

Opis przedmiotu zamówienia

Dostawa i wdrożenie systemu bezpieczeństwa zbudowanego w oparciu o urządzenia UTM pracujące w systemie HA do zabezpieczenia sieci LAN i Internetu w ramach projektu pn. „Małopolski System Informacji Medycznej (MSIM)”.

Wymagania minimalne:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa musi zostać dostarczony w postaci klastra wysokiej dostępności działającego co najmniej w trybie Active-Passive.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000
- System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 1GbE (SFP)
- System realizujący funkcję Firewall musi dysponować minimum 4 interfejsami optycznymi 10GbE (SFP+)
- System realizujący funkcję Firewall musi zostać dostarczony wraz z 4 wkładkami 10Gbe (SFP+) – po dwie do każdego z urządzeń pracującego w klastrze wysokiej dostępności. Wkładki muszą pochodzić z oficjalnego kanału dystrybucji, tego samego co producent sprzętu i muszą być objęte gwarancją producenta rozwiązania UTM.
- Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 85 000 nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 120 GB do celów logowania i raportowania.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
 - Kontrola dostępu - zaporą ogniową klasy Stateful Inspection
 - Ochrona przed wirusami – komercyjny antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
 - Poufność danych - IPSec VPN oraz SSL VPN
 - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
 - Kontrola stron Internetowych – Web Filter [WF]
 - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
 - Kontrola pasma oraz ruchu [QoS i Traffic shaping]
 - Kontrola aplikacji oraz rozpoznawanie ruchu P2P

- Analiza ruchu szyfrowanego protokołem SSL
- Wydajność systemu Firewall minimum 25 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2,5 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 14 Gbps
- Wydajność VPN IPsec, nie mniej niż 4 Gbps
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
 - Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
 - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
 - Praca w topologii Hub and Spoke oraz Mesh
 - Obsługa mechanizmów: IPsec NAT Traversal, DPD, Xauth
 - Obsługa ssl vpn w trybach portal oraz tunel
- Rozwiązanie musi zapewniać obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
- Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza filtra WWW pogrupowana w min 65 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
 - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
 - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny

- W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
 - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
 - Generowanie co najmniej 25 różnych typów raportów
- System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
- System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów
- Wraz z systemem musi zostać dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
- Urządzenie musi:
 - posiadać certyfikat Common Criteria EAL4+
 - posiadać certyfikat ICSE Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
- Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Wymaga się, aby dostawa obejmowała również:
 - 36 miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
 - Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.
 - Certyfikowane szkolenie zakończone egzaminem producenta dla 3 osób
 - Wdrożenie dostarczonego rozwiązania w infrastrukturze zamawiającego. Wdrożenie powinno odbyć się w siedzibie zamawiającego.
- W ramach dostawy Zamawiający wymaga, aby rozwiązanie zostało wdrożone wg. przekazanych wytycznych przez zamawiającego dotyczących konfiguracji sieci LAN, WAN oraz zdefiniowania polityk bezpieczeństwa. Zamawiający aktualnie posiada urządzenia Stormshield SN900 i SN160.
- W okresie 30 dni od zakończonego wdrożenia dostawca zapewni wsparcie powdrożeniowe. Wsparcie będzie realizowane w trybie zdalnym w wymiarze 3 godzin.