MCN.5.261.2.2023 Kraków, dnia 10.02.2023r.

WYJAŚNIENIA TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego, którego przedmiotem jest: **dostawa, wdrożenie i uruchomienie infrastruktury IT dla nowo budowanego budynku Małopolskiego Centrum Nauki Cogiteon.**

Zamawiający – Małopolskie Centrum Nauki Cogiteon, ul. Lubelska 23, 30 – 003 Kraków informuje, iż wpłynęły od Wykonawców wnioski, dotyczące treści specyfikacji warunków zamówienia. Na podstawie art. 135 ust. 1 oraz 2 ustawy z dnia 11.09.2019 r. – Prawo zamówień publicznych (tj. Dz. U. 2022 r. poz. 1710 z pózn.zm.) zwanej dalej „ustawą Pzp", Zamawiający przekazuje treść wniosków wraz z udzielonymi odpowiedziami.

Pytanie nr 1:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy Zamawiający pod pojęciem „Możliwość zainstalowania dedykowanego napędu optycznego" dopuści rozwiązanie umożliwiające podłączenie zewnętrznego napędu optycznego?

Odpowiedź nr 1:

Zamawiający dopuszcza możliwość zaoferowania serwera z możliwością podłączenia zewnętrznego napędu optycznego dedykowanego przez producenta do oferowanego serwera.

Pytanie nr 2:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy Zamawiający zamiast rozwiązania ze wsparciem dla technologii: Memory Scrubbing lub równoważnej, SDDC lub równoważnej, ECC lub równoważnej, Memory Mirroring lub równoważnej, ADDDC lub równoważnej, dopuści rozwiązanie ze wsparciem dla następujących zabezpieczeń pamięci: Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing lub równoważnych?

Odpowiedź nr 2:

Zamawiający uzna za równoważne rozwiązania wskazane przez Wykonawcę.

Pytanie nr 3:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy Zamawiający zamiast rozwiązania wyposażonego w procesor osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 148pkt (wynik osiągnięty dla zainstalowanego jednego procesora) dopuści rozwiązanie wyposażone w procesor, którego wynik w teście SPEC

CPU2017 Floating Point będzie osiągnięty dla dwóch zainstalowanych procesorów i będzie wynosił minimum 286?

Odpowiedź nr 3:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 4:

Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy Zamawiający zamiast rozwiązania posiadającego: 2 porty USB 3.0 wewnętrzne, 2 porty USB 3.0 dostępne z tyłu serwera, 1 port USB 3.0 na panelu przednim dopuści rozwiązanie posiadające: jeden port USB 3.0 wewnątrz serwera, dwa porty USB z tyłu serwera w tym jedno USB 3.0 oraz port USB 2.0 z przodu serwera?

Odpowiedź nr 4:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 5:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Biorąc pod uwagę założenia Zamawiającego – zakup 3 serwerów do wirtualizacji, wnioskujemy o modyfikację zapisów co pozwoli na zmniejszenie kosztów zakupu serwerów bez utraty wymaganej przez Zamawiającego funkcjonalności. Serwery wymagają tylko dysków do uruchomienia wirtualizatora, wymagane są tylko 2 karty rozszerzeń oraz możliwość rozbudowy pamięci do 1024GB. Biorąc pod uwagę wskazane parametry jako kluczowe, wnioskujemy o modyfikację zapisów w sposób następujący:

1. Obudowa:
   • Typu RACK, wysokość nie więcej niż 1U;
   • Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
   • ~~Możliwość zainstalowania 16 dysków twardych hot plug 2,5";~~
   • Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
   • Zainstalowane 2 szt. dyski SSD M.2 SATA lub M.2 NVMe SSD 240GB podpięte do sprzętowego kontrolera RAID-1;
   • Możliwość zainstalowania dedykowanego napędu optycznego;
2. Płyta główna:
   • Dwuprocesorowa;
   • Wyprodukowana i zaprojektowana przez producenta serwera
   • Możliwość zainstalowania modułu TPM 2.0;
   • Min 3 złącza PCI Express generacji 4:~~w tym:~~
   ~~o 4 fizyczne złącza o prędkości x16;~~
   ~~o 3 fizyczne złącza o prędkości x8;~~
   ~~o Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;~~
   ~~o Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; Lub~~
   ~~o 6 fizycznych złącz o prędkości x8~~
   ~~o 2 fizyczne złącza o prędkości x16~~
   • 32 gniazd pamięci RAM;
   ~~• Obsługa minimum 4TB pamięci RAM DDR4;~~
   ~~• Obsługa minimum 8TB pamięci RAM DDR4 + pamięć nieulotna;~~

• Wsparcie dla technologii: Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing lub równoważnych;
~~o Memory Scrubbing lub równoważne~~
~~o SDDC lub równoważne~~
~~o ECC lub równoważne~~
~~o Memory Mirroring lub równoważne~~
~~o ADDDC lub równoważne;~~
• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
• Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

3. Procesory:
• Zainstalowany minimum jeden procesor maksymalnie 16-sto rdzeniowy
• Taktowanie 2,9GHz
• architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 286 pkt (wynik osiągnięty dla zainstalowanych dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html

Odpowiedź nr 5:

Zamawiający podtrzymuje zapisy OPZ. Zaproponowane zmiany powodują znaczną utratę funkcjonalności serwera i uniemożliwiają jego rozbudowę w przyszłości.

Pytanie nr 6:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy Zamawiający dopuści rozwiązanie obsługujące min. 2TB pamięci RDIMM lub 8TB pamięci LRDIMM?

Odpowiedź nr 6:

Zamawiający specyfikuje wymaganie Obsługa minimum 4TB pamięci RAM DDR4 oraz 8TB pamięci RAM DDR4+ pamięć nieulotna. Taki zapis nie definiuje czy ma to być osiągnięte przy pomocy pamięci RDIMM czy LRDIMM.

Pytanie nr 7:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.1.1 Serwer do wirtualizacji Czy zamawiający dopuszcza rozwiązanie dwuprocesorowe 8 rdzeniowe spełniające pozostałe wymagania, zamiast opisanego 1 procesorowego 16 rdzeniowego?

Odpowiedź nr 7:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 8:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy Zamawiający pod pojęciem „Możliwość zainstalowania dedykowanego napędu optycznego" dopuści rozwiązanie umożliwiające podłączenie zewnętrznego napędu optycznego?

Odpowiedź nr 8:

Zamawiający informuje, iż odpowiedź w przedmiotowym zakresie znajduje się w odpowiedzi na pytanie nr 4 z dnia 02.02.2023 r.

Pytanie nr 9:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy Zamawiający zamiast rozwiązania ze wsparciem dla technologii: Memory Scrubbing lub równoważnej, SDDC lub równoważnej, ECC lub równoważnej, Memory Mirroring lub równoważnej, ADDDC lub równoważnej, dopuści rozwiązanie ze wsparciem dla następujących zabezpieczeń pamięci: Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing lub rówoważnych?

Odpowiedź nr 9:

Zamawiający uzna za równoważne rozwiązania wskazane przez Wykonawcę.

Pytanie nr 10:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy Zamawiający zamiast rozwiązania wyposażonego w procesor osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 81 pkt (wynik osiągnięty dla zainstalowanego jednego procesora) dopuści rozwiązanie wyposażone w procesor, którego wynik w teście SPEC CPU2017 Floating Point będzie osiągnięty dla dwóch zainstalowanych procesorów i będzie wynosił minimum 149?

Odpowiedź nr 10:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 11:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy Zamawiający zamiast rozwiązania posiadającego: 2 porty USB 3.0 wewnętrzne, 2 porty USB 3.0 dostępne z tyłu serwera, 1 port USB 3.0 na panelu przednim dopuści rozwiązanie posiadające jeden port USB 3.0 wewnątrz serwera, dwa porty USB z tyłu serwera w tym jedno USB 3.0 oraz port USB 2.0 z przodu serwera?

Odpowiedź nr 11:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 12:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy zamawiający dopuści rozwiązanie oparte na RAID 5 zawierające 5 Dysków 8TB zamiast 6 dysków 6 TB?

Odpowiedź nr 12:

Zamawiający zmienia zapisy OPZ w ten sposób, że dopuszcza rozwiązanie polegające na wyposażeniu systemu kopii zapasowych w nie mniej niż 5 dysków i nie więcej niż 6 dysków SATA 7.2K RPM o takiej samej pojemności, o łącznej pojemności nie mniejszej niż 36 TB, dyski Hotplug.

Zamawiający aktualizuje treść zał. nr 1a do formularza ofertowego publikując plik pn. „Załącznik nr 1a do Formularza ofertowego - Parametry oferowanego sprzętu i oprogramowania_10_02_2023.docx”.

Pytanie nr 13:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.3 System kopii zapasowych Czy Zamawiający dopuści rozwiązanie obsługujące min. 1TB pamięci RDIMM (bez obsługi pamięci nieulotnej)?

Odpowiedź nr 13:

Zamawiający specyfikuje wymaganie Obsługa minimum 4TB pamięci RAM DDR4 oraz 8TB pamięci RAM DDR4 + pamięć nieulotna. Taki zapis nie definiuje czy ma to być osiągnięte przy pomocy pamięci RDIMM czy LRDIMM.

Pytanie nr 14:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa W punkcie 8 „Minimalne wymagane parametry” w części: „Kontrolery”, Zamawiający wymaga dostarczenia macierzy obsługującej deduplikację i kompresję. Obecnie producenci używają holistycznie redukcji i kompresji danych, w związku z czym wyłączenie jednej z tych funkcjonalności jest niekorzystne z punktu widzenia wydajności. Biorąc to pod uwagę, czy Zamawiający zrezygnuje z możliwości włączenie samej deduplikacji lub kompresji i wyrazi zgodę na modyfikację ww. punktu w sposób następujący:

„8. Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:

~~a. Sama deduplikacja wybranego LUN;~~

~~b. Sama kompresja wybranego LUN;~~

c. Kombinacja technologii kompresji i deduplikacji dla wybranego LUN;

d. Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;”?

Odpowiedź nr 14:

Zamawiający podtrzymuje zapisu OPZ.

Pytanie nr 15:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 4 „Minimalne wymagane parametry”, część „Interfejsy”. Wielu producentów dla uruchomienia funkcjonalności plikowej wymaga osobnej przestrzeni dla danych. Aby uniknąć problemów z podziałem przestrzeni w przyszłości wnioskujemy, aby już na etapie dostawy oferowane rozwiązanie miało obie licencje aktywne. W związku z powyższym wnosimy o modyfikację ww. punktu w sposób następujący: 4. Dla komunikacji plikowej NAS z serwerami oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać co najmniej następujące protokoły i porty: CIFS, NFS oraz interfejsy Ethernet 1Gbit/s i 10Gbit/s. Oferowany model macierzy musi umożliwiać jednoczesne użytkowanie portów do komunikacji blokowej i plikowej. W obecnym

postępowaniu wymagana jest macierz z aktywnym dostępem blokowym oraz ~~możliwością rozbudowy o~~ dostępem realizowanym na poziomie plikowym.

Odpowiedź nr 15:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 16:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 1 „Minimalne wymagane parametry", część: Poziomy RAID. W wymaganych poziomach RAID znajduje się RAID 0, który nie wprowadza dodatkowego zabezpieczenia danych oraz RAID 50, który nie wnosi większej korzyści niż RAID 5. Czy w związku z tym Zamawiający dopuści rozwiązanie wspierające poziomy RAID 1, 5, 6 i 10, jednocześnie rezygnując z RAID 0 i 50? W związku z powyższym wnosimy o modyfikację ww. punktu w sposób następujący: „1. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: ~~0~~, 1, 10, 5, ~~50~~, 6."

Odpowiedź nr 16:

Zamawiający zmienia zapisy OPZ w ten sposób, że dopuszcza macierz o następujących parametrach: "1. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany co najmniej poziomami RAID: 1,10,5,6".

Pytanie nr 17:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 1 tiret pierwsze „Minimalne wymagane parametry", część: Wspierane dyski. Czy Zamawiający dopuści rozwiązanie wspierające dyski SSD SAS o pojemności minimum 15TB zamiast o pojemności minimum 30TB?

Punkt 1 tiret drugie „Minimalne wymagane parametry", część: Wspierane dyski. W punkcie 8, Zamawiający wymaga, aby macierz umożliwiała szyfrowanie danych na zainstalowanych dyskach dowolnego typu. Zakładając, że szyfrowanie jest realizowane z poziomu kontrolerów macierzy i umożliwia szyfrowanie na dowolnych dyskach, czy Zamawiający zrezygnuje z wspierania dysków SSD SAS SED lub FED?

W związku z powyższym wnosimy o modyfikację ww. punktu w sposób następujący:

„1. Oferowana macierz wspiera co najmniej następujące typy dysków hot-plug:

- dyski elektroniczne SSD SAS o pojemności minimum ~~30 TB 15TB"~~

~~- dyski elektroniczne SSD SAS SED lub FDE o pojemności minimum 4TB (…)"~~

Odpowiedź nr 17:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 18:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa

W punkcie 5 „Minimalne wymagane parametry", części: Wspierane dyski, Zamawiający wymaga dostarczenia macierzy zawierającej 17 dysków SSD SAS 1.92TB.

Czy Zamawiający zamierza korzystać z dysków talerzowych? Jeśli nie, to prosimy o wykreślenie zapisów dotyczących dysków talerzowych oraz funkcjonalności wskazujących na zastosowanie różnych typów dysków. Pozwoli to na zaproponowanie macierzy All Flash, która lepiej wpasuję się w założenie wykorzystania dysków SSD.

W związku z powyższym wnosimy o modyfikację tabeli w części „Minimalne wymagane parametry" Załącznika nr 7 pkt 6.2.2 Macierz dyskowa w sposób następujący:

1. Obudowa:

7. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów dyskowych dla dalszej rozbudowy w co najmniej trzech wariantach:

a. maksimum 2U przy gęstości upakowania minimum 24 dysków 2,5" typu hotplug ~~(jednoczesna obsługa dowolnej kombinacji dysków SAS, SSD w pojedynczej półce);~~

~~b. maksimum 2U przy gęstości upakowania minimum 12 dysków 3,5" typu hotplug lub 4U przy gęstości upakowania minimum 24 dyski 3,5" typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków NL-SAS, SSD);~~

~~c. maksimum 4U przy gęstości upakowania minimum 60 dysków 3,5" typu hotplug; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji półek dyskowych typu a, b, c; (np. jednoczesne użycie półek gęstego upakowania typu c. i półek 2U dla dysków 2,5" typu a. w jednej macierzy).~~

3. Kontrolery:

8. (…) Jeżeli do uruchomienia wymaganych funkcjonalności deduplikacji i kompresji są wymagane jakiekolwiek licencje lub elementy hardware wymaga się ich dostarczenia dla maksymalnej obsługiwanej przez macierz pojemności. Deduplikacja i kompresja realizowane w trybie in-line lub online dla danych blokowych udostępnianych za pośrednictwem FC/iSCSI/SAS. Dane muszą być od razu zapisane na dyski w postaci zdeduplikowanej/skompresowanej. Deduplikacja i kompresja musi być wspierana przez macierz na dowolnym typie obsługiwanych dysków – co najmniej ~~NL-SAS, SAS~~, SSD.

6. Wspierane dyski:

1. Oferowana macierz wspiera co najmniej następujące typy dysków hot-plug:

(…)

~~- dyski mechaniczne HDD SAS o pojemności minimum 900GB i prędkości 15 tysięcy obrotów na minutę~~

~~- dyski mechaniczne HDD SAS o pojemności minimum 2,4TB, 10k RPM~~

~~- dyski mechaniczne HDD NL-SAS o pojemności minimum 18TB 7.2k RPM~~

2. Macierz obsługuje dyski hot-plug SSD i ~~HDD~~ wyposażone w porty SAS 12Gb/s. (…)

4. Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5" i ~~3,5~~"

7. Opcje software-owe

~~12. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy trzech różnych technologiach dyskowych równocześnie: SSD, SAS, NLSAS. Macierz musi pozwalać na definiowanie minimum 120~~

~~różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB.~~

~~Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O.~~

~~Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność.~~

Odpowiedź nr 18:

Zamawiający zamierza w przyszłości korzystać z dysków talerzowych w związku z tym podtrzymuje zapisy OPZ.

Pytanie nr 19:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa W punkcie 5 „Minimalne wymagane parametry", części: Wspierane dyski, Zamawiający wymaga dostarczenia macierzy zawierającej 17 dysków SSD SAS 1.92TB. Czy Zamawiający dopuszcza dostarczenie macierzy: 15 dysków 2.5" SSD SAS 12Gb/s o pojemności min. 1,92 TB każdy?

Odpowiedź nr 19:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 20:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 1 „Minimalne wymagane parametry", część: Opcje software-owe. Czy Zamawiający dopuści rozwiązanie umożliwiające wykonanie minimum 1500 kopii migawkowych zamiast minimum 4000 kopii migawkowych i wyrazi zgodę na modyfikację ww. punktu w sposób następujący: „1. Macierz wyposażona jest w system kopii migawkowych umożliwiających wykonanie minimum 4000 1500 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy."?

Odpowiedź nr 20:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 21:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 2 „Minimalne wymagane parametry", część: Opcje software-owe. Czy Zamawiający dopuści rozwiązanie umożliwiające zdefiniowanie minimum 1500 woluminów zamiast 4096 i wyrazi zgodę na modyfikację ww. punktu w sposób następujący: „2. Macierz musi umożliwiać zdefiniowanie minimum ~~4096~~ 1500 woluminów tzw. LUN."?

Odpowiedź nr 21:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 22:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.2 Macierz dyskowa Punkt 5 „Minimalne wymagane parametry”, część: Opcje software-owe. Czy Zamawiający dopuści rozwiązanie, które nie posiada wsparcia dla Oracle VM i wyrazi zgodę na modyfikację ww. punktu w sposób następujący: „5. Model macierzy musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server /2016/2019/2022, SuSE Linux, Oracle Linux, ~~Oracle VM~~, RedHat Linux, VMWare, Citrix XEN Server.”?

Odpowiedź nr 22:

Zamawiający zmienia zapisy OPZ w ten sposób, że dopuszcza model macierzy posiadający wsparcie co najmniej dla systemów operacyjjnych: MS Windows Server /2016/2019/2022, SuSE Linux, Oracle Linux, RedHat Linux, VMWare, Citrix XEN Server.

Pytanie nr 23:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność” wskazał, iż przyzna 7 pkt. jeżeli Serwery do wirtualizacji i system kopii zapasowych będą posiadały możliwość zainstalowania dedykowanego wewnętrznego napędu LTO. Czy Zamawiający przyzna punkty w przypadku, gdy zaoferowane rozwiązanie umożliwia podłączenie zewnętrznego napędu LTO, co w odniesieniu do dobrych praktyk backup-u zapewnia ciągłość pracy, nienaruszalność i stały dostęp do kopii, nawet w przypadku awarii serwera, co nie jest możliwe w przypadku zainstalowania napędu LTO wewnątrz serwera?

Odpowiedź nr 23:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 24:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność” wskazał, iż przyzna 3 pkt. jeżeli Serwery do wirtualizacji i system kopii zapasowych będą posiadały Kartę LAN, nie zajmującą żadnego z dostępnych slotów PCI Express, wyposażoną minimum w interfejsy: 2x 10Gbit SFP+, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCI. Czy Zamawiający przyzna punkty, w przypadku zaoferowania rozwiązania posiadającego możliwość instalacji karty 100GbE QSFP28 w slocie PCIe?

Odpowiedź nr 24:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 25:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność” wskazał, iż przyzna 5 pkt. jeżeli Macierz dyskowa będzie posiadała możliwość instalacji minimum 8 portów SAS 12Gbit/s. Zamawiający w powyższym kryterium nie dookreślił do czego mają być przeznaczone ww. porty. W związku z powyższym wnosimy o potwierdzenie czy Zamawiający przyzna punkty, jeżeli zaoferowana macierz dyskowa będzie posiadała możliwość instalacji dodatkowych 8 portów do półek dyskowych. UNITY2x4 PORT SAS EXP FLD RCK.

Odpowiedź nr 25:

Zamawiający podtrzymuje zapisy OPZ. Zamawiający porty SAS będzie wykorzystywał do dalszych rozbudów infrastruktury.

Pytanie nr 26:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 2.4) Czy Zamawiający dopuści rozwiązanie, w którym redundancja połączeń realizowana będzie za pomocą protokołu LACP lub statycznej agregacji połączeń (bez LACP)?

Odpowiedź nr 26:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 27:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 3.1) Czy Zamawiający dopuści rozwiązanie, w którym każde z urządzeń będzie dysponować następującą liczbą portów?

- 12 portów 1G/2.5G/5G/10G RJ-45
- 11 gniazd 1G/10G SFP/SFP+
- 4 gniazda 1G/10G/25G SFP/SFP+/SFP28
- 2 porty 1G RJ-45 HA

Odpowiedź nr 27:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 28:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 3.2) Czy Zamawiający dopuści rozwiązanie, które będzie posiadało port micro USB dla zapewnienia funkcji ZTP (możliwość automatycznej konfiguracji urządzenia i przygotowania do działania) ale bez możliwości podłączenia modemu 3G/4G oraz instalacji oprogramowania z klucza USB?

Odpowiedź nr 28:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 29:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 3.3) Czy Zamawiający wymaga, aby Wykonawca zapewnił odpowiednie wkładki dla zestawienia klastra niezawodnościowego active/passive lub active/active? Połączenie active/active wymaga 3 połączeń pomiędzy urządzeniami natomiast active/passive 2 połączeń.

Odpowiedź nr 29:

Zamawiający wymaga, aby Wykonawca zapewnił odpowiednie wkładki dla zestawienia klastra niezawodnościowego active/active.

Pytanie nr 30:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktów 4.1) Czy Zamawiający dopuści rozwiązanie, którego maksymalna wartość jednoczesnych połączeń to 1,4 mln., a ilość nowych połączeń na sekundę to 145 tys.?

Odpowiedź nr 30:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 31:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 4.2) Zgodnie z najnowszymi dobrymi praktykami metodyki Zero Trust Architecture, każdy ruch powinien być poddawany inspekcji (z każdego miejsca może pochodzić atak). Czy Zamawiający dopuści zatem rozwiązanie, dla którego producent nie deklaruje przepustowości w statefull firewall i pakietach 512B?

Odpowiedź nr 31:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 32:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 4.4) Zgodnie z najnowszymi dobrymi praktykami metodyki Zero Trust Architecture, każdy ruch powinien być poddawany inspekcji (z każdego miejsca może pochodzić atak). Czy Zamawiający dopuści, wobec tego rozwiązanie, którego przepustowość IPSEC VPN wynosi 6,8Gbps i jest większa niż maksymalna wymagana przepustowość urządzenia z włączoną ochroną z punktu 4.6.

Odpowiedź nr 32:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 33:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 4.5) Zgodnie z najnowszymi dobrymi praktykami metodyki Zero Trust Architecture, każdy ruch powinien być poddawany inspekcji (z każdego miejsca może pochodzić atak). Czy Zamawiający dopuści zatem rozwiązanie producenta nie deklarującego wydajności samego mechanizmu IPS i posługującego się wydajnością wspólną mechanizmów identyfikacji aplikacji, IPS, antywirus, URL Filtering, antyspyware które zdefiniowane są w punkcie 4.6?

Odpowiedź nr 33:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 34:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 4.6) Czy Zamawiający dopuści rozwiązanie, którego producent podaje wydajność Threat prevention z włączonymi funkcjami IPS, Application Control Antywirus dla specyfikacji ruchu appmix (różnorodne wykryte aplikacje) w wysokości 5,6Gbps? Jest ona zbliżona do wymaganej w specyfikacji, a jednocześnie test appmix zapewnia wydajność na zbliżonej do rzeczywistości próbce ruchu.

Odpowiedź nr 34:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 35:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 4.7) W funkcji dekrypcji ruchu SSL dla inspekcji parametr wydajności jest znacznie mniej istotny (i przewidywalny w środowisku rzeczywistym) niż parametr ilości transakcji SSL wspieranych przez system jednocześnie. Czy Zamawiający dopuści rozwiązanie, które umożliwia obsługę jednoczesną 140 tys. sesji deskrypcji SSL oraz pozwala za cache 10 tys. certyfikatów?

Odpowiedź nr 35:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 36:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 5.5) Czy Zamawiający wymaga, aby zaoferowane rozwiązanie w ramach funkcjonalności umożliwiało wykrywanie wycieku danych logowania użytkowników (Credential Thief Attack) i przeciwdziałało takim atakom?

Odpowiedź nr 36:

Zamawiający nie specyfikował takiej funkcjonalności.

Pytanie nr 37:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 5.7) Czy Zamawiający dopuści rozwiązanie, które zapewnia w ramach pojedynczej platformy sprzętowej wszystkie wymienione w punkcie 5 funkcjonalności poza funkcją „Kontrola zawartości poczty” w rozumieniu Antyspam? Proponowane rozwiązanie będzie zapewniało „kontrolę zawartości poczty” pod względem analizy i wykrywania niepożądanych plików oraz zachowań, ale nie w rozumieniu ochrony przed niechcianą pocztą (antyspam) i będzie to realizowało za pomocą pozostałych modułów opisanych w punkcie 5.

Odpowiedź nr 37:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 38:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 5.10) Czy Zamawiający dopuści rozwiązanie, które wspiera dwuskładnikowe i wieloskładnikowe uwierzytelnianie, ale nie oferuje tokenów sprzętowych i programowych?

Odpowiedź nr 38:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 39:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 5.13) Czy Zamawiający dopuści rozwiązanie, które umożliwia inspekcję ruchu DNS (również DoT oraz DoH) ale bez możliwości tworzenia lokalnego serwera (Rozwiązanie będzie natomiast umożliwiało realizowanie funkcji DNS proxy) w tej technologii?

Odpowiedź nr 39:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 40:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 6.18) Czy Zamawiający dopuści rozwiązanie integrujące się z rozwiązaniami AWS, GCP oraz Vmware (ESX oraz vCenter), ale bez domyślnego wsparcia dla Microsoft Azure oraz OpenStack?

Odpowiedź nr 40:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 41:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 7.1.4) Czy Zamawiający dopuści rozwiązanie, które będzie umożliwiało tworzenie topologii Hub and Spoke bez dynamicznego zestawienia tuneli pomiędzy spoke i hub? Funkcjonalność taka z reguły działa i tak tylko pomiędzy rozwiązaniami jednego tego samego producenta a przedmiotem przetargu są tylko dwa urządzenia firewall.

Odpowiedź nr 41:

Zamawiający podtrzymuje zapisy OPZ. Zamawiający wymaga, aby urządzenia w zakresie systemu firewall były tego samego producenta.

Pytanie nr 42:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 11.5) Czy Zamawiający dopuści rozwiązanie nie posiadające funkcji blokowania aktywnej zawartości plików PDF oraz MS bez konieczności blokowania transferu całego pliku?

Odpowiedź nr 42:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 43:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 11.6) – Czy Zamawiający wymaga, aby oferowane rozwiązania umożliwiało lokalne wykrywanie zagrożeń typu malware (lokalna analiza ML) w sytuacji braku posiadania aktywnej sygnatury dla pliku?

Odpowiedź nr 43:

Zamawiający podtrzymuje zapisy OPZ.

Pytanie nr 44:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 17.1) Czy Zamawiający dopuści rozwiązanie posiadające moduł logowania bezpośrednio na platformie sprzętowej firewall?

Odpowiedź nr 44:

Zgodnie z punktem 17.1 Zamawiający wymaga: Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

Pytanie nr 45:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 17.1) Czy Zamawiający wymaga, aby w ramach oferty Wykonawca uwzględnił przechowywanie logów w chmurze?

Odpowiedź nr 45:

Zgodnie z punktem 17.1 Zamawiający wymaga: Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze **lub** w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

Pytanie nr 46:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 17.1) Wykonawca zwraca się z prośbą o jednoznaczne wskazanie jaka polityka retencji danych logowania powinna obowiązywać dla wspomnianej usługi w chmurze?

Odpowiedź nr 46:

Zamawiający wymaga retencji danych logowania minimum 90 dni.

Pytanie nr 47:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.17 System firewall – cluster (w zakresie punktu 20.1) Czy Zamawiający wymaga, aby oferowane wsparcie techniczne było realizowane w języku polskim (dla pierwszej linii wsparcia)?

Odpowiedź nr 47:

Tak. Zamawiający wymaga by zaoferowane wsparcie techniczne dla systemu firewall było świadczone w języku polskim (dla pierwszej linii wparcia).

Pytanie nr 48:

Dotyczy Załącznika nr 7 do SWZ pkt od 6.2.4 do 6.2.16 Całość rozwiązania opisanego w punktach od 6.2.4 do 6.2.16 spełnia włącznie rozwiązanie jednego producenta– firmy Extreme Networks. W związku z powyższym czy Zamawiający jako równoważne dopuści rozwiązanie spełniające analogiczne funkcje opisane poniżej:

Przełącznik Typ 1 i Typ 2

1. Typ i liczba portów:

   Minimum 48 portów 10GbE/25GbE SFP28 umieszczonych z przodu obudowy Minimum 8 portów 40GbE/100GbE QSFP28 umieszczonych z przodu obudowy. Porty QSFP28 muszą zapewniać możliwość użycia kabli rozszywających (split cable) do 4 portów 10GbE SFP+ i 4 portów 25GbE SFP28. Minimum 2 porty 1GbE SFP (niezależne od portów SFP28 i QSFP28)
2. Wbudowany, dodatkowy, niezależny, dedykowany port Ethernet SFP do zarządzania poza pasmem - out of band management
3. Wbudowany, dodatkowy, niezależny, dedykowany port Ethernet RJ-45 do zarządzania poza pasmem - out of band management
4. Port konsoli RS232 ze złączem DB9 lub RJ45
5. Port konsoli Mini lub Micro USB
6. Port USB 2.0 (niezależny od portu konsoli)
7. Wydajność: minimum 4Tb/s (prędkość przełączania „wirespeed” dla każdego portu przełącznika)
8. Przepustowość: minimum 2000 Mp/s
9. Przełączanie w warstwie 2 i 3 modelu OSI
10. Opóźnienie przełączania transmisji 10GbE dla pakietów 64 bajtowych poniżej 1µs
11. Mechanizmy przełączania: co najmniej cut through
12. Wielkość bufora pakietów (packet buffer): minimum 32MB
13. Pamięć RAM: co najmniej 8GB
14. Pamięć nieulotna typu flash(zabudowana, nie dopuszcza się pamięci zewnętrznej typu pendrive, itp.): co najmniej 1GB
15. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów)
16. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza.
17. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
18. Wielkość tablicy routingu: minimum 320000 wpisów dla IPv4 oraz 160000 dla IPv6

19. Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 480 portów 25GbE SFP28. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)).
20. Łącznie w stos z wykorzystaniem portów 25GbE, 40GbE, 100GbE i agregowanych portów 25GbE, 40GbE, 100GbE (w celu zwiększenia przepustowości w stosie)
21. Możliwość realizacji łączy agregowanych w ramach różnych przełączników będących w stosie
22. Możliwość realizacji łączy agregowanych w ramach różnych przełączników nie będących w stosie (tzw. MLAG, Multi chassis Link Aggregation)
23. Tablica adresów MAC o wielkości minimum 280000 pozycji
24. Tablica ARP o wielkości minimum 270000 wpisów
25. Obsługa ramek Jumbo o wielkości minimum 9400B
26. Obsługa Quality of Service
27. Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), explicit congestion notification (ECN), SP+WFQ oraz SP+WDRR
28. Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
29. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ oraz co najmniej 2000 interfejsów VLAN
30. Funkcja mapowania VLAN (co najmniej 1:1, N:1 2:2 i 1:2)
31. Obsługa IGMP v1/v2/v3 oraz IGMP Snooping
32. Obsługa MLD v1/v2 oraz MLD Snooping
33. Wsparcie dla FibreChannel over Ethernet
34. Obsługa VXLAN ze wsparciem co najmniej 4000 tuneli
35. Wsparcie dla Data Center Bridging (DCB):

- Data Center Bridging Exchange (DCBX)
- IEEE 802.1Qbb Priority Flow Control (PFC)
- IEEE 802.1Qaz Enhanced Transmission Selection (ETS)

36. Routing IPv4 – statyczny i dynamiczny (min. RIP, OSFP, ISIS, BGP)
37. Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, IS-ISv6, BGP4+)
38. Obsługa Policy Based Routing (dla IPv4 i IPv6)
39. Obsługa PIM-DM oraz PIM-SM
40. Obsługa Multicast Source Discovery Protocol (MSDP)
41. Obsługa Multicast VLAN dla IPv4 oraz IPv6
42. Obsługa tunelowania GRE

43. Obsługa mechanizmów: Dual stack (RFC 2767), tunelowania (IPv4 over IPv4, IPv4 over IPv6, IPv6 over IPv4, IPv6 over IPv6, ISATAP)
44. Obsługa ECMP (Equal Cost Multi Path)
45. Obsługa mechanizmu Bidirectional Forwarding Detection (BFD) dla OSFP, ISIS, BGP, OSPFv3, ISISv6, BGP4+, PIM oraz routing statycznego
46. Obsługa Unicast Reverse Path Forwarding (uRPF, RFC 3704)
47. Obsługa Virtual Router Redundancy Protocol (VRRP)
48. Funkcja typu Smart Link backup – umożliwiająca szybkie (poniżej 100ms) przełączanie pomiędzy redundantnymi ścieżkami
49. Funkcja pozwalająca na automatyczne wyłączenie określonego połączenia w przypadku awarii innego, określonego połączenia
50. Obsługa Ethernet Ring Protection Switching (ERPS)
51. Funkcja izolacji portów
52. Serwer DHCP (RFC 2131), klient DHCP, obsługa opcji 82 (RFC 3046), DHCP snooping, serwer DHCPv6
53. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia.
54. Obsługa standardu 802.1p, 8 kolejek wyjściowych na każdym porcie
55. Funkcja ograniczania pasma na porcie oraz committed access rate (CAR)
56. Funkcja zmiany wartości pola DSCP i wartości priorytetu 802.1p
57. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, Flow mirroring, L2 remote mirroring, L3 remote mirroring
58. Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS
59. Zarządzanie poprzez port konsoli, SNMP v1, 2c i 3, Telnet, SSH v2, Puppet
60. Obsługa Syslog
61. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED
62. Obsługa sFlow
63. Obsługa Network Configuration Protocol (NETCONF)
64. Obsługa Network Time Protocol (NTP) i Simple Network Time Protocol (SNTP)
65. Obsługa Precision Time Protocol (PTP)
66. Obsługa Ethernet OAM
67. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego
68. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python oraz TCL
69. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter

70. Funkcja przechwytywania pakietów (packet capture) i zapisywania ich do pliku typu pcap z możliwością późniejszej ich analizy przy pomocy zewnętrznego oprogramowania oraz bezpośrednio na przełączniku
71. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
72. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
73. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
74. Funkcja automatycznego zapisywania konfiguracji (archiwizacji) w określonych interwałach czasu
75. Funkcja przywracania konfiguracji (tzw. rollback) po zadanym okresie czasu, np. w przypadku utraty połączenia z przełącznikiem
76. Funkcja porównywania i znajdowania różnic pomiędzy konfiguracjami zapisanymi na przełączniku (w tym aktualnie działającej konfiguracji, nawet jeżeli nie została jeszcze zapisana do pamięci stałej)
77. Funkcja automatycznej podmiany aktualnej konfiguracji na konfigurację wcześniej zapisaną bez konieczności resetu (rebootu) przełącznika
78. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
79. Minimalny zakres temperatur pracy od 0°C do 45°C
80. Wysokość w szafie 19” – 1U. Głębokość nie większa niż 50cm
81. Maksymalny pobór mocy nie większy niż 700W
82. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
83. Minimum 5 letnia gwarancja (serwis) producenta zapewniająca dostawę sprawnego sprzętu na wymianę na maksymalnie następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu z oprogramowaniem. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego.

Przełącznik Typ 3

1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T

2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130 Mp/s
5. Tablica adresów MAC o wielkości minimum 16000 pozycji
6. Pamięć stała (typu Flash): minimum 256MB
7. Pamięć operacyjna: minimum 512MB
8. Obsługa ramek Jumbo
9. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT, nie mniej niż 210 portów 1000BaseX i ich kombinacji.
10. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
11. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
12. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
13. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
14. Policy Based Routing
15. Wsparcie dla Bidirectional Forwarding Detection (BFD)
16. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
17. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
18. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
19. Obsługa IEEE 802.1ad QinQ i Selective QinQ
20. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
21. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
22. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)
23. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
24. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
25. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
26. Obsługa standardu 802.1p – min. 8 kolejek na porcie
27. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p

28. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
29. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
30. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
31. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

    • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

    • Możliwość uwierzytelniania wielu użytkowników na jednym porcie

    • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

    • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
32. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
33. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
34. TACACS+ i RADIUS Network Login
35. RADIUS Accounting
36. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
37. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
38. Syslog
39. Obsługa NETCONF
40. Obsługa sFlow
41. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
42. Obsługa NTP i SNTP
43. Obsługa protokołów 802.3ah
44. Obsługa protokołu IPsec
45. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
46. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
47. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
48. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku

tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

49. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
50. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol
51. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
52. Minimalny zakres pracy od -5°C do 45°C
53. Wysokość w szafie 19” – 1U, głębokość nie większa niż 25 cm
54. Maksymalny pobór mocy nie większy niż 45W
55. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
56. 5 letnia gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczony bezpośrednio przez autoryzowany serwis producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producentem sprzętu.

Przełącznik Typ 4

1. Minimum 24 porty 10BASE-T/100BASE-TX/1000BASE-T
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 95 Mp/s
5. Tablica adresów MAC o wielkości minimum 16000 pozycji
6. Pamięć stała (typu Flash): minimum 256MB
7. Pamięć operacyjna: minimum 512MB
8. Obsługa ramek Jumbo
9. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT, nie mniej niż 210 portów 1000BaseX i ich kombinacji.
10. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
11. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie

12. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
13. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
14. Policy Based Routing
15. Wsparcie dla Bidirectional Forwarding Detection (BFD)
16. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
17. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
18. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
19. Obsługa IEEE 802.1ad QinQ i Selective QinQ
20. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
21. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
22. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)
23. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
24. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
25. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
26. Obsługa standardu 802.1p – min. 8 kolejek na porcie
27. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
28. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
29. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
30. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
31. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

    • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

    • Możliwość uwierzytelniania wielu użytkowników na jednym porcie

    • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

    • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
32. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
33. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
34. TACACS+ i RADIUS Network Login

35. RADIUS Accounting
36. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
37. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
38. Syslog
39. Obsługa NETCONF
40. Obsługa sFlow
41. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
42. Obsługa NTP i SNTP
43. Obsługa protokołów 802.3ah
44. Obsługa protokołu IPsec
45. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
46. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
47. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
48. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
49. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
50. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol
51. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
52. Minimalny zakres pracy od -5°C do 45°C
53. Wysokość w szafie 19” – 1U, głębokość nie większa niż 20 cm
54. Maksymalny pobór mocy nie większy niż 25W
55. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
56. 5 letnia gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczony bezpośrednio przez autoryzowany serwis

producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producentem sprzętu.

Przełącznik Typ 5

1. Minimum 24 porty 100/1000BaseT wspierające standard 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP), umieszczonych z przodu obudowy
3. Minimum jeden slot rozszerzeń pozwalający na rozbudowę o dodatkowe dwa porty: 10Gb SFP+, 10Gb w standardzie 10GBaseT ze wsparciem dla MACsec i pełnym wsparciem standardu 10GBaseT – transmisja na odległość 100m. Wymagane jest by obie opcje rozbudowy były dostępne w momencie zaoferowania przełącznika
4. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa, niezależne, moduły wentylatorów)
5. Modularny, wewnętrzny, zasilacz prądu zmiennego, zapewniający budżet mocy dla PoE nie mniejszy niż 450W. Slot na drugi modularny, wewnętrzny zasilacz prądu zmiennego. Zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco. Drugi zasilacz musi zwiększać budżet mocy do co najmniej 740W.
6. Przepustowość: minimum 168 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
7. Wydajność: minimum 160 Mp/s
8. Tablica adresów MAC o wielkości minimum 32000 pozycji
9. Bufor pakietów nie mniejszy niż 4MB
10. Pamięć stała (typu Flash): minimum 512MB
11. Pamięć operacyjna: minimum 2GB
12. Port USB co najmniej w wersji 2.0
13. Niezależny od portów podstawowych, port Ethernet dedykowany do zarządzania pozapasmowego (out-of-band management).
14. Obsługa ramek Jumbo
15. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 400 portów 100/1000BaseT
16. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
17. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
18. Routing IPv4 – minimum: statyczny, RIP v1 i v2
19. Routing IPv6 – minimum: statyczny
20. Policy Based Routing
21. Tablica routingu: minimum 8000 wpisów

22. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
23. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
24. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
25. Obsługa IEEE 802.1ad QinQ i Selective QinQ
26. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
27. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
28. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping
29. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
30. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
31. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
32. Obsługa standardu 802.1p – min. 8 kolejek na porcie
33. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
34. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
35. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
36. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
37. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

    • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

    • Możliwość uwierzytelniania wielu użytkowników na jednym porcie

    • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

    • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
38. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
39. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
40. TACACS+ i RADIUS Network Login
41. RADIUS Accounting
42. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
43. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
44. Syslog

45. Obsługa NETCONF
46. Obsługa sFlow
47. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
48. Obsługa NTP
49. Obsługa protokołu 802.3ah
50. Obsługa TR-069
51. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
52. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
53. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
54. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
55. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
56. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol
57. Modularny system operacyjny ze wsparciem skryptów w języku Python
58. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
59. Minimalny zakres pracy od -5°C do 45°C
60. Wysokość w szafie 19” – 1U, głębokość nie większa niż 47 cm
61. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
62. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. Wszystkie opisane funkcje muszą być dostępne łącznie, to jest na tym samym rodzaju i wersji systemu operacyjnego przełącznika (firmware)
63. 5 letnia gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczony bezpośrednio przez autoryzowany serwis

producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producentem sprzętu.

Przełącznik Typ 6

1. Minimum 48 portów 100/1000BaseT wspierające standard 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP), umieszczonych z przodu obudowy
3. Minimum jeden slot rozszerzeń pozwalający na rozbudowę o dodatkowe dwa porty: 10Gb SFP+, 10Gb w standardzie 10GBaseT ze wsparciem dla MACsec i pełnym wsparciem standardu 10GBaseT – transmisja na odległość 100m. Wymagane jest by obie opcje rozbudowy były dostępne w momencie zaoferowania przełącznika.
4. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa, niezależne, moduły wentylatorów)
5. Modularny, wewnętrzny, zasilacz prądu zmiennego, zapewniający budżet mocy dla PoE nie mniejszy niż 800W. Slot na drugi modularny, wewnętrzny zasilacz prądu zmiennego. Zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco. Drugi zasilacz musi zwiększać budżet mocy do co najmniej 1440W.
6. Przepustowość: minimum 216 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
7. Wydajność: minimum 180 Mp/s
8. Tablica adresów MAC o wielkości minimum 32000 pozycji
9. Bufor pakietów nie mniejszy niż 4MB
10. Pamięć stała (typu Flash): minimum 512MB
11. Pamięć operacyjna: minimum 2GB
12. Port USB co najmniej w wersji 2.0
13. Niezależny od portów podstawowych, port Ethernet dedykowany do zarządzania pozapasmowego (out-of-band management).
14. Obsługa ramek Jumbo
15. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 400 portów 100/1000BaseT
16. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
17. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
18. Routing IPv4 – minimum: statyczny, RIP v1 i v2
19. Routing IPv6 – minimum: statyczny
20. Policy Based Routing
21. Tablica routingu: minimum 8000 wpisów

22. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
23. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
24. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
25. Obsługa IEEE 802.1ad QinQ i Selective QinQ
26. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
27. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
28. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping
29. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
30. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
31. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
32. Obsługa standardu 802.1p – min. 8 kolejek na porcie
33. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
34. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
35. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
36. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
37. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

    • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

    • Możliwość uwierzytelniania wielu użytkowników na jednym porcie

    • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

    • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
38. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
39. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
40. TACACS+ i RADIUS Network Login
41. RADIUS Accounting
42. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
43. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
44. Syslog
45. Obsługa NETCONF

46. Obsługa sFlow
47. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
48. Obsługa NTP
49. Obsługa protokołu 802.3ah
50. Obsługa TR-069
51. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
52. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
53. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
54. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
55. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
56. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol
57. Modularny system operacyjny ze wsparciem skryptów w języku Python
58. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
59. Minimalny zakres pracy od -5°C do 45°C
60. Wysokość w szafie 19” – 1U, głębokość nie większa niż 47 cm
61. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
62. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
63. 5 letnia gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczona bezpośrednio przez autoryzowany serwis producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producenta sprzętu.

Przełącznik Typ 7 i Typ 8

1. Minimum 14 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+) na co najmniej 12 portach
2. Minimum 2 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 68 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 45 Mp/s
5. Bufor pakietów: minimum 12 MB
6. Minimum 4GB pamięci operacyjnej
7. Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port konsoli USB
9. Port USB 2.0 (niezależny od portu konsoli USB)
10. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 130W. Pobór mocy (bez PoE) nie może być większy niż 25W.
11. Wielkość tablicy routingu: minimum 500 wpisów IPv4, 500 wpisów IPv6
12. Wielkość tablicy ARP co najmniej 1000 wpisów, wielkość tablicy ND co najmniej 500 wpisów
13. Tablica adresów MAC o wielkości minimum 8000 pozycji
14. Obsługa Jumbo Frames co najmniej 9198 bajtów
15. Obsługa sFlow lub Netflow
16. Obsługa REST API
17. Obsługa RMON (minimum grupy 1,2,3 i 9)
18. Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN
19. Obsługa protokołu MVRP
20. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
21. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
22. Obsługa Secure FTP lub SCP
23. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
24. Obsługa SNTPv4 lub NTP
25. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
26. Obsługa protokołów rutingu: ruting statyczny
27. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup)
28. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)

29. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
30. Mechanizmy związane zzapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
31. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
32. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
33. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
34. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
35. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
36. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
37. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
38. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
39. Obsługa list kontroli dostępu (ACL)
40. Zakres pracy od 0 do 45°C
41. Pasywne chłodzenie (brak wentylatorów)
42. Przełącznik w obudowie maksymalnie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 27 cm.
43. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
44. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
45. 5 letnia gwarancja producenta zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczona bezpośrednio przez autoryzowany serwis producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producenta sprzętu.

Bezprzewodowy punkt dostępowy i kontroler sieci bezprzewodowej

1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax.
2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej

3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:

   a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https

   b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki

   c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.

4. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:

   a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego

   b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny

   c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe

   d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję

   e. Tworzenie klastra do 130 urządzeń

5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP
6. Punkt dostępowy musi mieć możliwość pracy jako analizator widma
7. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa
8. W system musi być wbudowany serwer DHCP
9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:

    a. EAP-TLS

    b. PEAP-MSCHAPv2

    c. PEAP-GTC

    d. TTLS-MSCHAPv2

11. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP
12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:

a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania

b. Zewnętrzny portal WWW

15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:

    a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe

    b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu

    c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma

    d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału

    e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz

    f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)

    g. Wsparcie dla 802.11d oraz 802.11h

    h. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane
18. Minimalizacja interferencji związanych z sieciami 3G/4G LTE
19. Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej
20. Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 7dBm)
21. Obsługa roamingu klientów w warstwie 2
22. Obsługa monitoringu przez SNMP
23. Obsługa logowania na zewnętrznym serwerze SYSLOG
24. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
25. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
26. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:

    a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością

    b. Wykorzystanie pasma

    c. Ilość klientów korzystających z systemu/interferujących

    d. Ilość ramek wejściowych/wyjściowych dla każdego radia

    e. Ilość odrzuconych/błędnych ramek/s dla każdego radia

f. Szum tła dla każdego radia

g. Wyświetlanie logów systemowych

27. Punkt dostępowy musi posiadać 4 wbudowane anteny pracujące w trybie 4x4 MIMO, z parametrami co najmniej: 4 dBi dla 2,4GHz, 7.5 dBi dla 5 GHz
28. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax
29. Praca w trybie SU MIMO 4X4:4 dla 5GHz
30. Specyfikacja radia 802.11a/n/ac/ax:

a. Obsługiwana technologia OFDM oraz OFDMA

b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM

c. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm

d. Prędkości transmisji:

• 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,

• MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n

• MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac

• MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz)

• MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz)

e. Obsługa HT – kanały 20/40MHz dla 802.11n

f. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac

g. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax

h. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz

i. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac

j. Wsparcie dla:

• MRC (Maximal ratio combining)

• CDD/CSD (Cyclic delay/shift diversity)

• STBC (Space-time block coding)

• LDPC (Low-density parity check)

• Technologia TxBF

31. Specyfikacja radia 802.11b/g/n/ax:

a. Częstotliwość 2,400 ~2,4835

b. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA

c. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM

d. Moc transmisji konfigurowalna przez administratora

32. Punkt dostępowy musi posiadać co najmniej:

a. 1 interfejs 100/1000 BaseT

- z funkcją auto-sensing link oraz MDI/MDX
- obsługa równoważenie obciążenia „load balancing”

b. 1 interfejs 100/1000/2.5G BaseT (zgodny z 802.3bz)
- z funkcją auto-sensing link oraz MDI/MDX
- z funkcją PoE/PoE+
- obsługa równoważenie obciążenia „load balancing”

c. interfejs konsoli RS-232 (RJ-45) lub USB

d. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli)

e. przycisk przywracający konfigurację fabryczną

f. slot zabezpieczający Keningston

33. Parametry pracy urządzenia:

a. Temperatura otoczenia (zakres minimalny): 0-50 º C

b. Wilgotność (zakres minimalny): 5% - 92%

c. Obsługiwane standardy:

- Ethernet IEEE 802.3 / IEEE 802.3u
- Power-over-Ethernet IEEE 802.3af
- Wireless IEEE 802.11a/b/g/n/ac/ax

d. Znak CE

e. EN 300 328

f. EN 301 489

g. EN 301 893

h. EN 60601-1-1, EN60601-1-2

34. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE.
35. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac
36. Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
37. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni
38. Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

System zarządzania i system analizy aplikacji

- System musi być zbudowany w architekturze klient – serwer

- System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie:

o Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA

o Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetFlow (lub podobnych protokołów) oraz analizy zawartości pakietów SMTP, FTP, http

o Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu

o MPLS oraz VPLS

o Zarządzanie dostępem zdalnym Ipsec/VPN

o Wbudowany serwer TACACS

o Funkcja monitorowania wydajności aplikacji

- System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu

- Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów

- System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet

- Zarządzanie siecią bezprzewodową WLAN (licencja pozwalająca na obsługę co najmniej 50 punktów dostępowych)

- Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz NetFlow (lub podobnych protokołów) z urządzeń sieciowych oraz obrazowanie wyników (licencja na obsługę w tym zakresie co najmniej 5 urządzeń jednocześnie)

- System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o:

o Średnim wykorzystaniu CPU i pamięci RAM

o Średnim czasie odpowiedzi urządzenia

o Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego)

o Ilość błędnych lub odrzuconych pakietów na interfejsie

- System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH

- System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup'ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup'ów (minimum 30 dni) wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia

- System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL.

- System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate)

- System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN a zarządzanych urządzeniach.

- System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej implementacji przechowywanych w systemie ACL na urządzeniach

- System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń

- System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy)

- System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany.

- System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS'em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane.

- System musi pozwalać na budowanie widoków przez administratora

- System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.)

- System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu.

- System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci.

- System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik

- System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10- 1800 sekund)

- System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC, Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy.

- System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie

- System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym:

o Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect, Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect

o Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku.

o Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku.

-System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową

- System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android

- System musi posiada funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox)

- System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail

- System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia.

- System musi posiadać funkcję zarządzania VXLAN – tworzenie listy urządzeń wspierających VXLAN, tworzenie tuneli, tworzenie topologii sieci VXLAN, wyświetlanie informacji o statystykach ruchu w tunelach

- System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na:

o Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP.

o Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell.

o Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI.

o Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami.

o Migrację wirtualnych maszyn pomiędzy fizycznymi serwerami.

o Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w:

*Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania), CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych.

*Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów.

*Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended).

o Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej.

o Dodawanie, klonowanie i usuwanie wirtualnych masz.

o Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V,zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny.

o Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu" pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego. Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby.

- System musi posiadać funkcje zarządzania co najmniej dla 1000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System

- System musi posiadać funkcję automatycznej aktualizacji przez Internet. - System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.

- System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled)

- System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy

- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

System kontroli dostępu

System do kontroli dostępu musi charakteryzować się następującymi cechami:

• Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)

• System musi odsługiwać minimum 2500 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia

• Praca jako maszyna wirtualna

• Musi posiadać wbudowany serwer Radius oraz TACACS + (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)

• Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:

o Cisco Systems

o Fortinet

o Microsoft

o Alcatel-lucent Enterprise

o Huawei Networks

o Extreme Networks

o PaloAlto Networks

o Producenta urządzeń opisanych w tym dokumencie

•System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.

• System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.

• Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.

• Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych

o Microsoft Active Directory

o Radius

o Kerberos

o LDAP

o ODBC

o Współpraca z serwerami tokenów

• Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)

o DHCP

o TCP

o MAC OUI

o SNMP

o Cisco device sensor

• Wspierać protokoły

o Radius, Radius CoA, TACACS +, web authentication, SAML v2.0

o EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)

o PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)

o TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)

o EAP-TLS o PAP, CHAP, MSCHAPv1 i v2, EAP-MD5

o NAC, Microsoft NAP

o Windows machine authentication

o MAC Auth

o Audit (role oparte na porcie oraz skanowanie podatności)

o OCSP (Online Certificate Status Protocol)

o SNMP generic MIB, SNMP private MIB

o CEF (Common Event Format), LEEF (Log Event Extended Format)

o TLS 1.2

• Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)

• Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:

o Co najmniej ESX 4.0, ESXi 4.1 do 6.0

o Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise

- Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich. Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności o Samodzielna rejestracja klientów gościnnych w oparciu o:

o Adres e-mail

o Numer telefonu (wiadomość SMS)

o Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)

o Logowanie w oparciu o portale społecznościowe

o Funkcja integracji z systemami trzecimi poprzez API

o Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową

o Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.

o Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.

o Funkcja personalizacji strony gościnnej

- Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

• Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT

• System musi wspierać obsługę następujących systemów operacyjnych

o MS Windows

o Mac OS X

o iOS

o Android

o Chromebook

o Ubuntu

• Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci

• Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej

• Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.

• Funkcja tworzenia unikalnych certyfikatów dla urządzeń.

• Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń

• Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID - Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

System kontroli końcówek klienckich musi mieć następujące funkcjonalności

• System musi wspierać następujące systemy operacyjne

o Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)

o Apple Mac OS X 10.7 i nowsze

o Red HAT Enterprise Linux 4 i nowsze

o CentOS 4 (Community Enterprise Operating System) i nowsze

o Fedora Core 5 i nowsze

o SUSE linux 10.x i nowsze

• Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall

• Wyświetlanie informacji on-line o statusie monitorowanych końcówek

• System powinien obsługiwać agenta w formie

o Stałej (Presistent Agent)

o Tymczasowej (Dissolvabe Agent)

o Agenta NAP

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio

przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

Odpowiedź nr 48:

Zamawiający podtrzymuje zapisy OPZ. W ocenie Zamawiającego zapisy spełnia więcej niz jeden producent.

Pytanie nr 49:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność" wskazał, iż przyzna 5 pkt jeżeli przełączniki typ 3- 6 będą posiadały obsługę RADIUS over TLS (RadSec). W związku z tym, iż ww. protokół nie jest obligatoryjnie wymagany na wszystkich rodzajach przełączników dostępowych technologia ta nie zapewnizakładanej skuteczności, co podważa istotę zastosowania tej technologii i jej punktacji. W ocenie Wykonawcy wartością dodaną dla Zamawiającego byłoby przyznanie 5 punktów za rozwiązanie technologiczne oparte o licencje wieczyste/permanentne. Tego typu rozwiązanie jest korzyścią dla Zamawiającego gdyż ogranicza koszty i oszczędza czas jaki Zamawiający musiałby przeznaczyć na zakupy subskrypcji w kolejnych latach.

Odpowiedź nr 49:

Zamawiający podtrzymuje zapisy SWZ umieszczone w rozdziale XVI Kryteria oraz sposób oceny ofert dotyczące kryterium "Funkcjonalność".

Pytanie nr 50:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność" wskazał, iż przyzna 3 pkt jeżeli przełączniki typ 3- 6 będą posiadały możliwość rozbudowy przełącznika o „wyniesione" porty (urządzenia) zarządzane z przełącznika – przykładowo zamiast prostych niezarządzalnych 8 portowych przełączników, urządzenie zarządzalne z przełącznika nadrzędnego. W związku z niejednoznacznie interpretowanym przez Wykonawców a utworzonym przez Zamawiającego zapisem dotyczącym „wyniesionych" portów (urządzeń) w opisach przełączników Wykonawca zwraca się z wnioskiem o dodanie zapisu: „Łączenie w stos min. 9 przełączników"

Odpowiedź nr 50:

Zamawiający podtrzymuje zapisy SWZ umieszczone w rozdziale XVI Kryteria oraz sposób oceny ofert dotyczące kryterium "Funkcjonalność".

Pytanie nr 51:

Dotyczy Rozdziału XVI. Kryteria oraz sposób oceny ofert SWZ Zamawiający w Kryterium „Funkcjonalność" wskazał, iż przyzna 2 pkt jeżeli przełączniki typ 1 będą posiadały obsługę 802.1aq Shortest Path Bridging (SPB) MAC-in-MAC oraz obsługę IETF RFC 6329 IS-IS Extensions supporting IEEE 80 2.1aq SPB. Wykonawca wskazuje, iż ww. technologia jest już przestarzała. Czy w związku z powyższym Zamawiający wyrazi zgodę na modyfikację ww. kryterium i przyznanie punktu w przypadku gdy zaoferowane rozwiązanie będzie obsługiwało technologię nowszej generacji, tj. Virtual eXtensible Local Area Network (VXLAN).

Odpowiedź nr 51:

Zamawiający podtrzymuje zapisy SWZ umieszczone w rozdziale XVI Kryteria oraz sposób oceny ofert dotyczące kryterium "Funkcjonalność".

Pytanie nr 52:

Dotyczy Załącznika nr 7 do SWZ pkt 6.2.4 Przełącznik typ 1 W ocenie Wykonawcy architektura, którą należy zaprojektować w tym postępowaniu, wymagać powinna:

A) od przełączników typ 1

Punkt 1 1.2 Zwiększenie liczby portów 100Gb z 6 do 8.

Punkt 1 1.5 Zwiększenie tablicy MAC z 92000 do 280000.

Punkt 2 1.2 Zwiększenie pojemności tablicy routingu IPv4 z 16000 wpisów do 300000 wpisów

Punkt 3 1.2 Zwiększenie pojemności tablicy routingu IPv6 z 7500 wpisów do 160000 wpisów

B) od przełączników typ 2

Punkt 1 1.6 (pierwsze wymaganie w tym typie urządzeń błędnie oznaczone numerem 1.6) Zwiększenie liczby portów 100Gb z 6 do 8.

Punkt 1 1.10 Zwiększenie tablicy MAC z 92000 do 280000.

Punkt 2 1.2 Zwiększenie pojemności tablicy routingu IPv4 z 128 000 wpisów do 300 000 wpisów

Punkt 3 1.2 Zwiększenie pojemności tablicy routingu IPv6 z 32 000 wpisów do 160 000 wpisów

Punkt 2 1.4 b, c, d oraz punkt 3 1.4 a, b, c – protokoły routingu dynamicznego grają kluczową rolę w środowiskach Data Center. W związku z tym w ocenie Wykonawcy uznać należy, że protokoły te powinny być od razu dostępne, bez narażania Zamawiającego na nadmierne koszty związane z późniejszym zakupem dodatkowych licencji? Wykonawca sugeruje wykreślenie zapisów „możliwość rozszerzenia przez licencje”

Odpowiedź nr 52:

Zamawiający podtrzymuje zapisy OPZ.

Zamawiający informuje, iż powyższe pytania i odpowiedzi, wyjaśnienia do treści SWZ, stanowią jej integralną część, a przy tym z uwagi na ich zakres i charakter oraz termin wprowadzenia nie wpływają na konieczność przedłużenia terminu składania ofert. Nie są tym samym spełnione przesłanki wynikające z ustawy PZP. Dlatego też, Zamawiający zawiadamia, iż terminy składania i otwarcia ofert nie ulegają zmianie, podobnie jak i godziny składania i otwarcia ofert oraz miejsce pozostają bez zmian.

Dokument podpisany przez Piotr Szymański
Data: 2023.02.10 14:53:00 CET