**Załącznik Nr.1 Szczegółowy opis przedmiotu zamówienia pn. „Zakup i dostawa urządzenia klasy UTM (wielofunkcyjna zapora sieciowa) wraz ze wsparciem technicznym, licencją, aktualizacjami, wdrożeniem i szkoleniem”.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka** |
| Elementy systemu bezpieczeństwa | * Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most ) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu * System pełniący funkcję zapory musi mieć co najmniej 8 interfejsów Ethernet 10/100/1000 * Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q. * W zakresie Firewall, obsługa nie mniej niż 1 000 000 jednoczesnych połączeń i 48 000 nowych połączeń na sekundę. * System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania. * Możliwość rozszerzenia pamięci do 1,92 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia * Musi posiadać 2x USB 3.0 z przodu urządzenia * System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu. * System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do 5 poprzez dodatkową licencję w przyszłości * Systemy wirtualne muszą obsługiwać QOS |
| Funkcjonalności | * Kontrola dostępu — zapora sieciowa Stateful Inspection * Ochrona przed wirusami - komercyjny antywirus [AV] * Poufność danych - IPSec VPN i SSL VPN * Kontrola witryn sieci Web — filtr URL * Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3) * 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 * Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji * Reputacja IP * Cloud Sandbox |
| Wydajność | * Analiza ruchu szyfrowanego protokołem SSL * Wydajność Firewall co najmniej 5 Gb/s * Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 1,2 Gb/s * Wydajność ochrony przed atakami (IPS) minimum 3.2 Gb/s * Wydajność AV nie mniej niż 2Gb/s |
| Funkcjonalności VPN | * Wydajność IPSec VPN, nie mniej niż 2 Gb/s * Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja * Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem. * Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności * Praca w toplogiach Hub and Spoke i Mesh * Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec, * Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24 * Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24 * Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) * Obsługa PnPVPN (Plug and Play VPN) |
| Routing | * Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS * Obsługa Policy Based Routing * Funkcjonalność Virtual Wire |
| Translacja adresów NAT | * Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego. * Obsługa NAT46, NAT64, DNS64 * Wsparcie dla STUN |
| Polityka bezpieczeństwa systemu | * 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). * Możliwość budowania min. 8000 poliyk * Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego * Musi być w stanie skonfigurować agregowane polityki * Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P) |
| Wydzielenie stref bezpieczeństwa | * Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN * Musi mieć możliwosc konfiguracji oddzielnych wirtualnych routerów * Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników |
| Ochrona antywirusowa | * Silnik antywirusowy musi by ć oparty na przepływie tzw. flow-based * Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB * Możliwosc ręcznego dodawania lub usuwania sygantury MD5 do bazy danych AV * 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 |
| Rownoważenie obciążenia | * Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania * Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin * Kontrola stanu serwera, monitorowanie sesji i ochrona sesji |
| Ochrona IPS | * Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. * Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos. * Funkcjonalnosc zapobiegania atakom SQL injection, XSS injection * Możliwość budowania własnych niestandardowych reguł IPS |
| Obrona przed atakiem | * Ochrona przed nieprawidłowym działaniem protokołu * Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp. * Wsparcie IPv4 jak i IPv6 dla o chrony przed DNS query flood i DNS reply flood * Biała listę docelowych adresów IP |
| Kontrola aplikacji | * Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP. * Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka |
| Filtr adresów URL | * Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków. * Możliwość zdefiniowania własnej bazy kategorii www. * Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL. * Kategoria takie jak hazard, malware, spam, botnety * Obsługa Safe Search * Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne * Dostosowanie strony ostrzeżenia |
| Ochrona danych | * Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy * Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP * Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS * Filtrowanie plików przesyłanych przez SMB |
| Reputacja IP | * Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force * Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP |
| Zapobieganie botnetom | * Wykrywanie intranetowych hostó botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware * Wsparcie DNS sinkhole * Wsparcie wykrywania tunelowania DNS * Wyrywanie i blokowanie DGA |
| Cloud Sandbox | * Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w ceu wykrywania nieznanych zagrożeń * Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB * Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów * Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń. |
| Uwierzytelnianie użytkownika | * System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:   + Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu   + Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP   + Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych   + Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA * Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory * Wsparcie usług terminalowych * Uwierzytelnianie użytkownika przez Web przed dotępem do internetu * Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny |
| Raportowanie i przeglądanie logów | * Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie * W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:   + Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego   + Generowanie co najmniej 10 rodzajów raportów |
| System logowania | * 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. |
| Certyfikaty | Rozwiązanie musi:   * posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall * być pozycjonowanym w raporcie Gartnera przez ostatnie 7 lat |
| Zarządzanie | * 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. * Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola |
| Gwarancja | Dostawa musi zawierać również:   * Minimalną 12-miesięczną gwarancję producenta na dostarczone elementy systemu * Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 12 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C) * Wsparcie techniczne dystrybutora rozwiązań * Wdrożenie dostarczonego rozwiązania. * Szkolenie dla Administratora z konfiguracji oferowanego rozwiązania |