**Opis przedmiotu zamówienia**

**część 1: Zakup sprzętu komputerowego - UTM**

# Szczegółowe wymagania techniczne dla zapory UTM. Zamawiający wymaga dostarczenia 2 urządzeń o poniższej specyfikacji wraz z analizatorem logów z UTM.

Miejsce dostawy: Urząd Miejski w Nowym Tomyślu, ul. Poznańska 33, 64-300 Nowy Tomyśl

Wymagana dostawa 2 szt. jednakowych UTM wraz z wdrożeniem i implementacją w środowisku zamawiającego zgodnie z wymaganiami zamawiającego (migracja z obecnie używanego urządzenia Fortigate 310B). Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku zamawiającego oraz szkoleniem z obsługi urządzenia.

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

|  |  |
| --- | --- |
| **L.p.** | **Szczegółowe wymagania techniczne** |
| **1.** | **Wymagania minimalne** |
| 1.1. | System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| 1.2. | System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. |
| 1.3. | Istnieje możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu. |
| 1.4. | System wspiera protokoły IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. |
| **2.** | **Redundancja, monitoring i wykrywanie awarii** |
| 2.1. | System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514. |
| 2.2. | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
| 2.3. | Monitoring stanu realizowanych połączeń VPN. |
| 2.4. | System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **3.** | **Interfejsy, Dysk, Zasilanie** |
| 3.1. | System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  • 16 portami Gigabit Ethernet RJ-45.  • 8 gniazdami SFP 1 Gbps.  • 4 gniazdami SFP+ 10 Gbps. |
| 3.2. | System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. |
| 3.3. | System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. |
| 3.4. | System jest wyposażony w zasilanie AC. |
| **4.** | **Parametry wydajnościowe** |
| 4.1. | W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 140 tys. nowych połączeń na sekundę. |
| 4.2. | Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B |
| 4.3. | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. |
| 4.4. | Wydajność szyfrowania IPSec VPN nie mniej niż 33 Gbps. |
| 4.5. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. |
| 4.6. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. |
| 4.7. | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. |
| **5.** | **Funkcje Systemu Bezpieczeństwa** |
| W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: |
| 5.1. | Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |
| 5.2. | Kontrola Aplikacji. |
| 5.3. | Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |
| 5.4. | Ochrona przed malware. |
| 5.5. | Ochrona przed atakami - Intrusion Prevention System. |
| 5.6. | Kontrola stron WWW. |
| 5.7. | Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. |
| 5.8. | Zarządzanie pasmem (QoS, Traffic shaping). |
| 5.9. | Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |
| 5.10. | Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. |
| 5.11. | Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. |
| 5.12. | Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |
| 5.13. | Rozwiązanie posiada 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). |
| **6.** | **Polityki, Firewall** |
| 6.1. | Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |
| 6.2. | 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. |
| 6.3. | W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| 6.4. | Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. |
| 6.5. | Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. |
| 6.6. | Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. |
| 6.7. | 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.  • Kubernetes. |
| **7.** | **Połączenia VPN** |
| 7.1. | System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  • Wsparcie dla IKE v1 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. |
| 7.2. | System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  • 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. |
| **8.** | **Routing i obsługa łączy WAN** |
| W zakresie routingu rozwiązanie zapewnia obsługę: |
| 8.1. | Routingu statycznego. |
| 8.2. | Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). |
| 8.3. | Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. |
| 8.4. | Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. |
| 8.5. | ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. |
| 8.6. | BFD (Bidirectional Forwarding Detection). |
| 8.7. | Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **9.** | **Funkcje SD-WAN** |
| 9.1. | System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. |
| 9.2. | SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **10.** | **Zarządzanie pasmem** |
| 10.1. | System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
| 10.2. | System daje możliwość określania pasma dla poszczególnych aplikacji. |
| 10.3. | System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. |
| 10.4 | System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **11.** | **Ochrona przed malware** |
| 11.1. | Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
| 11.2. | Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. |
| 11.3. | 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. |
| 11.4. | System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. |
| 11.5. | System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| 11.6. | Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| 11.7. | 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. |
| 11.8. | System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| 11.9. | Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| 11.10. | Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **12.** | **Ochrona przed atakami** |
| 12.1. | Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
| 12.2. | System chroni przed atakami na aplikacje pracujące na niestandardowych portach. |
| 12.3. | Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| 12.4. | Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
| 12.5. | System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |
| 12.6. | Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). |
| 12.7. | Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. |
| 12.8. | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| 12.9. | Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **13.** | **Kontrola aplikacji** |
| 13.1. | Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
| 13.2. | Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| 13.4. | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |
| 13.5. | Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |
| 13.6. | Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. |
| 13.7. | Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). |
| 13.8. | 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). |
| **14.** | **Kontrola WWW** |
| 14.1. | Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |
| 14.2. | W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |
| 14.3. | Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. |
| 14.4. | Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |
| 14.5. | Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). |
| 14.6. | Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. |
| 14.7. | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. |
| 14.8. | Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. |
| 14.9. | System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **15.** | **Uwierzytelnianie użytkowników w ramach sesji** |
| 15.1. | System Firewall umożliwia 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. |
| 15.2. | System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. |
| 15.3. | 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. |
| 15.4. | Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **16.** | **Zarządzanie** |
| 16.1. | 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. |
| 16.2. | Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. |
| 16.3. | Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |
| 16.4. | System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. |
| 16.5. | System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
| 16.6. | Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| 16.7. | Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| 16.8. | Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). |
| 16.9. | Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **17.** | **Logowanie** |
| 17.1. | 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. |
| 17.2. | 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. |
| 17.3. | Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. |
| 17.4. | Możliwość włączenia logowania per reguła w polityce firewall. |
| 17.5. | System zapewnia możliwość logowania do serwera SYSLOG. |
| 17.6. | Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **18.** | **Testy wydajnościowe oraz funkcjonalne** |
| 18.1 | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta. |
| **19.** | **Serwis i licencja** |
| 19.1. | 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), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. |
| **20.** | **Gwarancja oraz wsparcie** |
| 20.1. | System jest objęty gwarancją producenta przez okres minimum 24 miesięcy, polegającą na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tej gwarancji producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| 20.2. | Wykonawca musi zapewnić pierwszą linię wsparcia przez okres minimum 36 miesięcy w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty należy dostarczyć przed podpisaniem umowy.** |
| **21.** | **Dodatkowe wymagania** |
| 21.1. | Wykonawca gwarantuje możliwość i realizuje migracje ustawień z obecnego UTM (Fortigate FG310B) znajdującego się w Urzędzie Miejskim w Nowym Tomyślu na nowy UTM zakupiony w ramach Cyberbezpiecznego Samorządu |

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Zamawiający dopuszcza równoważnie zaoferowanie wyłącznie urządzeń UTM, jeżeli dostarczony sprzęt będzie posiadał funkcjonalności i parametry wskazane poniżej.

**Wymagana dostawa 1 szt. analizatora wraz z wróżeniem i implementacją w środowisku zamawiającego zgodnie z wymaganiami zamawiającego. Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku zamawiającego oraz szkoleniem z obsługi urządzenia.**

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

|  |  |
| --- | --- |
| **L.p.** | **Wymagania minimalne** |
| **1.** | **Interfejsy** |
| 1.1. | System musi obsługiwać co najmniej 4 interfejsy sieciowe. |
| **2.** | **Parametry wydajnościowe** |
| 2.1. | System musi być w stanie przyjmować minimum 5 GB logów na dzień. |
| 2.2. | Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |
| **3.** | **Logowanie** |
| W zakresie logowania system musi zapewniać: |
| 3.1. | Podgląd logowanych zdarzeń w czasie rzeczywistym. |
| 3.2. | Możliwość przeglądania logów historycznych z funkcją filtrowania. |
| 3.3. | System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: • Listę najczęściej wykrywanych ataków. • Listę najbardziej aktywnych użytkowników. • Listę najczęściej wykorzystywanych aplikacji. • Listę najczęściej odwiedzanych stron www. • Listę krajów , do których nawiązywane są połączenia. • Listę najczęściej wykorzystywanych polityk Firewall. • Informacje o realizowanych połączeniach IPSec. |
| 3.4. | Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. |
| 3.5. | Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. |
| 3.6 | System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |
| **4.** | **Raportowanie** |
| W zakresie raportowania system musi zapewniać: |
| 4.1. | Generowanie raportów co najmniej w formatach: PDF, CSV. |
| 4.2. | Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników |
| 4.3. | Funkcję definiowania własnych raportów. |
| 4.4. | Możliwość spolszczenia raportów. |
| 4.5. | Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |
| **5.** | **Korelacja logów** |
| W zakresie korelacji zdarzeń system musi zapewniać: |
| 5.1. | Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |
| 5.2. | Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |
| Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. |
| 5.3. | Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. |
| **6.** | **Zarządzanie** |
| 6.1. | System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.  Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. |
| 6.2. | System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |
| **7.** | **Gwarancja oraz wsparcie** |
| 7.1. | System musi być objęty gwarancją producenta przez okres 24 miesięcy, umożliwiającą aktualizacje oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| 7.2. | Wykonawca musi zapewnić pierwszą linię wsparcia przez okres 36 miesięcy w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty należy dostarczyć przed podpisaniem umowy.** |

# Szczegółowe wymagania techniczne dla zapory UTM dla jednostek podległych. Zamawiający wymaga dostarczenia 7 urządzeń o poniższej specyfikacji.

**Wymagana dostawa 7 szt. jednakowych UTM wraz z wdrożeniem i implementacją w środowisku danej jednostki zgodnie z wymaganiami danej jednostki. Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku danej jednostki oraz szkoleniem z obsługi urządzeń.**

Wykaz jednostek podległych:

1. Szkoła Podstawowa nr 1 im. Tadeusza Kościuszki w Nowym Tomyślu

ul. Wierzbowa 1, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 2 im. Marii Skłodowskiej – Curie w Nowym Tomyślu

ul. 3 Stycznia 12, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 3 im. Feliksa Szołdrskiego w Nowym Tomyślu

os. Północ 25, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Marii Kownackiej w Wytomyślu

ul. Szkolna 18, 64-300 Wytomyśl;

1. Szkoła Podstawowa im. Marii Konopnickiej w Borui Kościelnej

ul. Szkolna 14, 64 - 300 Boruja Kościelna;

1. Zespół Przedszkolno - Szkolny w Bukowcu

ul. Kościelna 75, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Leonarda Śliwińskiego w Sątopach

ul. Szkolna 3, 64-300 Sątopy.

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.

|  |  |
| --- | --- |
| **L.p.** | **Szczegółowe wymagania techniczne** |
| **1.** | **Wymagania minimalne** |
| 1.1. | System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| 1.2. | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 3 administratorów do poszczególnych instancji systemu. |
| 1.3. | System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. |
| **2.** | **Redundancja, monitoring i wykrywanie awarii** |
| 2.1. | 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. |
| 2.2. | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
| 2.3. | Monitoring stanu realizowanych połączeń VPN. |
| 2.4. | System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| **3.** | **Interfejsy, Dysk, Zasilanie** |
| 3.1. | System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. |
| 3.2. | System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. |
| 3.3. | W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |
| 3.4. | System musi być wyposażony w zasilanie AC. |
| **4.** | **Parametry wydajnościowe** |
| 4.1. | W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. |
| 4.2. | Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. |
| 4.3. | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps. |
| 4.4. | Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. |
| 4.5. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps. |
| 4.6. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. |
| 4.7. | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps. |
| **5.** | **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: |
| 5.1. | Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |
| 5.2. | Kontrola Aplikacji. |
| 5.3. | Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |
| 5.4. | Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. |
| 5.5. | Ochrona przed atakami - Intrusion Prevention System. |
| 5.6. | Kontrola stron WWW. |
| 5.7. | Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. |
| 5.8. | Zarządzanie pasmem (QoS, Traffic shaping). |
| 5.9. | Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |
| 5.10. | Dwu-składnikowe 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. |
| 5.11. | Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. |
| 5.12. | Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system |
| **6.** | **Polityki, Firewall** |
| 6.1. | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |
| 6.2. | 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. |
| 6.3. | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| 6.4. | Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. |
| 6.5. | Element systemu realizujący funkcję Firewall musi integrować 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  • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. |
| **7.** | **Połączenia VPN** |
| 7.1. | 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 Diffie-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. |
| 7.2. | 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. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| **8.** | **Routing i obsługa łączy WAN** |
| 8.1. | W zakresie routingu rozwiązanie zapewnia obsługę: |
| 8.2. | Routingu statycznego. |
| 8.3. | Policy Based Routingu |
| 8.4. | Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
| **9.** | **Funkcje SD-WAN** |
| 9.1. | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. |
| 9.2. | Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. |
| **10.** | **Zarządzanie pasmem** |
| 10.1. | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
| 10.2. | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. |
| 10.3. | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **11.** | **Ochrona przed malware** |
| 11.1. | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
| 11.2. | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. |
| 11.3. | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| 11.4. | System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |
| 11.5. | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| 11.6. | Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| **12.** | **Ochrona przed atakami** |
| 12.1. | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
| 12.2. | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. |
| 12.3. | Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| 12.4. | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
| 12.5. | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |
| 12.6. | 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. |
| 12.7. | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| **13.** | **Kontrola aplikacji** |
| 13.1. | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
| 13.2. | Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| 13.3. | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |
| 13.4. | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |
| 13.5. | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| **14.** | **Kontrola WWW** |
| 14.1. | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |
| 14.2. | W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |
| 14.3. | Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. |
| 14.4. | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |
| 14.5. | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. |
| 14.6. | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| 14.7. | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| **15.** | **Uwierzytelnianie użytkowników w ramach sesji** |
| 15.1. | 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. |
| 15.2. | Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. |
| 15.3. | Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| 15.4. | Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **16.** | **Zarządzanie** |
| 16.1. | 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. |
| 16.2. | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
| 16.3. | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |
| 16.4. | System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |
| 16.5. | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
| 16.6. | Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| 16.7. | Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| **17.** | **Logowanie** |
| 17.1. | Elementy systemu bezpieczeństwa muszą realizować logowanie 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. |
| 17.2. | W ramach logowania system pełniący funkcję Firewall 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. |
| 17.3. | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. |
| 17.4. | Musi istnieć możliwość logowania do serwera SYSLOG. |
| **18.** | **Serwis i licencja** |
| 18.1. | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres gwarancji producenta trwającej przynajmniej 24 miesiące. |
| **19.** | **Gwarancja oraz wsparcie** |
| 19.1. | System musi być objęty gwarancją producenta przez okres 24 miesięcy, polegającą na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tej gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| 19.2. | Wykonawca musi zapewnić pierwszą linię wsparcia przez okres 36 miesięcy w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty należy dostarczyć przed podpisaniem umowy.** |
| **20.** | **Certyfikaty** |
| 20.1. | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall. |

# Szczegółowe wymagania techniczne dla przełączników dla jednostek podległych. Zamawiający wymaga dostarczenia 14 urządzeń o poniższej specyfikacji.

**Wymagana dostawa 14 szt. jednakowych przełączników wraz z wdrożeniem i implementacją w środowisku danej jednostki zgodnie z wymaganiami danej jednostki. Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku danej jednostki oraz szkoleniem z obsługi urządzenia.**

Wykaz jednostek podległych:

1. Szkoła Podstawowa nr 1 im. Tadeusza Kościuszki w Nowym Tomyślu

ul. Wierzbowa 1, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 2 im. Marii Skłodowskiej – Curie w Nowym Tomyślu

ul. 3 Stycznia 12, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 3 im. Feliksa Szołdrskiego w Nowym Tomyślu

os. Północ 25, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Marii Kownackiej w Wytomyślu

ul. Szkolna 18, 64-300 Wytomyśl;

1. Szkoła Podstawowa im. Marii Konopnickiej w Borui Kościelnej

ul. Szkolna 14, 64 - 300 Boruja Kościelna;

1. Zespół Przedszkolno - Szkolny w Bukowcu

ul. Kościelna 75, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Leonarda Śliwińskiego w Sątopach

ul. Szkolna 3, 64-300 Sątopy.

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. Zamawiający wymaga dostarczenia 14 przełączników o poniższej specyfikacji.

|  |  |
| --- | --- |
| L.p. | Wymagania minimalne |
| 1. | Parametry fizyczne platformy |
| 1.1. | Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. |
| 1.2. | Zasilanie AC 230V. |
| 1.3. | Maksymalny pobór mocy: 28 W. |
| 1.4. | Zakres temperatury pracy: 0-45ᵒC. |
| **2.** | **Interfejsy sieciowe** |
| 2.1. | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • 24 porty GE RJ-45 • 4 porty 10 GE SFP+ |
| **3.** | **Zarządzanie** |
| 3.1. | Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. |
| 3.2. | Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). |
| 3.3. | Wsparcie dla SNMP w wersjach 1-3 |
| 3.4. | Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. |
| 3.5. | Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. |
| 3.6. | Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. |
| 3.7. | Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). |
| 3.8. | Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. |
| 3.9. | Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. |
| 3.10. | Automatycznie wykonywane rewizje konfiguracji. |
| **4.** | **Parametry wydajnościowe** |
| 4.1. | Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. |
| 4.2. | Tablica adresów MAC o pojemności co najmniej 32k wpisów. |
| 4.3. | Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |
| **5.** | **Wymagane funkcje** |
| 5.1. | Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. |
| 5.2. | Obsługa Jumbo Frames. |
| 5.3. | Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). |
| 5.4. | Agregacja portów zgodna ze standardem 802.3ad. |
| 5.5. | Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. |
| 5.6. | Obsługa routingu statycznego. |
| 5.7. | Port-mirroring. |
| 5.8. | Uwierzytelnianie 802.1x na poziomie portu. |
| 5.9. | Uwierzytelnianie 802.1x w oparciu o adres MAC. |
| 5.10. | W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). |
| 5.11. | W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. |
| 5.12. | W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. |
| 5.13 | Obsługa protokołu sFlow. |
| **6.** | **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC** |
| 6.1. | Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:  • Centralne zarządzanie konfiguracją urządzenia  • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki itp... • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.  • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwa hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.  • Automatyczna detekcja i rekomendacje konfiguracji.  • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC • Wykrywanie aplikacji komunikujących się w sieci. |
| 6.2. | Musi być możliwe redundantne połączenie z elementami zarządzającymi. |
| 6.3. | W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| **7.** | **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa** |
| **7.1.** | System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. |
| 7.2. | System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| **8.** | **Gwarancja oraz wsparcie** |
| 8.1. | System musi być objęty gwarancją producenta przez okres 24 miesięcy, polegającą na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tej gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| 8.2. | Wykonawca musi zapewnić pierwszą linię wsparcia przez okres 36 miesięcy w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty należy dostarczyć przed podpisaniem umowy.** |