**Odpowiedzi na pytania Wykonawców**

1. **Czy Zamawiający dopuści możliwość zaoferowania rozwiązania konkurencyjnego do opisanego w dokumentacji i uzna za równoważne zestaw dwóch urządzeń pracujących w klastrze HA:**

|  |
| --- |
| **System** |
| **Konstrukcja** |
| System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. |
| Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2. |
| Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) |
| Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. |
| System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. |
| Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażęnie opcjonalne). |
| Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19". |
| Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). |
| Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. |
| Możliwość przeprowadzenia konfiguracji w trybie Zero Touch. |
|  |
| WYMAGANIA |  |
| Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) | 64 |
| Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: | 12 |
| Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: | 2 |
| Liczba fizycznych interfejsów 10GBASE-X nie mniej niż: |  |
| Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: | 128 |
|  |  |
| **Wydajność** |   |
| Wydajność Firewall nie mniej niż (Gbps) | 10 |
| Wydajność Firewall IMIX nie mniej niż (Gbps) | 4 |
| Wydajność IPS nie mniej niż (Gbps) | 2,5 |
| Wydajność FW+IPS+AV nie mniej niż (Gbps) | 0,9 |
| Wydajność NGFW nie mniej niż (Gbps) | 2,5 |
| Liczba równoczesnych połączeń nie mniejsza niż: | 5000000 |
| Liczba nowych połączeń na sekundę nie mniejsza niż: | 69000 |
| Wydajność IPsec VPN nie mniej niż (Gbps): | 4 |
| Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): | 0,8 |
| Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: | 12000 |
| Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: | 1500 |
| Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: | 1100 |
|  |  |
| **Zarządzanie** |
| Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. |
| Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (ExternalTrusted CA). |
| Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time PasswordAlgorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. |
| Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, namelookup, routelookup czy packetcapture w oparciu o Berkley PacketFilter. |
| Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. |
| Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. |
| System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. |
| System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. |
| System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. |
| Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). |
| System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. |
| Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time PasswordAlgorithm). |
| System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). |
| Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. |
| System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). |
| Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. |
| System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpwiednika). |
| System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. |
| System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta |
| Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji. |
| Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. |
|  |  |
|  |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** |
| **Zapora sieciowa** |
| Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm StatefulPacketInspection. |
| System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. |
| Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. |
| Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. |
| Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. |
| System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). |
| System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika. |
|  |
| **Trasowanie ruchu** |
| Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. |
| Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. |
| Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. |
| Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. |
| Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). |
| Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast SparseMode (PIM-SM). |
| Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parentproxy) dla IPv4 i IPv6. |
|  |
| **Translacja adresów i portów** |
| Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. |
| Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT |
|  |
| **Kształtowanie pasma i jakość usług** |
| System powinien zapewniać możliwość elastycznego kształtowania pasma (TrafficShaping) dla sieci, użytkowników i aplikacji. |
| Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. |
| System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. |
| Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. |
| Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet. |
|  |
| **Podstawowa ochrona przed atakami DoS i DDoS** |
| System powinien zapewniać ochronę przed atakami DoS czy DDoS (floodprotection). |
|  |
| **Pozostałe** |
| Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. |
| Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiplebridge) oraz mostów zbudowanych z wielu portów (multiportbridge). |
| System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. |
| System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. |
| Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). |
| System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. |
| Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapiddeployment (6rd). |
| Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). |
| Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. |
|  |
|  |
| **Uwierzytelnianie i obsługa użytkowników** |
| Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. |
| Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. |
| System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. |
| Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. |
| System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time PasswordAlgorithm). |
| Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. |
| System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. |
| Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. |
| Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. |
| Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. |
| Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. |
| Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. |
|  |
| **Koncentrator VPN** |
| System musi umożliwiać konfigurację połączeń typu IPsecsite-to-site VPN dla IKE v1 oraz IKE v2. |
| System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). |
| System musi obsługiwac połączenia IPsecsite-to-site VPN jak i IPsecclient-to-site VPN oraz SSL client-to-site VPN. |
| Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsecsite-to-site VPN. |
| Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. |
| Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsecsite-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. |
| Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. |
| Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeńIPsecclient-to-site VPN jak i SSL client-to-site VPN. |
| Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsecclient-to-site VPN jak i SSL client-to-site VPN. |
| Urządzenie musi obsługiwać połączenia L2TP overIPsec. |
|  |
| **Logowanie i raportowanie** |
| System musi możliwiać monitorowanie logów ruchu w czasie rzeczywistym. |
| System powinien umożliwiać składowanie oraz archiwizację logów. |
| Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. |
| Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. |
| Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa |
| System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. |
| System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. |
| Rozwiązanie powinno umożliwiać wysyłanie raportów via email. |
| Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. |
| Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. |
| System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. |
| System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. |
| Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. |
| System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. |
|  |
| **Intrusion Prevention System i Advanced Threat Protection** |
| Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. |
| Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. |
| Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. |
| System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command& Control / Botnet. |
|  |
| **Ochrona i kontrola web** |
| **Ochrona przez Malware** |
| Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. |
| Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. |
| System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. |
| Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. |
| Rozwiązanie musi przeprowadzać emulację skryptów Java. |
| Rozwiązanie powinno przeprowadzać tzw. live-lookupst.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. |
| System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap PatternUpdates) |
|  |
| **Inspecja ruchu SSL/TLS** |
| Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. |
| Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. |
| Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. |
| Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. |
| Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. |
|  |
| **Filtr Web** |
| Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron. |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. |
| Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. |
| System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji. |
|  |  |
|  |
| **Ochrona i kontrola aplikacji** |
| Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. |
| Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. |
| Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. |
| Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. |
| Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. |
| Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN. |
|  |
| **Ochrona przed nieznanymi zagrożeniami** |
| Rozwiązanie klasy Sandbox do ochrony przez zadrożeniami typu Zero-Day. |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. |
| Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. |
| Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików. |
| System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. |
| System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. |
| System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. |

**2.**

**W zakresie oprogramowania opisanego jako Windows Server 2022 PL Standard – zainstalowanego w roli kontrolera domeny Microsoft Active Directory na min. 50-100 użytkowników – prosimy o wskazanie na jaką ilość użytkowników (tzw. licencje dostępowe CAL), Wykonawca ma skalkulować ofertę ? Czy Zamawiający wymaga dostarczenia licencji dla 50 użytkowników czy też dla 50 urządzeń ?**

**3.W zakresie serwerów – Zamawiający wskazuje serwer wyposażony w dwa porty VGA, informujemy, że w związku z aktualnym kryzysem na rynku komponentów są problemy z dostępnością niektórych konfiguracji sprzętu – w związku z tym:**

**a) czy Zamawiający dopuści serwer wyposażony w 1 port VGA z możliwością rozbudowy o dodatkowy port cyfrowy dla podłączenia monitora. Obecnie zdecydowana większość pracy administratora serwera odbywa się poprzez połączenia zdalne więc lokalnie jeden port z tyłu serweradla podłączenia monitora zewnętrznego jest całkowicie wystarczającym rozwiązaniem**

**b) czy Zamawiający dopuści serwer nie wyposażony w sprzętowy kontroler RAID z pamięcią 2GB z uwagi na fakt, że wskazany w postępowaniu system wirtualizacji posiada wbudowane mechanizmy umożliwiające budowę woluminów RAID o poziomach wskazanych w specyfikacji technicznej załącznik nr 1 w związku z tym wspomniany kontroler jest zbędny.**

**c) czy Zamawiający dopuści serwer wyposażony w diody LED umożliwiające wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz przekroczonej temperaturze pracy zamiast wyświetlacza LCD**

ad. 1

***Odpowiedź: Zamawiający wyjaśnia, iż uznaje powyższe rozwiązanie za równoważne funkcjonalnie.***

ad. 2

***Odpowiedź: Zamawiający wyjaśnia, iż szacowana liczba klientów systemu AD jest wielkością zmienną będzie oscylowała w zakresie 50-100 szt. co stanowi podstawę do oszacowania wydajności kontrolera. Zamawiający wyjaśnia, że wymagana w tym przypadku liczby licencji do 100 szt. CAL na urządzenie.***

ad. 3

a) ***Odpowiedź: Zamawiający wyjaśnia, iż dopuści rozwiązanie, w którym serwer będzie wyposażony w 1 port VGA z możliwością rozbudowy, pod warunkiem dostępności konsoli VGA
z poziomu oprogramowania poprzez IP.***

b) ***Odpowiedź: Zamawiający dopuszcza rozwiązanie równoważne, w którym zostanie dostarczony i zainstalowany kontroler RAID wbudowany w mechanizm systemu wirtualizacji. Zamawiający wymaga aby zachować wydajność klastra na wymaganym poziomie.***

c) ***Odpowiedź: Zamawiający wyjaśnia, że dopuści serwer z sygnalizacją za pomocą diod LED pod warunkiem dostępności rozszerzonej informacji o statusie urządzenia za pomocą konsoli zdalnej IP.***