

Opis przedmiotu zamówienia

Kod CPV:

32420000-3 - Urządzenia sieciowe

Przedmiotem zamówienia jest dostawa do siedziby Zamawiającego dwóch (2) wielofunkcyjnych zapór sieciowych (UTM). O terminie dostawy Wykonawca zobowiązany jest poinformować Zamawiającego z co najmniej 3 dniowym wyprzedzeniem.

Każde oferowane przez Wykonawcę urządzenie musi spełniać wszystkie graniczne parametry podane przez poniżej. Przedmiot zamówienia musi spełniać wymagane polskim i europejskim prawem wszelkie normy, posiadać dokumenty dopuszczające do obrotu na terenie Rzeczypospolitej Polskiej oraz niezbędne świadectwa, certyfikaty, atesty, w tym deklaracje zgodności CE.

1. Wymagania ogólne w zakresie dostawy sprzętu

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty powystawowe, demonstracyjne, prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230 V.
6. Urządzenia muszą współpracować z systemem zabezpieczeń sieci wewnętrznej wykorzystywanym przez Zamawiającego.
7. Miejsce dostawy: Dolnośląskie Centrum Rehabilitacji i Ortopedii Sp. z o.o., ul. J. Korczaka 1, 58-400 Kamienna Góra, serwerownia w Pawilonie 1A.
8. Urządzenia zostaną dostarczone w dniach roboczych Zamawiającego, tj. od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, w godzinach 8:00 ÷ 12:00.
9. Wdrożenie urządzenia przez Wykonawcę na miejscu wraz z konfiguracją urządzenia.

2. Graniczne parametry techniczne i funkcjonalne dla dostarczanych urządzeń:

1. Elementy systemu bezpieczeństwa:
 - a. Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu.
 - b. Możliwość stworzenia minimum 128 wirtualnych interfejsów, zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
 - c. W zakresie Firewall - obsługa nie mniej niż 2 000 000 jednoczesnych połączeń i min. 140 000 nowych połączeń na sekundę.
 - d. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
 - e. Możliwość rozszerzenia pamięci do 1,92 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia.
 - f. Musi posiadać 2 x USB 3.0 z przodu urządzenia oraz 1 Consola Port – również z przodu.
 - g. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
 - h. System musi mieć możliwość włączenia min. 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości.

- i. Systemy wirtualne muszą obsługiwać QOS.
 - j. System pełniący funkcję zapory musi posiadać nie mniej niż: 2 x SFP+, 8 x SFP, 16 x GE (w tym co najmniej jedną parę bypass) interfejsów.
 - k. Urządzenie musi posiadać co najmniej jeden dedykowany port przeznaczony do zarządzania urządzeniem RJ45.
 - l. Urządzenie musi posiadać co najmniej jeden dedykowany port HA.
 - m. Dostarczone urządzenia muszą mieć możliwość pracy w trybie Active-Passive oraz Active-Active.
 - n. Urządzenia muszą ściśle współpracować z systemami bezpieczeństwa posiadanymi przez Zamawiającego, w szczególności z systemem NDR firmy HillStone (HillStone BDS). System NDR musi mieć bezpośrednią możliwość wykonywania komend na dostarczonym systemie Firewall, takich jak: blokada portów, blokada adresów źródłowych, blokada adresów docelowych lub dowolna kombinacja wcześniejszych opcji. Jeśli nie ma takiej możliwości, Wykonawca zobowiązany jest do dostarczenia komercyjnego systemu pośredniczącego w komunikacji pomiędzy urządzeniem NDR a urządzeniem Firewall.
2. Funkcjonalności:
- a. Kontrola dostępu — zaporą sieciową Stateful Inspection.
 - b. Ochrona przed wirusami - komercyjny antywirus [AV].
 - c. Poufność danych - IPSec VPN i SSL VPN.
 - d. Kontrola witryn sieci Web — filtr URL.
 - e. Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3).
 - f. Kontrola przepustowości i ruchu (QoS i kształtowanie ruchu) z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN.
 - g. Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji.
 - h. Reputacja IP.
 - i. Cloud Sandbox.
3. Wydajność:
- a. Analiza ruchu szyfrowanego protokołem SSL.
 - b. Wydajność Firewall co najmniej 20 Gb/s.
 - c. Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji > 5,4 Gb/s.
 - d. Wydajność ochrony przed atakami (IPS) minimum 10 Gb/s.
 - e. Wydajność AV > 4,8 Gb/s.
 - f. Inspekcja SSL Proxy > 900 Mb/s.
 - g. Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 3 Gb/s.
4. Funkcjonalności VPN:
- a. Wydajność IPSec VPN, nie mniej niż 6 Gb/s.
 - b. Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja.
 - c. Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
 - d. Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności.
 - e. Praca w topologiach Hub and Spoke i Mesh.
 - f. Wspierane mechanizmy: IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec.
 - g. Wsparcie grup DH dla IKEv1: 1, 2, 5, 19, 20, 21, 24.
 - h. Wsparcie grup DH dla IKEv2: 1, 2, 5, 14, 15, 16, 19, 20, 21, 24.
 - i. Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance).
 - j. Obsługa PnPVPN (Plug and Play VPN).
5. Routing:
- a. Rozwiązanie musi zapewniać obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS.

- b. Obsługa Policy Based Routing.
 - c. Funkcjonalność Virtual Wire.
6. Translacja adresów NAT:
- a. Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
 - b. Obsługa NAT46, NAT64, DNS64.
 - c. Wsparcie dla STUN.
7. Polityka bezpieczeństwa systemu:
- a. Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
 - b. Możliwość budowania > 19000 polityk.
 - c. Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego.
 - d. Musi być w stanie skonfigurować agregowane polityki.
 - e. Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P).
8. Wydzielenie stref bezpieczeństwa:
- a. Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN.
 - b. Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów.
 - c. Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników.
9. Ochrona antywirusowa:
- a. Silnik antywirusowy musi być oparty na przepływie tzw. flow-based.
 - b. Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB.
 - c. Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV.
 - d. Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji.
10. Równoważenie obciążenia:
- a. Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania.
 - b. Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin.
 - c. Kontrola stanu serwera, monitorowanie sesji i ochrona sesji.
11. Ochrona IPS:
- a. Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
 - b. Baza danych wykrytych ataków musi zawierać co najmniej 15000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
 - c. Funkcjonalność zapobiegania atakom SQL injection, XSS injection.
 - d. Możliwość budowania własnych niestandardowych reguł IPS.
12. Obrona przed atakiem:
- a. Ochrona przed nieprawidłowym działaniem protokołu.
 - b. Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
 - c. Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood.
 - d. Biała lista docelowych adresów IP.
13. Ochrona antyspam:
- a. Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym.
 - b. Wspieranymi protokołami muszą być minimum SMTP, SMTPS, POP3, POP3S.
 - c. Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach.
 - d. Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen.

14. Kontrola aplikacji:
 - a. Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP.
 - b. Baza danych aplikacji zawierająca ponad 6000 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka.
15. Filtr adresów URL:
 - a. Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
 - b. Możliwość zdefiniowania własnej bazy kategorii www.
 - c. Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
 - d. Kategoria takie jak hazard, malware, spam, botnety.
 - e. Obsługa Safe Search.
 - f. Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne.
 - g. Dostosowanie strony ostrzeżenia.
16. Ochrona danych:
 - a. Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy.
 - b. Identyfikacja protokołu transferu pliku, w tym HTTP,FTP, SMTP, POP3, IMAP.
 - c. Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS.
 - d. Filtrowanie plików przesyłanych przez SMB 1 i 2.
17. Reputacja IP:
 - a. Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamery, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force.
 - b. Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP.
18. Zapobieganie botnetom:
 - a. Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware.
 - b. Wsparcie DNS sinkhole.
 - c. Wsparcie wykrywania tunelowania DNS.
 - d. Wyrwanie i blokowanie DGA.
19. Cloud Sandbox:
 - a. Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanymi zagrożeń.
 - b. Obsługa protokołów takich jak: HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB.
 - c. Obsługa typów plików: PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów.
 - d. Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanymi zagrożeń.
20. Uwierzytelnianie użytkownika:
 - a. System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:
 - i. Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu,
 - ii. Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP,
 - iii. Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych,
 - iv. Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA.
 - b. W przyszłości pozwala na umożliwienie budowy architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory.
 - c. Wsparcie usług terminalowych.
 - d. Uwierzytelnianie użytkownika przez Web przed dostępem do Internetu.
 - e. System musi obsługiwać dwuskładnikowe uwierzytelnianie, SMSy, certyfikaty i tokeny.

21. Raportowanie i przeglądanie logów:
 - a. Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie.
 - b. W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
 - i. Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego,
 - ii. Generowanie co najmniej 10 rodzajów raportów.
22. System logowania:
 - a. Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.
23. Certyfikaty - rozwiązanie musi:
 - a. Posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall.
 - b. Być pozycjonowanym w Raporcie Gartnera (www.gartner.com) w każdym roku w okresie 2015÷2022.
24. Zarządzanie:
 - a. Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
 - b. Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola.
25. Gwarancja:
 - a. Co najmniej 12-miesięczna gwarancja producenta na dostarczone elementy systemu.
 - b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 12 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C).
 - c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim.
 - d. Oferta musi być złożona przez autoryzowanego partnera producenta urządzenia.