Załącznik nr 2

Wymagania ogólne

W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta.

System bezpieczeństwa (UTM) - 2 sztuki

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie usług dostarczanych od dostawcy łącza internetowego.

|  |  |
| --- | --- |
| Wymagania minimalne | Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.) |
| Należy podać producenta i oferowany model |  |
| System realizujący funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |  |
| System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. |  |
| System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego
 |  |
| Redundancja, monitoring i wykrywanie awarii |
| W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewnić funkcję synchronizacji sesji. |  |
| System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| System musi umożliwić monitoring stanu realizowanych połączeń VPN. |  |
| System musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| Interfejsy, Dysk, Zasilanie |
| System musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:• 10 portów Gigabit Ethernet RJ-45. |  |
| System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie |  |
| modemu 4G/5G oraz instalacji oprogramowania z klucza USB. |  |
| System realizujący funkcję firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności 128 GB. |  |
| System musi umożliwić skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. |  |
| System musi być wyposażony w zasilanie AC wraz z zasilaczem. |  |
| Parametry wydajnościowe |
| W zakresie Firewall'a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. |  |
| Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. |  |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. |  |
| Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. |  |
| Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix -1.3 Gbps. |  |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - 650 Mbps. |  |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - 600 Mbps. |  |
| Funkcje Systemu Bezpieczeństwa |
| W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje: |
| Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |  |
| Kontrola Aplikacji. |  |
| Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |  |
| Ochrona przed malware. |  |
| Ochrona przed atakami - Intrusion Prevention System. |  |
| Kontrola dostępu do stron WWW. |  |
| Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3. |  |
| Zarządzanie pasmem (QoS, Traffic shaping). |  |
| Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |  |
| Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPIM typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla |  |
| tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN. |  |
| Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. |  |
| Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |  |
| Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |  |
| Polityki, Firewall |
| W ramach polityk i firewalla muszą być realizowane wszystkie poniższe funkcje: |
| Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |  |
| System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
 |  |
| W ramach systemu możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  |
| System wykorzystuje w politykach bezpieczeństwa zewnętrzne repozytoria zawierających: kategorie URL, adresy IP. |  |
| Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. |  |
| System posiada możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. |  |
| Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.* Amazon Web Services (AWS).
* Microsoft Azure.

® Cisco ACI.* Google Cloud Platform (GCP).

® OpenStack.* VMware NSX.
 |  |
| Połączenia VPN |
| W ramach połączeń VPN muszą być realizowane wszystkie poniższe funkcje: |
| System umożliwia konfigurację połączeń typu IPSec VPN.W zakresie tej funkcji musi zapewnić:* Wsparcie dla IKE vl oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to- Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling" dla połączeń Client-to- Site.
 |  |
| System umożliwia konfigurację połączeń typu SSL VPN.W zakresie tej funkcji musi zapewnić:* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
 |  |
| • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  |
| Routing i obsługa łączy WAN |
| W zakresie routingu rozwiązanie musi zapewnić obsługę: |
| Routingu statycznego. |  |
| Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). |  |
| Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. |  |
| Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. |  |
| ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu. |  |
| BFD (Bidirectional Forwarding Detection). |  |
| Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |
| Funkcje SD-WAN |
| System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. |  |
| SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |
| Zarządzanie pasmem |
| System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |  |
| System daje możliwość określania pasma dla poszczególnych aplikacji. |  |
| System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. |  |
| System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| Ochrona przed malware |
| W ramach systemu ochrony przez malware muszą być realizowane wszystkie poniższe funkcje: |
| Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |  |
| Silnik antywirusowy zapewnia skanowanie następujących protokołów: FłTTP, FITTPS, FTP, POP3, IMAP, SMTP, CIFS. |  |
| System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów |  |
| zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. |  |
| System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. |  |
| System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego). |  |
| Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. |  |
| System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| Możliwość wykorzystania silnika sztucznej inteligencji Al wytrenowanego przez laboratoria producenta. |  |
| Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |
| Ochrona przed atakami |
| W ramach systemu ochrony przed atakami muszą być realizowane wszystkie poniższe funkcje: |
| Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |  |
| System chroni przed atakami na aplikacje pracujące na niestandardowych portach. |  |
| Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. |  |
| System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |  |
| System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. |  |
| Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). |  |
| Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. |  |
| Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |
| Kontrola aplikacji |
| W ramach kontroli aplikacji muszą być realizowane wszystkie poniższe funkcje: |
| Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |  |
| Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |  |
| Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |  |
| Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). |  |
| System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |  |
| Kontrola WWW |
| W ramach kontroli WWW muszą być realizowane wszystkie poniższe funkcje: |
| Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |  |
| W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamie DNS, proxy. |  |
| Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. |  |
| Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL. |  |
| Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). |  |
| Filtr WWW daje możliwość wykonania akcji typu „Warning" - ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. |  |
| Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. |  |
| Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. |  |
| System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |
| Uwierzytelnianie użytkowników w ramach sesji |
| W ramach uwierzytelnianie użytkowników w ramach sesji muszą być realizowane poniższe funkcje: |
| System Firewall umożliwia weryfikację tożsamościużytkowników za pomocą:* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurlD) w oparciu o zewnętrzne bazy danych.
 |  |
| System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. |  |
| System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. |  |
| Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
| Zarządzanie |
| W ramach systemu zarządzania muszą być realizowane wszystkie poniższe funkcje: |
| Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. |  |
| Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |  |
| System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. |  |
| System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |  |
| Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |  |
| Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). |  |
| Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |  |
| Logowanie |
| W ramach systemu logowania muszą być realizowane wszystkie poniższe funkcje: |
| Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |  |
| W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |  |
| Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. |  |
| Możliwość włączenia / wyłączenia logowania per reguła w polityce firewall. |  |
| System zapewnia możliwość logowania do serwera SYSLOG. |  |
| Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |
| Testy wydajnościowe oraz funkcjonalne |
| Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy wydajnościowe. |  |
| Serwisy i licencje |
| Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy. |  |
| Gwarancja oraz wsparcie |
| Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware |  |
| replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
| Rozszerzone wsparcie serwisowe AHB/SOS |
| System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres co najmniej 60 miesięcy. |  |
| Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina - reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. |  |
| Wymagania powinny być potwierdzone dokumentami:* Oświadczanie wykonawcy lub producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) dołączyć do oferty.
* Certyfikat ISO 9001 lub równoważny podmiotu serwisującego należy załączyć do oferty.
 |  |
| Technologia podwójnego zastosowania |
| W przypadku zaistnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania Wykonawca składa niezbędne oświadczenie. |  |
| Należy dołączyć do oferty dokument - oświadczenie wykonawcy lub producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferowane produkty pochodzą z autoryzowanego kanału sprzedaży. |  |