Parametry dodatkowo punktowane

1. Urządzenie koncentrator HUB VPN

- Urządzenie jest produktem o uznanej na rynku pozycji co oznacza, że zostało wyprodukowane przez producenta występującego w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej ostatnie 3 (trzy) lata z rzędu.
- System zabezpieczeń firewall zapewni wewnętrzne wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym.
- System zabezpieczeń firewall pozwala na definiowanie i przydzielanie różnych profili ochrony (anty-malware, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
- System zabezpieczeń firewall zapewni inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
- System zabezpieczeń firewall posiada możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie takiej samej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.
- System zabezpieczeń firewall umożliwia inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
- System zabezpieczeń firewall zapewni integrację z MS Exchange,
- System zabezpieczeń firewall posiada możliwość przekierowania ruchu (PBR - policy base routing) dla wybranych aplikacji i konkretnych użytkowników z pominięciem tablicy routingu.
- System zabezpieczeń firewall posiada możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Przywrócenie jednej z poprzednich wersji konfiguracji jako konfiguracji aktywnej nie może powodować konieczności restartu urządzenia.
- System zabezpieczeń firewall automatycznie weryfikuje spójność konfiguracji polityk bezpieczeństwa z punku widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki.

2. Urządzenie firewall do jednostek oświatowych

- Urządzenie jest produktem o uznanej na rynku pozycji co oznacza, że zostało wyprodukowane przez producenta występującego w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej ostatnie 3 (trzy) lata z rzędu.

- System zabezpieczeń firewall zapewni wewnętrzne wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym.

- System zabezpieczeń firewall pozwala na definiowanie i przydzielanie różnych profili ochrony (anty-malware, IPS, URL, blokowanie plików) per aplikacja. System zapewni możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

- System zabezpieczeń firewall zapewni inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

- System zabezpieczeń firewall posiada możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. System umożliwi wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie takiej samej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.

- System zabezpieczeń firewall umożliwia inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

- System zabezpieczeń firewall zapewnia integrację z MS Exchange,

- System zabezpieczeń firewall posiada możliwość przekierowania ruchu (PBR - policy base routing) dla wybranych aplikacji i konkretnych użytkowników z pominięciem tablicy routingu.

- System zabezpieczeń firewall posiada możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Przywrócenie jednej z poprzednich wersji konfiguracji jako konfiguracji aktywnej nie może powodować konieczności restartu urządzenia.

- System zabezpieczeń firewall automatycznie weryfikuje spójność konfiguracji polityk bezpieczeństwa z punku widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki.

3. System zarządzania

- System zarządzania, logowania i raportowania umożliwia odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.

- System zarządzania, logowania i raportowania umożliwia tworzenie kopii zapasowych zarządzanych firewalli.

• System zarządzania, logowania i raportowania pozwala na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu konsoli zarządzającej. • System zarządzania umożliwia zarządzanie w zakresie opisanym w punktach powyżej posiadanymi przez Zamawiającego urządzeniami PaloAlto Networks model 5250 (2 szt.)	
Potwierdzam spełnienie wszystkich parametrów dodatkowo punktowanych	**TAK / NIE***

** - niewłaściwe skreślić*

.....
podpis osoby / osób upoważnionych do
występowania w imieniu wykonawcy

Wykaz zaoferowanych urządzeń

Typ urządzenia	**Dokładna specyfikacja producenta (producent, typ, model, part numer), jeżeli urządzenie wyposażone jest w dodatkowe elementy/opcje oferowane przez producenta oddzielnie należy podać wszystkie informacje także dla tych elementów/opcji łącznie z podaniem ilości tych elementów/opcji wchodzących w skład jednego urządzenia. Podane informacje muszą w sposób jednoznaczny wskazywać na urządzenie/element/opcję w katalogu producenta.**
Koncentrator HUB VPN	
Firewall do jednostek oświatowych	
System zarządzania	

.....
podpis osoby / osób upoważnionych do
występowania w imieniu wykonawcy