RFC 1286,
- RFC 1350,
- RFC 1442,
- RFC 1451,
- RFC 1493,
- RFC 1533,
- RFC 1541,
- RFC 1542,
- RFC 1573,
- RFC 1624,
- RFC 1643,
- RFC 1700,
- RFC 1757,
- RFC 1867,
- RFC 1907,
- RFC 2011,
- RFC 2012,
- RFC 2013,
- RFC 2030,
- RFC 2131,
- RFC 2132,
- RFC 2233,
- RFC 2576,
- RFC 2616,
- RFC 2618,
- RFC 2665,
- RFC 2666,
- RFC 2674,
- RFC 2737,
- RFC 2819,
- RFC 2863,
- RFC 3164,
- RFC 3176,

- RFC 3411,
- RFC 3412,
- RFC 3413,
- RFC 3414,
- RFC 3415,
- RFC 3416,
- RFC 4330

25. Zarządzanie urządzeniem poprzez co najmniej:
    a. Port konsoli – USB typu C i RJ-45,
    b. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia,
    c. Obsługę protokołów SNMPv3, SSHv2, https, syslog, SCP,
    d. Dedykowaną aplikacja mobilną,
    e. Wbudowany graficzny interfejs zarządzania urządzeniem dostępny z poziomu przeglądarki internetowej,
    f. Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu.
26. Urządzenie musi być objęte **co najmniej 36-miesięcznym** serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.
27. Wraz z urządzeniami należy dostarczyć **oprogramowanie umożliwiające centralne zarządzanie siecią**. Rozwiązanie musi pozwolić na centralne monitorowanie, konfigurację oraz optymalizację urządzeń w sieci. Oprogramowanie musi pozwalać na powiadomienia o aktualizacjach oraz prosty system aktualizacji urządzeń typu przełącznik. Platforma musi mieć możliwość instalacji na systemach: Microsoft Hyper-V, Oracle VirtualBox, VMware ESXi, Fusion, and Workstation, Amazon Web Services (AWS), Microsoft Azure. Zamawiający nie wymaga dostarczenia dedykowanego sprzętu dla uruchomienia centralnego zarządzania. System zostanie uruchomiony w środowisku Zamawiającego.

Dodatkowe moduły i okablowania

Zamawiający wymaga dostarczenia modułów i okablowania, które muszą być kompatybilne z dostarczonymi urządzeniami:

1) 9x twinax 2 metrowe 10G,
2) 2x twinax 1 metrowe 10G
3) 5x wkładka MM 10G wraz z niezbędnym okablowaniem.

Pozostałe wymagania dotyczące dostarczanych urządzeń

1) Dostarczony sprzęt musi być fabrycznie nowy, nieużywany oraz niedostarczany wcześniej innym klientom.
2) Dostarczony sprzęt musi być objęty gwarancją świadczoną bezpośrednio przez Producenta sprzętu. Wykonawca wraz z ofertą ma obowiązek dostarczyć dokument wystawiony przez Producenta, poświadczający, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży oraz zarejestrowanym na użytkownika końcowego (tj. Zamawiającego).
3) Zamawiający zastrzega sobie prawo sprawdzenia, poprzez numery katalogowe czy dostarczony sprzęt spełnia wszystkie wyżej wymienione warunki. W przypadku niespełnienia przez sprzęt któregokolwiek z wyżej wymienionych warunków Zamawiający zastrzega sobie prawo zwrotu całego dostarczonego sprzętu (na koszt dostawcy), jak również obciążenia Wykonawcy, karami umownymi określonymi w umowie, tytułem niedotrzymania jej warunków.
4) W ramach składanej oferty, Wykonawca zobowiązany jest do wyszczególnienia wszystkich numerów katalogowych produktów (licencje, sprzęt i oprogramowanie) w formularzu ofertowym. Lista ta będzie podlegała weryfikacji przez Zamawiającego lub niezależną firmę zewnętrzną,

wskazaną przez Zamawiającego, w celu weryfikacji z wymaganiami i zgodnością z niniejszym opisem przedmiotu zamówienia.

5) Zamawiający wymaga także, aby Wykonawca posiadał status oficjalnego partnera handlowego Producenta oferowanych urządzeń, a możliwość zweryfikowania tego faktu była publicznie dostępna poprzez stronę internetową Producenta.

Specyfikacja prac wdrożeniowych i instalacyjnych w ramach dostawy urządzeń

1) Przed rozpoczęciem prac wdrożeniowych należy ustalić plan adresacji i wykorzystania adresów oraz sieci logicznych VLAN. Ustalenia te będą prowadzone z wyznaczonymi do tego celu pracownikami Zamawiającego.
2) Przed rozpoczęciem prac Wykonawca musi przeprowadzić analizę stanu sieci, serwerów i jego usług oraz ustalić harmonogram prac.
3) Konfiguracja będzie obejmowała nowo dostarczone oprogramowanie i sprzęt oraz już znajdujące się urządzenia w infrastrukturze Zamawiającego. Ze względów bezpieczeństwa, szczegółowy wykaz istniejących urządzeń zostanie udostępniony tylko wyłonionemu Wykonawcy.
4) Wszystkie dostarczane urządzenia muszą zostać wcześniej prekonfigurowane i sprawdzone u Wykonawcy, tak, aby zminimalizować ilość prac realizowanych w siedzibie Zamawiającego.
5) W ramach prac należy również przeprowadzić rekonfigurację urządzeń, posiadanych przez Zamawiającego, do współpracy z urządzeniami dostarczonymi w ramach realizacji zamówienia jak i mechanizmami jakie zostaną uruchomione na dostarczonych urządzeniach. Sieć musi stanowić spójną całość.
6) Prace powinny zostać prowadzone w oknach serwisowych wyznaczonych przez Zamawiającego (dopuszcza się prace w godzinach wieczornych/nocnych lub w weekendy w celu minimalizacji przestoju).
7) Usługa konfiguracji dostarczonych urządzeń zawierać będzie m.in.:
   a) konfigurację reguł ACL na urządzeniach brzegowych (Zamawiający zastrzega, że w tym zakresie ma bardzo złożone wymagania, które dotyczą dużej ilości usług, jaka hostowana jest w ramach infrastruktury),
   b) protokoły VLAN, Trunk, STP, RSTP, MSTP, LACP, adresację IP, konfigurację DNS, routingu,
   c) baner logowania, usługa NTP, SSH, wbudowane mechanizmy RBAC oraz konta użytkowników,
   d) wysyłanie zdarzeń syslog do wskazanego serwera Syslog,
   e) mechanizmy bezpieczeństwa: Port Security, IP DHCP Snooping, IP Source Guard i Dynamic ARP Inspection lub w pełni równoważne,
   f) hardening urządzeń sieciowych według najlepszych praktyk Producenta,
   g) personalizację ustawień do przedstawionych wymagań,
   h) integrację urządzeń z obecnymi w infrastrukturze,
   i) konfigurację innych funkcjonalności dostarczonych urządzeń i oprogramowania, które okażą się potrzebne w trakcie wdrożenia, gdy Wykonawca uzna zasadność ich aktywacji.
   j) integrację urządzeń z systemem centralnego zarządzania i monitorowania,
   k) przygotowanie szablonów konfiguracji dla portów dostępowych.
   l) Cała sieć uruchomiona musi stanowić spójną całość z aktualną siecią LAN i bazować na tych samych mechanizmach ochrony oraz obsługi ruchu
8) Wykonawca, w terminie ustalonym z Zamawiającym, przeprowadzi instruktaż (do 2 godzin lekcyjnych) u Zamawiającego dla 2 osób. Szkolenie powinno dotyczyć zmian zaistniałych w sieci, wykorzystanych technologii, sposobu działania nowego systemu, procedur aktualizacji oprogramowania na dostarczonych urządzeniach.
9) Wykonawca zobowiązany jest do zapewnienia gwarancji na wdrożoną konfigurację przez okres do 1 miesiąca po zamknięciu wdrożenia lub do momentu oddania pełnego dostępu do interfejsu zarządzającego dostarczonych urządzeń i oprogramowania. Wykonawca zobowiązany jest do udokumentowania zmian przeprowadzonych w systemie informatycznym Zamawiającego w dokumentacji powdrożeniowej. Dokumentacja ta powinna obejmować topologię oraz tabele adresacji. Wszelkie materiały i dokumentacje muszą być sporządzone w języku polskim.

10) Do prac wdrożeniowych i konfiguracyjnych musi zostać wyznaczona co najmniej jedna osoba posiadająca certyfikaty techniczne producenta oferowanych urządzeń, która nadzorować będzie integrację dostarczonych urządzeń z urządzeniami Zamawiającego. Certyfikaty te muszą być na co najmniej poziomie profesjonalnym Wszystkie certyfikaty należy dołączyć do składanej oferty. Ich brak będzie skutkował odrzuceniem oferty.