**IRP.272.4.51.2023**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup i dostawa sprzętu multimedialnego i RTV do bursy szkolnej w Łęcznej**

**Zadanie 2 – Urządzenia sieciowe**

1. **Punkt dostępowy – 11 szt.**

|  |  |
| --- | --- |
| Obsługiwana częstotliwość | 2,4GHz i 5GHz |
| Standardy komunikacyjne | IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.1Q |
| Liczba użytkowników | Powyżej 250 |
| MIMO | TAK |
| Obsługa sieci VLAN | TAK |
| QoS | TAK |
| Moc nadajnika | Powyżej 20 dBmW |
| Szyfrowanie/bezpieczeństwo | WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA3-Enterprise |
| Ilość portów Ethernet LAN | Min. 1 |
| PoE | TAK |
| Umieszczenie | Sufit |

1. **Przełącznik – 1 szt.**

|  |  |
| --- | --- |
| Porty | 24x GE RJ45, 4x 10GE SFP+ |
| Konsola(RJ-45) | Min. 1 |
| Zdolność przełączania (Duplex) | Min. 128Gbps |
| Pakiety na sekundę (Duplex) | Min. 190Mbps |
| Tablica adresów MAC | 32K |
| Opóźnienie sieciowe | Poniżej 1μs |
| Rozmiar grupy agregacji łączy | 8 |
| Całkowita liczba grup agregacji łączy | 128 |
| Bufory pakietów | 2MB |
| DRAM | Min. 512MB DDR3 |
| FLASH | Min. 64MB |
| Licencja/serwis min. 3lata | Jeśli wymagana przy zaoferowanym produkcie |

1. **Przełącznik z PoE - 2 szt.**

|  |  |
| --- | --- |
| Porty | 24x GE RJ45, 4x 10GE SFP+ |
| Konsola(RJ-45) | Min. 1 |
| Zdolność przełączania (Duplex) | Min. 128Gbps |
| Porty PoE | 12 (802.3af/at) |
| Moc PoE | 185W |
| Pakiety na sekundę (Duplex) | Min. 190Mbps |
| Tablica adresów MAC | 32K |
| Opóźnienie sieciowe | Poniżej 1μs |
| Rozmiar grupy agregacji łączy | 8 |
| Całkowita liczba grup agregacji łączy | 128 |
| Bufory pakietów | 2MB |
| DRAM | Min. 512MB DDR3 |
| FLASH | Min. 64MB |
| Licencja/serwis min. 3lata | Jeśli wymagana przy zaoferowanym produkcie |

1. **System ochrony sieci – 1 szt.**

|  |
| --- |
| **Minimalne wymagane parametry** |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję ochrony sieci 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: Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego. W przypadku systemu pełniącego funkcje: IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji ochrony siecil. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję ochrony sieci musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. System ochrony sieci musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu ochrony sieci powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. W zakresie frewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. Przepustowość stateful dla ochrony sieci: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość ochrony sieci z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN 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 - minimum 1.4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. 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; Zarządzanie pasmem (QoS, Traffic shaping); Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); 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; Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2; 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. Polityka ochrony sieci 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. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików. Element systemu realizujący funkcję ochrony sieci 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; 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. 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. 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 powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. System ochrony sieci 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. 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. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 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. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 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. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. System ochrony sieci 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 dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. 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. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję ochrony sieci musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji ochrony sieci. Element systemu realizujący funkcję ochrony sieci musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. W ramach logowania system pełniący funkcję ochrony siecil 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. Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie gwarancji na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen. **3letnia gwarancja producenta**. Dostawa nowego urządzenia po stwierdzeniu awarii. Wsparcie w reżimie 24x7 w językach angielskim i polskim. W ramach dostawy wykonawca dokona pełnego wdrożenia oferowanego przedmiotu zamówienia wg wytycznych Zamawiającego. |