Załącznik nr 7a do SWZ

Szczegółowy opis przedmiotu zamówienia dla Części I

1. Urządzenie sieciowe klasy UTM Stormshield SN720 w opcji SPARE lub równoważne – 1 szt.

Warunki równoważności dla urządzenia sieciowego UTM

Poprzez równoważność uważa się urządzenie spełniający następujące minimalne parametry oraz posiadające wymaganą funkcjonalność.

Parametry:

Przepustowość Firewall (1518 bajtów UDP)	Min. 18 Gbps
Przepustowość IPS	Min. 10 Gbps
Liczba jednoczesnych sesji	Min. 1000000
Nowe sesje na sekundę	Min. 50000
Zarządzanie przez stronę www	Tak
Serwisy podstawowe	Bez serwisów – urządzenie w trybie zapasowym z możliwością przeniesienia konfiguracji i licencji z posiadanego przez Zamawiającego urządzenia, w przypadku awarii
Interfejsy	Min. 8 x Ethernet 100/1000
Pamięć lokalna na logi	Min. wbudowany dysk 100 GB
Redundantne zasilanie	Tak

Wymagania/funkcjonalność

a) w związku z tworzeniem przez Zamawiającego środowiska Disaster Recovery, urządzenie musi umożliwiać bezpośrednie przeniesienia pełnej konfiguracji oraz licencji z posiadanego przez Zamawiającego urządzenia Stormshield SN720, za pomocą eksportu pliku konfiguracyjnego i zaimportowania go na nowe urządzenie w celu zachowania ciągłości działania w przypadku awarii. Urządzenie będzie pełnić funkcję urządzenia zapasowego,

b) w przypadku zaoferowania urządzenia równoważnego Wykonawca zobowiązany jest w ofercie udowodnić, że funkcjonalność oferowanego urządzenia jest równoważna w stosunku do urządzenia wskazanego powyżej przez Zamawiającego oraz posiada nie gorsze parametry techniczne,
c) Zamawiający informuje, że Wykonawca, który powołuje się na rozwiązania równoważne jest zobowiązany wykazać równoważność w zakresie parametrów technicznych, użytkowych, funkcjonalnych. W związku z powyższym Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenia pełnej zgodności oferowanego przedmiotu dostawy z wymogami specyfikacji. Sprawdzenie będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych u Zamawiającego. W tym celu Wykonawca na wezwanie Zamawiającego dostarczy do siedziby Zamawiającego w terminie 3 dni kalendarzowych od daty otrzymania wezwania oferowane urządzenie,
d) w przypadku zaoferowania urządzenia równoważnego, do oferty należy dołączyć kartę katalogową producenta lub dokumentacja producenta urządzenia potwierdzająca parametry oferowanego urządzenia,
e) sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2023 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”,
f) gwarancja producenta jest równa długości gwarancji urządzenia głównego posiadanego przez Zamawiającego,
g) bezpłatne zdalne wsparcie techniczne certyfikowanego inżyniera oficjalnego dystrybutora w języku polskim, przez min. okres ważności serwisu podstawowego, świadczone telefonicznie oraz drogą elektroniczną,

Obsługa sieci
a) Wsparcie dla protokołu IPv4 oraz IPv6 na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
b) Możliwość konfiguracji min. 3x. WAN.

Zapora (Firewall)

a) Firewall klasy Stateful Inspection.

b) Translacja adresów NAT n:1, NAT 1:1 oraz PAT.

c) Ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej.

d) Tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów w Interface (GUI). Określanie parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

e) Budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

f) Filtrowanie na podstawie adresów MAC.

g) Edytor reguł firewall ma wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

h) Wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

i) Budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS)

a) System detekcji i prewencji włamań (IPS) zaimplementowany w jądrze systemu, wykrywa włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

b) Moduł IPS opracowany przez producenta urządzenia.

c) Tworzenie własnych sygnatur dla systemu IPS.

d) Moduł IPS nie tylko wykrywa, ale również usuwa szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

e) Inspekcja ruchu tunelowanego wewnątrz protokołu SSL, w zakresie analizy HTTPS, POP3S oraz SMTPS.

f) Konfiguracja 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.

g) Ochronę przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

h) Automatyczna aktualizacja sygnatur kontekstowych.

Ochrona antywirusowa

a) Minimum jeden skaner antywirusowy dostarczany w ramach podstawowej licencji.

b) Określenie maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

c) Definiowanie treści komunikatu dla użytkownika o wykryciu infekcji.

Ochrona antyspam

a) Mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). Ochrona antyspam działa w oparciu o: białe/czarne listy, DNS RBL, Skaner heurystyczny.

Wirtualne sieci prywatne (vpn)

a) Tworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

b) Wspierane typy sieci VPN: IPSec VPN, SSL VPN.

Filtr dostępu do stron WWW

a) Wbudowany filtr URL.

b) Filtr URL działający w oparciu o klasyfikację URL stron internetowych.

c) Dodawanie własnych kategorii URL.

d) Definiowanie akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru:
blokowanie dostępu do adresu URL,
zezwolenie na dostęp do adresu URL,
blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

e) Filtr URL uwzględnia komunikację po protokole HTTPS.

f) Tworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

Uwierzytelnianie

a) W oparciu o lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory.

Administracja łączami do internetu (ISP)

a) Wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

b) Przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

c) Monitorowanie dostępności łącza w oparciu o ICMP oraz TCP.

Administracja urządzeniem

a) Konfiguracja urządzenia z wykorzystaniem polskiego interfejsu graficznego.

b) Interfejs konfiguracyjny dostępny poprzez przeglądarkę internetową, a komunikacja poprzez zaszyfrowany protokół HTTPS.

c) Wskazanie do komunikacji innego portu niż 443 TCP.

d) Zarządzanie z poziomu konsoli (SSH)

e) Możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania.

f) Wbudowany webowy, graficzny interfejs administracyjny urządzenia oferuje narzędzia diagnostyczne ping, traceroute, nslookup.

g) Wbudowany webowy, graficzny interfejs administracyjny zawiera narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

h) Wbudowany webowy, graficzny interfejs administracyjny zawiera zdefiniowane polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

i) Definiowanie własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

j) Eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

k) Eksportowanie backupu konfiguracji (kopia zapasowa) w zakresie manualnego eksportu do pliku w dowolnym momencie czasu.

l) Anonimizacja logów w zakresie adresu źródłowego oraz nazwy użytkownika.

m) Ręczna aktualizacja baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

a) Wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

b) Wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

c) Predefiniowane raporty dla ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

d) Eksport wyników raportu do formatu CSV.

e) Monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Usługi i funkcje

a) Wbudowany DHCP z dynamicznym jak i statycznym przypisywaniem adresu IP do adresu MAC karty sieciowej.

b) Przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

c) Tworzenie różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).

d) Usługa DNS Proxy.

Dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware).

2. Licencje na usługi do posiadanego przez Zamawiającego urządzenia UTM Stormshield SN720

a) Licencja 1 - Premium UTM Security Pack - licencja na 2 lata, migracja z UTM Security Pack – 1 szt.,

b) Licencja 2 - Sandboxing Breach Fighter - licencja na 2 lata – 1 szt.

Licencje muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta.