

Załącznik nr 9.9 do Opisu przedmiotu zamówienia

Wymagania dla Części 9

Bezpieczeństwo

Spis treści

| | |
|--|---|
| 1. KODY CPV | 3 |
| 2. FIREWALL – 1SZT | 3 |
| 3. OPROGRAMOWANIE ANTYWIRUSOWE – 70 SZT (LICENCJI) | 9 |
| 4. SZKOLENIA – 2 PAKIETY | 9 |

1. Kody CPV

Przedmiot zamówienia – kody CPV

- 30.23.60.00-2 Różny sprzęt komputerowy
- 32.41.70.00-3 Urządzenia sieciowe
- 48.42.20.00-2 Zestawy pakietów oprogramowania
- 80.50.00.00-9 Usługi szkoleniowe

2. Firewall – 1szt

| Nazwa wymagania | Opis wymagania |
|---|--|
| Wymagania ogólne | <p>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.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | <p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów</p> |

| | |
|--------------------------------|--|
| | redundantnych. |
| Porty i zasilanie | <p>System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.</p> <p>System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System musi być wyposażony w zasilanie AC.</p> |
| Parametry wydajnościowe | <p>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.</p> <p>Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.</p> <p>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.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.</p> |
| Funkcje systemu bezpieczeństwa | <p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 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 |

| | |
|--------------------|---|
| | <p>uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</p> <p>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</p> |
| Polityki, firewall | <p>Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>Translację jeden do jeden oraz jeden do wielu.</p> <p>Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p> <p>W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.</p> <p>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.</p> <p>Amazon Web Services (AWS).</p> <p>Microsoft Azure</p> <p>Google Cloud Platform (GCP).</p> <p>OpenStack.</p> <p>VMware NSX.</p> |
| Połączenia VPN | <p>System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <p>Wsparcie dla IKE v1 oraz v2.</p> <p>Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>Obsługa protokołu Diffie-Hellman grup 19 i 20.</p> <p>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.</p> <p>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> |

| | |
|-----------------------------|---|
| | <p>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.</p> <p>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.</p> |
| Routing i obsługa łączą WAN | <p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <p>Routing statycznego.</p> <p>Policy Based Routingu.</p> <p>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</p> |
| Funkcje SD-WAN | <p>System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.</p> <p>Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.</p> |
| Zarządzanie pasmem | <p>System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</p> |
| Ochrona przed malware | <p>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.</p> <p>System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>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.</p> <p>System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> |
| Ochrona przed atakami | <p>Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System powinien chronić przed atakami na aplikacje pracujące na</p> |

| | |
|--------------------|---|
| | <p>niestandardowych portach.</p> <p>Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>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.</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> |
| Kontrola aplikacji | <p>Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p> |
| Kontrola WWW | <p>Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>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.</p> <p>Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p> <p>W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p> |
| Uwierzytelnianie | <p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za</p> |

| | |
|-----------------------------|---|
| użytkowników w ramach sesji | <p>pomocą:</p> <p>Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.</p> <p>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p> |
| Zarządzanie | <p>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.</p> <p>Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <p>System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> |
| Logowanie | <p>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.</p> <p>W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.</p> <p>Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów</p> |

| | |
|--------------------|---|
| | <p>sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.</p> |
| Certyfikaty | <p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.</p> |
| Serwisy i licencje | <p>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 60 miesięcy.</p> <p>System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p> |

3. Oprogramowanie antywirusowe – 70 szt. (licencji)

| Nazwa komponentu | Wymagane minimalne parametry techniczne |
|------------------|---|
| Stan obecny | <p>Zamawiający obecnie posiada aktywna licencje na oprogramowanie ESET a dokładnie 54 licencje ESET Endpoint Antivirus Suite</p> |
| Wymaganie | <p>Zamawiający oczekuje podniesienia i rozszerzenia do pakietu ESET PROTECT Essential ON-PREM na 70 licencji (ochrona stacji Windows i serwerów Windows Serwer)</p> <p>Licencja na aktualizację sygnatur i oprogramowania na minimum 60 miesięcy.</p> |

4. Szkolenia – 2 pakiety

| Nazwa komponentu | Wymagane minimalne parametry techniczne |
|------------------|--|
| Pakiet 1 | <p>W ramach dostawy należy zapewnić VOUCHERY na pakiet stacjonarnych szkoleń z posiadanego przez Zamawiającego rozwiązania ESET tj. ESET CLIENT & NETWORK SECURITY ADMINISTRATOR oraz ESET ADVANCED ADMINISTRATION - WARSZTAT PRAKTYCZNY</p> |

| | |
|----------|---|
| | <p>Szkolenia mają być przeprowadzone w Autoryzowanym Centrum Szkoleniowym posiadającym autoryzację producenta.</p> <p>Należy do oferty wpisać link do strony www gdzie można zweryfikować autoryzację Centrum Szkoleniowego</p> |
| Pakiet 2 | <p>W ramach dostawy należy zapewnić VOUCHERY na pakiet stacjonarnych szkoleń z obsługi dostarczonego rozwiązania UTM w zakresie np. CERTIFIED NETWORK ADMINISTRATOR</p> <p>Szkolenia mają być przeprowadzone w Autoryzowanym Centrum Szkoleniowym posiadającym autoryzację producenta.</p> <p>Należy do oferty wpisać link do strony www gdzie można zweryfikować autoryzację Centrum Szkoleniowego</p> |