**Załącznik 4 Wymagania na dostawę zabezpieczenia styku z Internetem**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa urządzeń zabezpieczających styk z internetem do siedziby Zamawiającego, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.

Wymaga się dostarczenia, instalacji, skonfigurowania i uruchomienia **dwóch** urządzeń typu NGFW, pracujących, jako klaster w trybie Active/Passive.

Podane poniżej wymagania odnoszą się do pojedynczego urządzenia pracującego w klastrze.

**Wymagane minimalne parametry techniczne:**

|  |  |
| --- | --- |
| **L.p.** | **Nazwa parametru** |
|  | Zapora sieciowa typu Next Generation Firewall. |
|  | Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. |
|  | Mechanizm pozwalający na dwustronną analizę ruchu bez ograniczeń na rozmiar skanowanego pliku oraz rodzaj protokołu. |
|  | Rozwiązanie musi być zbudowane w oparciu o dedykowaną platformę sprzętową. |
|  | Minimalna ilość interfejsów:   1. 7 interfejsów 1 GbE 2. 1 interfejs USB do podłączenia modemu 3G/4G 3. 1 interfejs konsoli |
|  | Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa. |
|  | Możliwość utworzenia przynajmniej 50 interfejsów VLAN, w oparciu o standard 802.1q |
|  | Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej |
|  | Minimalna ilość jednocześnie obsługiwanych sesji: 90 000 |
|  | Możliwość obsłużenia przynajmniej 6000 nowych sesji w ciągu 1 sekundy. |
|  | Przepustowość urządzenia pracującego w trybie stateful firewall (SPI): 1.3 Gbps – dla ramki 1518B zgodnie z RFC 2544 |
|  | Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 900 Mbps |
|  | Przepustowość urządzenia pracującego jako koncentrator VPN:900 Mbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544 |
|  | Przepustowość urządzenia DPI (NGFW) - z włączonymi wszystkimi usługami bezpieczeństwa (antywirus, antyspyware, IPS, kontrola aplikacji) – 300 Mbps |
|  | Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 20 |
|  | Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec (komputer – urządzenie), dostarczonych z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 25. |
|  | Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP |
|  | Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site) |
|  | Funkcjonalność IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa) oraz DNS Proxy |
|  | Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP |
|  | Wsparcie dla Dynamicznego DNS tzw. DDNS |
|  | Zintegrowany mechanizm kontroli zawartości witryn (Content Filtering) |
|  | Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony, na które użytkownik wchodzi bezpośrednio). |
|  | Administrator powinien mieć możliwość tworzenia różnych akcji, dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:   1. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron) 2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony 3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. |
|  | Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps |
|  | Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. Inspekcja ruchu powinna być możliwa nie tylko na porcie 443. System powinien umożliwiać również inspekcję oraz deszyfrację ruchu SSH. |
|  | Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL |
|  | Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. Niezależnie urządzenie powinno wspierać routing ECMP (Equal Cost Multi Path). |
|  | Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN) |
|  | Kontrola dostępności zestawionych tuneli VPN |
|  | Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. |
|  | Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do internetu powinna być tworzona według reguł opartych o grupy i obiekty |
|  | Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić) |
|  | Funkcja NAT oparta o reguły bezpieczeństwa |
|  | NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe) |
|  | Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap, oraz wszystkich innych niezdefiniowanych. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych |
|  | Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer (możliwość filtrowania usług typu Kaaza, Emule itp.), buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach http |
|  | System IPS musi używać algorytmu szeregowego przetwarzania |
|  | Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). |
|  | System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. |
|  | Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między wewnętrznymi strefami bezpieczeństwa |
|  | Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji :   1. Bazy w/w systemów muszą być aktualizowane, co najmniej raz dziennie. 2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur 3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. |
|  | Możliwość kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi. |
|  | Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pracującymi w standardzie 802.11ac wave1 oraz wave2 |
|  | Wbudowany kontroler powinien umożliwiać podłączenie i obsługę 96 punktów dostępowych sieci bezprzewodowej pochodzących od tego samego producenta. |
|  | Licencja obejmująca funkcjonalności:   1. Antywirus (Gateway Anti-Wirus), 2. Anti-Spyware, 3. IPS (Intrusion Prevention and Application Intelligence and Control Service), 4. Kontrola Treści (Content Filtering) |
|  | Aktualizacja sygnatur antwirus, antyspyware, IPS, kontrola treści przez okres 3 lat, |
|  | Gwarancja oraz zapewnienie wsparcia technicznego w trybie 24x7 na okres 3 lat. |