

dotyczy: **rozpoznania rynku – zapytania ofertowego pozaustawowego dla zamówienia, którego wartość nie przekracza kwoty netto 130 000 zł**

Miejskie Centrum Oświaty i Usług Wspólnych w Nowym Targu, w celu rozpoznania rynku zaprasza do składania ofert na:

1. **Przedmiot zamówienia:** dostawa serwera, urządzenia UTM, zasilacza awaryjnego UPS z jednoczesnym wdrożeniem oprogramowania na serwerze i UTM dla potrzeb Miejskiego Centrum Oświaty i Usług Wspólnych w Nowym Targu
2. **Opis przedmiotu zamówienia:** przedmiot zamówienia zgodny z poniższymi parametrami:
 - I. **SERWER DELL PowerEdge T440:**
 - 1) **Obudowa:** Tower
 - 2) **Płyta główna:** obsługa dwóch procesorów, zaprojektowana przez producenta serwera,
 - 3) **Procesor 2 x Intel® Xeon® Silver 4208:**
 - ilość rdzeni: 8,
 - taktowanie: 2.1 Ghz,
 - taktowanie turbo: 3.20 Ghz,
 - szyna Pamięci (MHz): 2400 MHz,
 - pamięć cache: 11 MB,
 - QPI: 9.60 GT/s 2 UPI,
 - pobór mocy (W): 85 W,
 - ilość rdzeni/ wątków: 8/16.
 - 4) **Pamięć RAM**
 - całkowita pojemność pamięci min. 96 GB, przy czym jednostka powinna posiadać wolne sloty umożliwiające rozbudowę serwera do min. 128 GB,
 - szyna 3200 MHz,
 - typ DDR4,
 - rodzaj: RDIMM,
 - Dual Rank
 - 5) **Kontroler RAID: PERC H740P**
 - typ kontrolera: Sprzętowy,
 - poziomy RAID: 0,1,5,6,10,50,60,
 - rodzaje dysków: SATA, SAS, SSD, SED,
 - pamięć cache: 2GB NV,
 - max. Transfer: 12Gb/s,
 - wspierane systemy: Windows, Linux, Vmware.
 - 6) **Karta graficzna:**
 - zintegrowana karta graficzna
 - 7) **Dyski:** Dyski twarde typu Hot-Plug fabrycznie zainstalowane w serwerze. Serwer powinien pozwalać na zainstalowanie przynajmniej 8 dysków typu SATA, SAS, NLSAS, SSD SATA, SSD SAS lub PCIe.

Należy dostarczyć dyski o następujących parametrach:

- ilość dysków: 4 szt.,
- pojemność każdego dysku: 2 TB,
- typ dysku: magnetyczny,
- interfejs NLSAS 12Gb/s
- prędkość obrotowa: 7200 obr/min,
- typ obudowy: Hot-Plug.
- ilość dysków: 2 szt.,
- pojemność każdego dysku: 480 GB,
- typ dysku: SSD,
- interfejs SATA 6Gb/s
- typ obudowy: Hot-Plug.

8) Karta sieciowa:

- porty: 4 x RJ-45, GbE 10/100/1000 lub 2 karty po 2 x RJ45, GbE 10/100/1000

9) Zdalne zarządzanie iDRAC9 Enterprise

- dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera,
- dedykowany port: Tak

10) Zasilanie: 2 x 750W (Hot-Plug)

- certyfikowane jednostki zasilające Dell,
- typ: Hot-Plug,
- redundancja: Tak

11) Gwarancja 3 lata Basic NBD+ KYHD.

Gwarancja producenta realizowana w miejscu instalacji sprzętu z określonym czasem reakcji od przyjęcia zgłoszenia. Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela.

- okres gwarancji 3 lata,
- okres gwarancji dysków min. 1 rok,
- typ wsparcia Gwarancja podstawowa,
- czas reakcji Następnego dnia robocznego,
- dodatkowa opcja serwisowa gwarantująca, iż w przypadku awarii, uszkodzone dyski twarde pozostaną u użytkownika, a w ich miejsce zostaną dostarczone nowe: 3 lata.

12) Wyposażenie dodatkowe:

- Okablowanie niezbędne do uruchomienia urządzenia,
- RDX Cartridge 4TB 3 szt.

13) Oprogramowanie

- Microsoft Windows Server 2019 Standard,
- Microsoft Windows Server 2019 CAL User 20 lic.

II. URZĄDZENIE UTM Stormshieeld SN310:

1) Wydajność

- przepustowość Firewall (1518-bajtowa ramka danych) 4Gbps
- przepustowość IPS (1518-bajtowa ramka danych) 2,4 Gbps
- przepustowość IPS (pliki HTTP 1 MB) 1,2 Gbps
- przepustowość Antywirusa 495 Mbps

2) VPN

- przepustowość IPSec - AES GCM 175 Mbps
- przepustowość IPSec - AES256/SHA2 600 Mbps
- maks. liczba tuneli IPSec VPN 100
- maks. liczba SSL VPN (tryb Portal) 50
- liczba jednoczesnych klientów SSL VPN 20

3) Połączenia sieciowe

- liczba jednoczesnych sesji 300 000
- nowe sesje na sekundę 18 000
- maksymalna liczba dostawców internetu/zapasowych 64/64

4) Interfejsy sieciowe

- Interfejsy Ethernet 10/100/1000 8

5) Obsługa sieci

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.IPS

6) ZAPORA KORPORACYJNA (Firewall)

- urządzenie ma być wyposażone w Firewall klasy Stateful Inspection,
- urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT,
- urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge),
- Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie,
- administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia,
- rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
- administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
- edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
- Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

7) INTRUSION PREVENTION SYSTEM (IPS)

- system detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

- moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
- moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
- administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
- moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej.
- urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
- administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
- urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

8) KSZTAŁTOWANIE PASMA (Traffic Shapping)

- urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
- ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
- rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
- urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

9) OCHRONA ANTYWIRUSOWA

- rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
- administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

10) OCHRONA ANTYSZPAM

- producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
- ochrona antyspam ma działać w oparciu o:
 - i. białe/czarne listy,
 - ii. DNS RBL,
 - iii. heurystyczny skaner.
- w przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
- wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

11) FILTR DOSTĘPU DO STRON WWW

- urządzenie ma posiadać wbudowany filtr URL.
- filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
- administrator musi mieć możliwość dodawania własnych kategorii URL.
- urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
- moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
- administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
 - i. blokowanie dostępu do adresu URL,
 - ii. zezwolenie na dostęp do adresu URL,
 - iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
- administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
- filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
- urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

12) UWIERZYTELNIANIE

- urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
 - i. lokalną bazę użytkowników (wewnętrzny LDAP);
 - ii. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - iii. usługę katalogową Microsoft Active Directory.

13) Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.

- Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły:
 - i. SSL,
 - ii. Radius,
 - iii. Kerberos.
- urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
- co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
- autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

14) ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

- urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
 - i. równoważenie względem adresu źródłowego,

- ii. równoważenie względem połączenia.
- mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
- urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
- urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
- rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
- Rozwiązanie powinno wspierać technologię Link Aggregation.

15) POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

- urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
- urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
- konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
- urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS.
- urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
- urządzenie musi posiadać usługę DNS Proxy.
- urządzenie musi posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

16) ADMINISTRACJA URZĄDZENIEM

- konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
- komunikacja może odbywać się na porcie innym niż https (443 TCP).
- urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
- Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
- urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
- rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
- urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.

- urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
- urządzenie musi posiadać funkcjonalność anonimizacji logów.
- wymaga się, aby dostawa obejmowała również minimum 12-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.
- urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.

III. UPS ZASILACZ AWARYJNY SMC1500I-2UC Smart UPS C 1500VA/900W 2U Smart Connect:

1) Parametry

- Moc pozorna 1500 VA
- Moc czynna 900 W
- Architektura UPS-a line-interactive
- Liczba faz na wejściu 1 (230V)
- Czas przełączenia (maks.) 10 ms
- Czas podtrzymania (obciążenie 100%) 10.1 min
- Czas ładowania 3 h
- Typ obudowy Rack
- Porty zasilania we. IEC-C14
- Porty zasilania wy. 4 x IEC-C13
- Gniazda we/wy 1 x USB (Type B) 1 x RJ-45 (iLO Remote Management Network)

IV. WDROŻENIE OPROGRAMOWANIA NA SERWERZE I UTM

Szczegółowe dane dotyczące nazw serwerów, adresacji IP, parametrów maszyn wirtualnych, nazw i haseł użytkowników z uprawnieniami administratora zostaną dostarczone przed rozpoczęciem prac wdrożeniowych. Zakres usługi:

- 1) Montaż w serwerze napędu RDX.
- 2) Umieszczenie serwera w szafie.
- 3) Podłączenie do sieci LAN.
- 4) Konfiguracja RAID1 na dyskach SSD.
- 5) Konfiguracja RAID10 na dyskach SAS.
- 6) Aktualizacja oprogramowania układowego serwera.
- 7) Konfiguracja modułu zdalnego zarządzania iDRAC.
- 8) Instalacja systemu Windows Server 2019 Standard wraz z poprawkami bezpieczeństwa.
- 9) Instalacja roli Hyper-V.
- 10) Konfiguracja portu sieciowego serwera.
- 11) Konfiguracja trzech przełączników dla wirtualnych serwerów na osobnych portach karty sieciowej nie współdzielonych przez system hiperwizora.
- 12) Uruchomienie pierwszego serwera wirtualnego z rolą Active Directory i DHCP.
- 13) Przeniesienie AD ze starego serwera (Windows 2008R2) na nowy i podniesienie funkcjonalności domeny do najwyższej dostępnej.
- 14) Przeniesienie serwera DHCP z konfiguracją.

- 15) Uruchomienie drugiego serwera wirtualnego z rolą udostępniania plików i instancją serwera MS SQL 2019 Express.
- 16) Instalacja poprawek bezpieczeństwa na serwerach wirtualnych.
- 17) Przeniesienie zasobów udostępnionych ze starego serwera na nowy z niezmienionymi uprawnieniami.
- 18) Przeniesienie bazy danych programu Płatnik.
- 19) Przeniesienie bazy danych programu SJO B@stia.
- 20) Wirtualizacja starego serwera.
- 21) Odinstalowanie na starym serwerze instancji SQL z bazami programu Płatnik, SJO B@stia i wyłączenie nieużywanych więcej usług.
- 22) Konfiguracja kopii zapasowych na nośnik RDX całego serwera.
- 23) Przerobienie zasad grupy (group policy) oraz ustawień użytkowników uwzględniających nowe nazwy serwerów.
- 24) Instalacja i konfiguracja oprogramowania zarządzającego/monitorującego UTM
- 25) Aktualizacja oprogramowania wewnętrznego (firmware)
- 26) Konfiguracja ustawień systemowych – czas, nazwa, automatyczne aktualizacje, itp.
- 27) Konfiguracja interfejsów fizycznych i VLAN
- 28) Tworzenie obiektów zgodnych z topologią sieci i wykorzystywanych usług
- 29) Konfiguracja routingu
- 30) Konfiguracja NTP
- 31) Konfiguracja reguł zapory sieciowej
- 32) Konfiguracja translacji NAT (PAT, FORWARDING, BI-MAP (DMZ))
- 33) Konfiguracja PROXY HTTP, PROXY SMTP, PROXY POP3, PROXY FTP
- 34) Konfiguracja filtra URL
- 35) Konfiguracja SSL VPN (praca zdalna pracowników)
- 36) Testowanie wdrożonej konfiguracji
- 37) Strojenie IPS / HTTPS PROXY
- 38) Zabezpieczenie konfiguracji: kopia zapasowa konfiguracji
- 39) Wsparcie techniczne przez 30 dni po zakończeniu wdrożenia

3. **Dodatkowe wymagania dotyczące realizacji przedmiotu zamówienia:**

- 1) **Termin wykonania zamówienia:** dostawa jednorazowa w terminie 30 dni od daty podpisania umowy, realizacja usługi wdrożenia oprogramowania na serwerze i utm w terminie do 24 grudnia 2021 r.
- 2) Urządzenia muszą być fabrycznie nowe z bieżącej produkcji – rok produkcji 2021
- 3) Urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
- 4) Dostarczenie do Zamawiającego wraz z transportem, rozładunkiem i wniesieniem na wskazane przez Zamawiającego miejsce przedmiotu zamówienia.
- 5) Dostarczeniu i zrealizowaniu przedmiotu zamówienia w cenach brutto określonych zgodnie ze złożoną ofertą.
- 6) Wykonawca oświadcza, że spełnia wszelkie wymagania, jakie zgodnie z powszechnie obowiązującymi przepisami prawa są konieczne dla wykonania niniejszego zamówienia.

4. **Miejsce oraz termin składania ofert:** oferty należy składać w siedzibie Zamawiającego, tj. Miejskie Centrum Oświaty i Usług Wspólnych w Nowym Targu, Plac Evry 3, 34-400 Nowy Targ w terminie do dnia 15 listopada 2021 r. do godz. 10.00.

5. **Osoby upoważnione do kontaktu:** Ewa Bobek, tel. 18 2662043, mail: mcoiuw@mcoiuw.nowytag.pl

6. **Kryteria oceny ofert:** jednym kryterium oceny ofert jest cena brutto – 100%
7. **Płatność:** płatność przelewem wynagrodzenia na rachunek bankowy Wykonawcy wskazany na fakturze nastąpi w ciągu 14 dni od dnia odbioru przedmiotu zamówienia przez Zamawiającego i doręczenia prawidłowo wystawionej przez Wykonawcę faktury. Wykonawca wystawi fakturę na:
Nabywca: Gmina Miasto Nowy Targ, ul. Krzywa 1, 34-400 Nowy Targ, NIP:7350014012
Odbiorca: Miejskie Centrum Oświaty i Usług Wspólnych w Nowym Targu, Plac Evry 3, 34-400 Nowy Targ

Z poważaniem

DYREKTOR
MIEJSKIEGO CENTRUM OŚWIATY
i USŁUG WSPÓLNYCH w NOWYM TARGU

mgr Ewa Bobek

Załączniki:

1. Załącznik nr 1 - Formularz ofert
2. Załącznik nr 2 - Klauzula informacyjna

