Załącznik nr 16 do OPZ - Router typ B

# Specyfikacja urządzenia bezpieczeństwa i transmisji danych – Router typ B

## Obudowa i zasilanie

### Redundantne zasilanie 230 V 50 Hz.

### Montaż w stelażu/szafie RACK 19”.

### Wysokość maksymalna pojedynczego urządzenia 2U.

### **Wymagania Ogólne**

### Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

### System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

### System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

### Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

### Monitoring stanu realizowanych połączeń VPN.

### System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

### System musi zostać dostarczony w postaci redundantnej tj. dwa komplety, przy czym jeden komplet to są dwa urządzenia (razem 4 urządzenia).

### **Interfejsy, dyski:**

### System realizujący funkcję Firewall musi dysponować minimum 12 portami Gigabit Ethernet RJ-45, 8 gniazdami SFP oraz 4 portami 10 Gigabit Ethernet z gniazdami SFP+.

### System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

### W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

### System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 400 GB.

## Oprócz modułów i kabli potrzebnych do redundantnego podłączenia dostarczanych w niniejszym postepowaniu urządzeń każdy firawall należy wyposażyć w niżej wymienione moduły i kable potrzebne do dołączenia do infrastruktury podmiotu medycznego i operatora:

## jeden moduł SFP wielomodowy

## jeden moduł SFP jednomodowy

## dwa moduły SFP+ jednomodowe

## dwa patchcordy kategorii 6 UTP o długości 2 m

## dwa patchcordy kategorii 6 UTP o długości 5 m

## jeden patchcord duplex wielomodowy o długości 5 m ze złączami LC-LC

## jeden patchcord duplex jednomodowy o długości 5 m ze złączami LC-LC

### **Parametry wydajnościowe:**

### W zakresie Firewall’a obsługa nie mniej niż 12 mln. jednoczesnych połączeń oraz 300 tys. nowych połączeń na sekundę.

### Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B.

### Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps.

### Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 45 Gbps.

### Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 15 Gbps.

### Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4,8 Gbps.

### Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1 lub AES128-SHA256) dla ruchu http – minimum 9 Gbps.

### **Funkcje Systemu Bezpieczeństwa:**

### W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

### Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

### Kontrola Aplikacji.

### Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

### Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

### Ochrona przed atakami - Intrusion Prevention System.

### Kontrola stron WWW.

### Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.

### Zarządzanie pasmem (QoS, Traffic shaping).

### Analiza ruchu szyfrowanego protokołem SSL i SSH.

### Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

### Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

### **Polityki firewalla**

### System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.

### Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

### System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

### **Połączenia VPN**

### System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

### Wsparcie dla IKE v1 oraz v2.

### Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)

### Obsługa protokołu Diffiego-Hellman grup 19 i 20

### Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

### 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.

### Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

### Mechanizm „Split tunneling” dla połączeń Client-to-Site

### System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

### Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

### Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

### Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.

### Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

### **Routing i obsługa łączy WAN**

### W zakresie routingu rozwiązanie powinno zapewniać obsługę:

### Routingu statycznego

### Policy Based Routingu

### Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

### System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

### **Zarządzanie pasmem**

### System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

### Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

### System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

### **Kontrola Antywirusowa**

### Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

### System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

### Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

### **Ochrona przed atakami**

### Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

### Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora i ma zawierać wszystkie opublikowane aktualne sygnatury.

### Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

### System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

### Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

### **Kontrola aplikacji**

### Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

### Baza sygnatur Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora i ma zawierać wszystkie opublikowane aktualne sygnatury.

### Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

### Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.

### Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

### **Kontrola WWW**

### Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

### W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, np: malware, phishing, spam, Dynamic DNS, proxy avoidance.

### Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

### Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

### System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

### Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

### **Uwierzytelnianie użytkowników w ramach sesji**

### System Firewall musi umożliwiać weryfikację tożsamości użytkowników 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 SecurID) w oparciu o zewnętrzne bazy danych.

### Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

### Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

### **Zarządzanie**

### Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

### Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

### Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

### System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow (lub równoważny).

### System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

### System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

### Dedykowany port konsoli RS-232 lub USB. Z urządzeniem należy dostarczyć kabel lub adapter konsolowy.

### **Logowanie:**

### System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

### W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

### Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

### Musi istnieć możliwość logowania do serwera SYSLOG.

### **Serwisy i licencje**

### W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące:

### Kontrolę aplikacji,

### IPS,

### Antywirus,

### Antyspam,

### Web Filtering