Częstochowa, dnia 09.04.2018 r.

Zamawiający:

Asten Group Sp. z o.o.

42-202 Częstochowa, ul. Bór 77/81

34/360 88 77

www.astengroup.pl

projekt_3.3@astengroup.pl

ZAPYTANIE OFERTOWE

dotyczące zakupu wielofunkcyjnej zapory sieciowej (Firewall) - zakup 1 urządzenia

ASTEN GROUP Sp. z o. o. realizuje projekt pn. "Wdrożenie innowacyjnego systemu zarządzania zasobami informacyjnymi w przedsiębiorstwie, polegającego na połączeniu systemu klasy ECM z dostępem do aplikacji z urządzeń mobilnych oraz platformy komunikacji ekstranetowej, co w połączeniu z funkcjonującym w firmie Wnioskodawcy systemem ERP usprawni procesy biznesowe realizowane w przedsiębiorstwie w zakresie elektronicznego obiegu dokumentów i komunikacji wewnątrz przedsiębiorstwa, jak również usprawni bezpośrednią komunikację z klientami i partnerami biznesowymi poprzez elektroniczne biuro obsługi klienta". Projekt dofinansowany jest z Funduszy Europejskich w ramach REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA ŚLĄSKIEGO NA LATA 2014-2020, Działanie 3.3 Technologie informacyjno-komunikacyjne w działalności gospodarczej.

W związku z powyższym zwracamy się z prośbą o złożenie oferty handlowej na **zakup wielofunkcyjnej zapory sieciowej (Firewall) - zakup 1 urządzenia**, zgodnie z przedmiotem zamówienia opisanym poniżej.

Kody zamówienia CPV:

- 30200000-1 (Urządzenia komputerowe)

I. Przedmiot zamówienia obejmuje:

- ***Ia. Skrócony opis przedmiotu zamówienia:***

(I). zakup wielofunkcyjnej zapory sieciowej (Firewall) - zakup 1 urządzenia

Asten Group Sp. z o.o.
42-202 Częstochowa, ul. Bór 77/81
tel. 34 3608377, fax 34 3709469
IDS 241769047, NIP 573-281-47-33

Asteniusz Wyśliwiec
Prezes Zarządu

- ***Ib. Pełny opis przedmiotu zamówienia:***

(I). zakup wielofunkcyjnej zapory sieciowej (Firewall) - zakup 1 urządzenia, zgodnie ze wskazaną specyfikacją:

a. zakup niezbędnej wielofunkcyjnej zapory sieciowej (Firewall), zapewniającej kompletną ochronę, nadzorując ruch sieciowy na styku Internetu i sieci lokalnej (1 urządzenie).

b. Zamawiający założył, że optymalna z punktu widzenia realizacji projektu funkcjonalność zapory Firewall obejmować będzie:

- filtr antyspamowy,
- sieciowy filtr antywirusowy,
- wykrywanie włamań,
- filtrowanie treści,
- router,
- NAT
- standardowe usługi sieciowe.

c. Zamawiający sprecyzował także podstawowe parametry urządzenia i specyfikację sieciową:

- od 8 do 16 portów Ethernet 10/100/1000 Mbps
- od 2 do 4 portów światłowodowych 1Gb/10Gb

d. Zamawiający sprecyzował także specyficzne i niezbędne jego zdaniem kryteria wyboru zapory Firewall, zgodnie ze specyfikacją poniżej:

III. KRYTERIA WYBORU FIREWALLA

OBSŁUGA SIECI

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

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).
5. Interface (GUI) do konfiguracji firewalla 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.

6. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.

7. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).

8. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem typu Windows 2k (Kerberos) lub równoważnym.

INTRUSION PREVENTION SYSTEM (IPS)

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

10. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.

11. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

12. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.

13. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.

14. 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.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

15. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

16. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

17. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

18. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

19. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

20. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.

21. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

22. 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.

OCHRONA ANTYSPAM

23. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

24. Ochrona antyspam ma działać w oparciu o:

    a. białe/czarne listy,

    b. DNS RBL,

    c. heurystyczny skaner.

25. 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.

26. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE (VPN)

27. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

28. Odpowiednio kanały VPN można budować w oparciu o:

    a. PPTP VPN,

    b. IPSec VPN,

    c. SSL VPN

29. SSL VPN musi działać w trybach Tunel i Portal.

30. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

31. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.

32. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

33. Urządzenie ma posiadać wbudowany filtr URL.

34. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.

35. Administrator musi mieć możliwość dodawania własnych kategorii URL.

36. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.

Asten Group Sp. z o.o.
42-202 Częstochowa, ul. Bór 77/81
tel. 34 3608877, fax 34 3709469
IDS 241769047, NIP 573-281-47-33

Asteniusz Wyśniewiec
Prezes Zarządu

37. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.

38. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:

    a. blokowanie dostępu do adresu URL,

    b. zezwolenie na dostęp do adresu URL,

    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

39. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

40. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.

41. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.

42. Urządzenie posiada możliwość identyfikacji oraz blokowania przesyłanych danych z wykorzystaniem typu MIME.

43. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

44. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

UWIERZYTELNIANIE

45. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:

    a. lokalną bazę użytkowników (wewnętrzny LDAP),

    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

    c. usługę katalogową typu Microsoft Active Directory lub równoważną.

46. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:

    a. SSL,

    b. Radius,

    c. Kerberos,

    lub równoważne

47. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej typu Active Directory lub równoważnej.

48. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.

49. Autoryzacja użytkowników z usługi katalogowej typu Microsoft Active Directory lub równoważnej nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).

50. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

51. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

    a. równoważenie względem adresu źródłowego,

    b. równoważenie względem adresu źródłowego i docelowego (połączenia).

52. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do internetu.

53. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

54. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.

55. 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.

56. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

57. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIP, OSPF oraz BGP.

58. Rozwiązanie powinno wspierać technologię Link Aggregation.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

59. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.

60. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.

61. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.

62. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS

63. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.

64. Urządzenie musi posiadać usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM

65. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.

66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

67. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.

68. Komunikacja może odbywać się na porcie innym niż https (443 TCP).

69. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

70. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).

71. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.

72. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

RAPORTOWANIE

73. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

74. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

75. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.

76. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.

77. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.

78. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.

79. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

II. Złożona oferta musi zawierać:

1. nazwę i dane teleadresowe oferenta
2. datę sporządzenia
3. cenę całkowitą **netto i brutto wyrażoną w PLN**
4. termin ważności oferty min. do dnia **15.05.2018 r.**
5. termin wykonania zamówienia, wyrażony w dniach kalendarzowych
6. zasady płatności

III. Sposób i miejsce złożenia oferty:

Oferta musi:

Asten Group Sp. z o.o.
42-202 Częstochowa, ul. Bór 77/81
tel. 34 3608877, fax 34 3709469
IDS 241769047, NIP 573-281-47-33

Asteniusz Myśliwiec
Prezes Zarządu

1. zostać złożona na formularzu ofertowym, stanowiącym **załącznik nr 1** do niniejszego zapytania ofertowego

2. zostać podpisana przez osobę uprawnioną do reprezentacji oferenta, zgodnie z dokumentem rejestrowym oferenta, a w przypadku podpisania oferty przez pełnomocnika, do oferty należy dołączyć pełnomocnictwo uprawniające do jej złożenia i podpisania

3. zawierać załączone podpisane przez osobę uprawnioną do reprezentacji oferenta oświadczenie o braku powiązań osobowych lub kapitałowych z zamawiającym, zgodnie z wzorem stanowiącym **załącznik nr 2** do niniejszego zapytania ofertowego

Oferta może zostać doręczona do Zamawiającego na każdy ze wskazanych poniżej sposobów (decyduje data doręczenia oferty do siedziby Zamawiającego lub na wskazany adres e-mail):

1. przesłana na adres korespondencyjny Zamawiającego wskazany w niniejszym zapytaniu

2. dostarczona osobiście do Zamawiającego na adres wskazany w niniejszym zapytaniu

3. przesłana w formie skanów na adres e-mail: **projekt_3.3@astengroup.pl**

- **Oferty złożone w inny sposób lub dostarczone w innej formie nie będą brane pod uwagę**

IV. Termin składania ofert upływa w dniu **16.04.2018 r.**

- **Decyduje data dostarczenia do siedziby Zamawiającego lub na wskazane konto e-mail**
- **Oferty dostarczone po terminie nie będą rozpatrywane.**

V. Kryteria oceny ofert - maksymalnie 100 punktów:

1. cena netto w PLN - cena wyrażona w PLN netto za wykonanie wskazanego przedmiotu zamówienia (Cena): 85%

Sposób liczenia punktacji:

$$C_p = \frac{C_{min}}{C_o} \times 100 \times 85\%$$

C p - liczba punktów w kryterium "Cena"

C min - najniższa cena spośród złożonych ofert

C o - cena oferty badanej

2. Termin wykonania zamówienia (w dniach kalendarzowych) - czas wykonania wskazanego przedmiotu zamówienia, liczony w dniach kalendarzowych - krótszy termin wykonania zamówienia oznacza wyższą liczbę punktów (Termin wykonania zamówienia): 15%

Aston Group Sp. z o.o.
42-202 Częstochowa, ul. Bór 77/81
tel. 34 3608377, fax 34 3709469
IDS 241769047, NIP 573-281-47-33

Asteniusz Wydrzyński
Prezes Zarządu

Sposób liczenia punktacji wg poniższego wzoru:

$$T\,wz = \frac{T\,min}{T\,o} \times 100 \times 15\%$$

T wz - liczba punktów w kryterium "Termin wykonania zamówienia"

T min - najkrótszy termin wykonania zamówienia wskazany w złożonych ofertach

T o - Termin wykonania zamówienia oferty badanej

VI. Termin realizacji umowy:

- wykonanie przedmiotu zamówienia - przygotowanie dla Zamawiającego wielofunkcyjnej zapory sieciowej (Firewall) - 1 kompletnego urządzenia komputerowego, zgodnie z określoną specyfikacją techniczną - **do dnia 31 maja 2018 r.**

VII. Informacja na temat zakazu powiązań osobowych lub kapitałowych z Zamawiającym:

Zamówienie nie może być udzielane podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

a. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,

b. posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa,

c. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

d. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

W imieniu Zamawiającego,

asten group

Asteniusz Myśliwiec
Prezes Zarządu

asten group
Asten Group Sp. z o.o.
42-202 Częstochowa, ul. Bór 77/81
tel. 34 3608877, fax 34 3709469
Ips 241769047, NIP 573-281-47-33

podpis i pieczątka firmowa

Załączniki:

1. Formularz ofertowy
2. Oświadczenie o braku powiązań osobowych lub kapitałowych z zamawiającym