

Dostawa urządzenia klasy IPS wraz z oprogramowaniem (1 szt.).

Przedmiotem zamówienia jest dostawa urządzenia typu IPS (Intrusion Prevention System) inteligentnego systemu wykrywania i zapobiegania włamaniom, zwiększające bezpieczeństwo sieci w czasie rzeczywistym, wraz z oprogramowaniem (licencją enterprise).

Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa
 - a. Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U.
 - b. Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB.
 - c. Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli
 - d. Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem
 - e. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet.
 - f. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP.
 - g. System musi posiadać przynajmniej dwie pary portów typu bypass
 - h. Proponowane rozwiązanie musi posiadać co najmniej 480GB przestrzeni dyskowej.
 - i. Proponowane rozwiązanie musi obsługiwać przepustowość IPS 2 Gb/s
 - j. Proponowane rozwiązanie musi obsługiwać jednocześnie sesje o długości 1.2 M
 - k. Proponowane rozwiązanie musi obsługiwać min 30000 nowych sesji/sekundę w ruchu TCP.
 - l. Opóźnienia (tzw. Latency) nie mogą przekraczać 300µs
 - m. Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW
2. Usługi sieciowe
 - a. Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu)
3. Kontrola Aplikacji
 - a. Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów , czasu online, czasu offline.
 - b. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka.
 - c. Rozwiązanie powinno rozpoznawać aplikacje IPv6.
 - d. Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL
 - e. Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS.
 - f. Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie ruchu dla aplikacji.
 - g. Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze
4. Ochrona przez zagrożeniami
 - a. Rozwiązanie musi obsługiwać ponad 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń.
 - b. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL.

- c. Rozwiązanie musi obsługiwać ochronę środowiska IPV6.
 - d. Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS.
 - e. Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych.
 - f. Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
 - g. Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu.
 - h. Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia
 - i. Rozwiązanie musi obsługiwać opcję logowania pakietów.
 - j. Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu.
 - k. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp.
 - l. Rozwiązanie musi być wspierać weryfikację protokołów http typu Get, Head, Put, Post.
 - m. Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS.
 - n. Rozwiązanie musi obsługiwać tryb działania sniffera IDS.
 - o. Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS.
 - p. Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS.
 - q. Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP.
 - r. Proponowane rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS.
 - s. Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6
 - t. Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków
 - u. Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet
 - v. Obsługa inspekcji Reverse Shell
 - w. Ochrona i wykrywanie skanowania protokołów IP oraz UDP
 - x. Rozwiązanie musi mieć możliwość inspekcji payloadu w ramach MPLS
 - y. Rozwiązanie pozwala na automatyczne określanie wartości proponowanych dla ochrony przed atakami Flood
 - z. System pozwala na zdefiniowanie globalnej białej listy, pozwalając na dany ruch i nie sprawdzając go na warstwie aplikacyjnej
 - aa. System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK
5. Monitoring
- a. Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym nazwę ataku, ważność, czasem, adresem, protokołem, zalecanym rozwiązaniem itp.
 - b. Rozwiązanie musi obsługiwać usługę Threat Intelligence Pushing Service
 - c. Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym.
 - d. Rozwiązanie powinno obsługiwać monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania itp.
6. Polityki bezpieczeństwa
- a. Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS w jednej regule polityki.
 - b. Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty

- c. Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI
 - d. Rozwiązanie musi obsługiwać import i eksport polityk
7. Administrowanie, logi i raportowanie
- a. Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI)
 - b. Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę
 - c. Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS
 - d. Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog.
 - e. Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora
 - f. Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło
 - g. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
 - h. Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP.
 - i. Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych.
 - j. Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania
 - k. Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu.
 - l. Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety
 - m. Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi
 - n. Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP.
 - o. Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas.
 - p. Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania.
 - q. Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export
 - r. Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów
 - s. Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog.
 - t. Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach
 - u. Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195)
 - v. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika.
 - w. Rozwiązanie musi obsługiwać zaplanowany raport.
 - x. Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP.
 - y. Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF.
8. Wysoka dostępność
- a. Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive
 - b. Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:
 - HA z agregacją linków
 - Full mesh HA

- Geograficznie rozproszony HA
 - c. Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA
9. Gwarancja – Dostawa musi zawierać również
- a. 24-miesięczną gwarancję producenta na dostarczone elementy systemu
 - b. Licencje na funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, App control)
 - c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
 - d. Gwarancja musi być zapewniona przez autoryzowanego partnera