Szczegółowy opis przedmiotu zamówienia

Zakup wraz z dostawą systemu bezpieczeństwa brzegu sieci w postaci 12 sztuk nieużywanych, fabrycznie nowych, wyprodukowanych nie wcześniej niż w 2018 r. urządzeń Firewall UTM wraz z usługą aktualizacji funkcji bezpieczeństwa dla tych urządzeń w okresie 36 miesięcy od dnia podpisania przez Strony protokołu odbioru bez zastrzeżeń dla danego urządzenia.

Wymagania techniczne oraz ilość urządzeń:

I. Grupa I – 1 urządzenie Firewall UTM,
(w tym część gwarantowana 1 urządzenie Firewall UTM,
część objęta prawem opcji 0 urządzeń Firewall UTM).

- Firewall UTM musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000;
- Firewall UTM musi umożliwiać rozszerzenie dostępnych interfejsów o minimum 2 interfejsy optyczne 10GbE (SFP+);
- Możliwość utworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q;
- W zakresie Firewall-a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 48 000 nowych połączeń na sekundę;
- Firewall UTM powinien być wyposażony w lokalny dysk o pojemności minimum 100 GB SSD do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku wymagane jest dostarczenie systemu logowania i raportowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej wraz z oprogramowaniem realizującym logowanie i raportowanie do każdego urządzenia Firewall UTM;
- Wydajność systemu Firewall minimum 20 Gbps;
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2 Gbps;
- Wydajność ochrony przed atakami (IPS) minimum 11 Gbps;
- Wydajność VPN IPSec, nie mniej niż 4 Gbps.

II. Grupa II – 4 urządzenia Firewall UTM
(w tym część gwarantowana 1 urządzenie Firewall UTM,
część objęta prawem opcji maksymalnie 3 urządzenia Firewall UTM).

- Firewall UTM musi dysponować minimum 10 interfejsami miedzianymi Ethernet 10/100/1000;
- Możliwość utworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q;
- W zakresie Firewall-a obsługa nie mniej niż 500 000 jednoczesnych połączeń oraz 15 000 nowych połączeń na sekundę;

- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku wymagane jest dostarczenie systemu logowania i raportowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej wraz z oprogramowaniem realizującym logowanie i raportowanie do każdego urządzenia Firewall UTM;
- Wydajność systemu Firewall minimum 5 Gbps;
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 800 Mbps;
- Wydajność ochrony przed atakami (IPS) minimum 2.8 Gbps;
- Wydajność VPN IPSec minimum 1 Gbps.

III. Grupa III – 7 urządzeń Firewall UTM
(w tym część gwarantowana 1 urządzenie Firewall UTM,
część objęta prawem opcji maksymalnie 6 urządzeń Firewall UTM).

- Firewall UTM musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000;
- Możliwość utworzenia minimum 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q;
- W zakresie Firewall-a obsługa nie mniej niż 200 000 jednoczesnych połączeń oraz 15 000 nowych połączeń na sekundę;
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 64 GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie SD o pojemności co najmniej 64 GB do celów logowania i raportowania;
  W wypadku zastosowania dysku zewnętrznego, pendrive lub karty pamięci SD, wykonawca wraz z urządzeniem dostarczy kartę SD, pendrive lub zewnętrzny dysk o pojemności minimum 64 GB do każdego urządzenia;
- Wydajność systemu Firewall minimum 3 Gbps;
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 200 Mbps;
- Wydajność ochrony przed atakami (IPS) minimum 1.9 Gbps;
- Wydajność VPN IPSec, nie mniej niż 450 Mbps.

IV. Wymagania wspólne dla wszystkich zamawianych urządzeń, tj. urządzeń Firewall UTM z grupy I, II i III:

1) Wszystkie urządzenia muszą pochodzić z portfolio jednego producenta,
2) Wszystkie urządzenia muszą być fabrycznie nowe, nieużywane i wyprodukowane nie wcześniejszej niż w 2018 r. i musza mieć zainstalowany najnowszy na dzień podpisania umowy na dostawę firmware;
3) wykonawca zobowiązany jest do posiadania autoryzacji producenta do sprzedaży urządzeń na terenie Polski,
4) wykonawca zobowiązany jest do zapewnienia przez okres 36 miesięcy od dnia podpisania przez Strony protokołu odbioru bez zastrzeżeń ostatniego dostarczonego urządzenia polskojęzycznej obsługi posprzedażowej, serwisu gwarancyjnego

oraz wsparcia świadczonego przez 8 godzin we wszystkie dni robocze w języku polskim przez osoby certyfikowane przez producenta lub autoryzowanego przedstawiciela producenta; Za dni robocze Strony uznają dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.

5) Zamawiający nie dopuszcza ograniczenia funkcjonalności urządzeń po wygaśnięciu okresu licencji (z wyłączeniem braku pobierania aktualizacji sygnatur poszczególnych modułów systemu bezpieczeństwa). Urządzenia muszą pracować po okresie licencyjnym z pełną funkcjonalnością każdego modułu bezpieczeństwa, z sygnaturami aktualnymi na ostatni dzień obowiązywania licencji;
6) Dostarczone urządzenia muszą zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej wykonawca musi zapewnić zamawiającemu w ramach przedmiotu zamówienia niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym;
7) Urządzenia będą pracować w 12 odrębnych lokalizacjach. W każdej z lokalizacji Wykonawca musi zapewnić administratorowi lokalnemu pełną funkcjonalność dostarczonego systemu bezpieczeństwa wraz z systemem podglądu logów i raportów, bez stosowania dodatkowej np. centralnej lub chmurowej platformy zbierania logów umiejscowionej poza lokalizacją;
8) Urządzenia muszą umożliwiać pracę minimum w jednym z dwóch trybów: Router/NAT lub transparent;
9) Minimalne wymogi poszczególnych funkcji bezpieczeństwa:

    a. Kontrola dostępu:
    - zapora ogniowa klasy Stateful Inspection,
    - translacje adresów NAT adresu źródłowego i NAT adresu docelowego,
    - obsługa Policy Routingu, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP,
    - możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ, LAN

    b. Ochrona przed wirusami – antywirus (AV) – nie mniej niż:
    - analiza dla protokołów SMTP, POP3, HTTP, FTP, HTTPS,
    - system AV musi umożliwiać skanowanie AV dla plików archiwów typu: rar, zip,
    - silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021),
    - możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie AV,
    - możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP

    c. Poufność danych – obsługa IPSec VPN oraz SSL VPN – nie mniej niż:

- tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site,
- monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
- praca w topologii Hub and Spoke oraz Mesh,
- obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
- obsługa ssl vpn w trybach portal oraz tunel,
- obsługa VPN Failover,
- producent oferowanego rozwiązania VPN musi udostępniać klienta VPN współpracującego z proponowanym rozwiązaniem, dostępnego bez dodatkowych opłat

d. Ochrona przed atakami - Intrusion Prevention System oraz Intrusion Detection System (IPS/IDS) :
- ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS

e. Kontrola stron Internetowych – Web Filter (WF) – nie mniej niż:
- wbudowany filtr URL pogrupowany w kategorie tematyczne, minimum 50 kategorii tematycznych,
- możliwość dodawania własnych kategorii URL,
- brak limitu ilości dodawanych przez administratora własnych kategorii URL,
- moduł filtra URL, wspierany przez HTTP PROXY, zgodny z protokołem ICAP co najmniej w trybie REQUEST,
- możliwość zdefiniowania konkretnej akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii URL:
    a) blokowanie dostępu do adresu URL,
    b) zezwolenie na dostęp do adresu URL,
    c) blokowanie dostępu do adresu URL oraz wyświetlenie strony komunikatu HTML zdefiniowanego przez administratora,
- filtrowanie URL musi uwzględniać komunikację po protokole HTTPS,
- możliwość utworzenia tzw. białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane

f. Kontrola zawartości poczty – antyspam (AS) (dla protokołów SMTP, POP3) – nie mniej niż:
- AS działający minimum w oparciu o białe/czarne listy oraz serwery DNS RBL,
- AS musi posiadać możliwość modyfikacji listy serwerów DNS RBL,
- AS musi udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest to poczta niechciana (SPAM),
- możliwość wyboru czy poczta sklasyfikowana jako SPAM jest blokowana czy oznakowywana i dostarczana do użytkownika wraz z ustawieniem czułości filtru, np. na podstawie wartości punktowej jaką otrzyma wiadomość,
- wpis w nagłówku wiadomości zaklasyfikowanej jako spam musi być w formacie zgodnym z formatem programu Spamassassin

g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P:

- funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP

h. Analiza ruchu szyfrowanego protokołem SSL:
- inspekcja ruchu tunelowanego wewnątrz protokołu SSL co najmniej dla HTTPS, POPS, SMTPS, FTPS

i. Kontrola pasma oraz ruchu (QoS oraz Traffic shaping) – nie mniej niż:
- możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma

j. Wbudowany serwer DHCP posiadający funkcjonalność nie mniejszą niż:
- możliwość utworzenia w obrębie jednego przydzielanego zakresu IP, minimum 4 rozłącznych (nieciągłych) podzakresów (np. 10.0.0.1-10, 10.0.0.20-45, 10.0.0.55-80, 10.0.0.100-150) niezwiązanych z konkretnym MAC adresem urządzeń w sieci. Funkcjonalność dostępna odrębnie na każdym z interfejsów wewnętrznych zdefiniowanych jako LAN oraz DMZ

10) Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety);

11) Urządzenia muszą być wyposażone w mechanizm automatycznego ściągania sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL;

12) System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    k. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
    l. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
    m. Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych,
    n. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny;

13) Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów;

14) Obsługa administracyjna urządzeń:
    - urządzenia muszą posiadać wewnętrzny analizator reguł eliminujący błędy w konfiguracji,
    - urządzenia muszą mieć możliwość utworzenia minimum 5 rozłącznych profili zestawów reguł na firewall-u do szybkiej zmiany konfiguracji,
    - analiza ruchu musi udostępniać możliwość wyboru trybu pracy:
        a) pełny IPS,

b) tylko IDS,
c) lub tylko Firewall,

dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

- urządzenia muszą mieć możliwość zarządzania przez dowolną liczbę administratorów, także z nakładającymi się uprawnieniami,
- urządzenia muszą wspierać zgodność z RODO poprzez możliwość przydzielania uprawnień do przeglądania logów oraz raportów z danymi wrażliwymi (ip, hosty, użytkownicy itp.) tylko dla określonych administratorów, a fakt dostępu do tych danych musi być odnotowywany odrębnie w logach urządzenia;

15) Element oferowanego systemu bezpieczeństwa realizujący funkcjonalność Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network Firewall;

16) System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, wykonawca musi dostarczyć system logowania i raportowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej wraz z oprogramowaniem realizującym logowanie i raportowanie do każdego urządzenia Firewall UTM. Zamawiający nie dopuszcza mechanizmu wysyłania logów i raportów do chmury. System raportowania i przeglądania logów musi być dostarczony w ramach podstawowej licencji na urządzenie i nie może wymagać dodatkowych opłat w przyszłości;

17) W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
    a. Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego,
    b. Generowanie co najmniej 25 różnych typów raportów, w tym:
        - raporty typu WEB zawierające informacje o co najmniej: odwiedzanych stronach WWW, ilości połączeń do tych stron, ilości pobranych danych, kategoriach tematycznych (do których należą odwiedzane strony), użytkownikach, którzy łączyli się z danymi adresami oraz adresach IP z których wchodzono na owe strony,
        - raporty typu IPS zawierające informacje o co najmniej: wykrytych przez IPS zagrożeniach, adresach źródłowych i adresach docelowych hostów, których te zagrożenia dotyczą,
    c. Raporty muszą oferować możliwość:
        - przeszukiwania zgromadzonych informacji,
        - wyświetlenia zgromadzonych informacji, minimum dla wybranego: dnia, tygodnia, miesiąca,
        - eksportu do zewnętrznych plików obsługujących minimum format CSV,
    d. Narzędzie raportujące musi umożliwiać przeglądanie zgromadzonych logów, oraz dawać możliwość ich filtrowania po parametrach co najmniej takich jak: protokół, źródłowy adres IP, docelowy adres IP, port docelowy, nazwa docelowa, czas (od-do), nazwa użytkownika, akcja,
    e. Przeglądarka logów musi dawać możliwość ukrycia kolumn z informacjami

zbędnymi dla administratora,

18) System raportowania i przeglądania logów wbudowany w system bezpieczeństwa lub dostarczony wraz z systemem bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania;

19) Gwarancja dla wszystkich urządzeń – urządzenia muszą być przez okres 36 miesięcy od dnia podpisania przez Strony bez zastrzeżeń protokołu odbioru danego urządzenia objęte serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia przypadku jego wadliwości w terminie nie dłuższym niż 14 dni kalendarzowych, chyba że Strony wyznaczą inny termin. Na czas naprawy objętej gwarancją lub czas usuwania wady przekraczający 14 dni kalendarzowych Wykonawca zobowiązany jest w 1 dniu roboczym po upływie 14 dniowego terminu udostępnić Zamawiającemu urządzenie zastępcze tej samej lub wyższej klasy wraz z aktywną licencją modułów bezpieczeństwa. W razie niedostarczenia przez Wykonawcę urządzenia zastępczego tej samej lub wyższej klasy wraz z aktywną licencją modułów bezpieczeństwa Zamawiającemu przysługuje prawo do naliczenia kary umownej.

20) Dla wszystkich urządzeń wymagane jest dostarczenie pakietu licencyjnego, obejmującego co najmniej aktywację oraz aktualizację sygnatur następujących funkcji bezpieczeństwa: sygnatury IPS/IDS, antywirus, antyspam, filtr URL, IPSec VPN, SSL VPN, w okresie 36 miesięcy od dnia podpisania przez Strony bez zastrzeżeń protokołu odbioru.

V. Prawo opcji:

Zamawiający, korzystając z prawa opcji, zgodnie z art. 34 ust. 5 ustawy, określa maksymalną wielkość przedmiotu zamówienia jako:
a) grupa I: 1 urządzenie Firewall UTM,
b) grupa II: 4 urządzenia Firewall UTM,
c) grupa III: 7 urządzeń Firewall UTM.

Jednocześnie zamawiający określa minimalny zakres przedmiotu zamówienia (część gwarantowana) jako:
a) grupa I: 1 urządzenie Firewall UTM,
b) grupa II: 1 urządzenie Firewall UTM,
c) grupa III: 1 urządzenie Firewall UTM.

Prawem opcji objęty jest następujący zakres przedmiotu zamówienia:
a) grupa I: 0 urządzeń Firewall UTM,
b) grupa II: 3 urządzeń Firewall UTM,
c) grupa III: 6 urządzeń Firewall UTM.

Warunkiem uruchomienia prawa opcji jest złożenie przez zamawiającego pisemnego oświadczenia woli w przedmiocie i zakresie skorzystania z prawa opcji. Zamawiający nie ma obowiązku skorzystania z prawa opcji. Zamawiający ma możliwość skorzystania z prawa opcji w niepełnym zakresie. W przypadku nieskorzystania przez zamawiającego z prawa opcji lub w przypadku skorzystania z prawa opcji w niepełnym zakresie, wykonawcy nie przysługują żadne roszczenia z tego tytułu.

Zamawiający ma prawo skorzystać z prawa opcji w terminie do dnia 30 kwietnia 2019 r.

Wykonawca zobowiązany jest zrealizować prawo opcji w zakresie wskazanym przez zamawiającego w złożonym oświadczeniu o skorzystaniu z prawa opcji w terminie nie dłuższym niż 21 dni kalendarzowych liczonych od dnia złożenia przez zamawiającego oświadczenia.

Postanowienia odnoszące się do części gwarantowanej przedmiotu zamówienia znajdują odpowiednie zastosowanie do części objętej prawem opcji.

Cena jednostkowa urządzenia z danej grupy, określona w ofercie złożonej przez Wykonawcę w ramach postępowania, obowiązywać będzie zarówno w przypadku dostawy realizowanej w ramach części gwarantowanej jak i w przypadku części objętej prawem opcji.

Skorzystanie przez zamawiającego z prawa opcji uzależnione będzie od jego potrzeb i posiadania środków finansowych na zamówienie objęte prawem opcji.