

Opis Przedmiotu Zamówienia

Wariant 1

I. Ogólne

1. Dostarczenie sprzętu wraz wymaganymi licencjami na okres 36 miesięcy od wdrożenia:
 - a. 2 szt. Firewall działający w klastrze active-active (urządzenie centralne, siedziba główna),
 - b. 2 szt. Firewall urządzenia na lokalizacjach wyniesionych (2 lokalizacje),
 - c. 1 szt. urządzenia dostępowe dla urządzeń serwisowych (hala serwisowa w lokalizacji przy siedzibie głównej).
2. Usługi:
 - a. szkolenie administratorskie dla dwóch administratorów (dopuszczalne w formie zdalnej),
 - b. wsparcie w przygotowaniu do wdrożenia produkcyjnego zapory sieciowej, przeglądzie obecnej konfiguracji Zmawiającego (dopuszczalne w formie zdalnej),
 - c. instalacja nowych urządzeń, konfiguracja wstępna, fizyczne uruchomienie i testy (prace stacjonarne),
 - d. poprawki i rekonfiguracje (dopuszczalne w formie zdalnej),
 - e. asysta wdrożenia produkcyjnego (dopuszczalne w formie zdalnej),
 - f. dostarczenie dokumentacji powdrożeniowej pozwalającej na otworenie konfiguracji i ponowną instalację.
3. Obecne rozwiązania techniczne Zamawiającego które zostaną zastąpione:

Sztuk	Nazwa	Licencje	Lokalizacja
2	SOPHOS XG210	XG 210 Enhanced to Enhanced Plus Support (SKU: EP212CEUP), XG 210 Email Protection (SKU: XM212CTAA), XG 210 Webserver Protection (SKU: XS212CTAA), XG 210 Xstream Protection - (SKU: XX212CTES)	Siedziba Główna
2	SOPHOS XG86	XG 86 Xstream Protection (SKU: XX8B2CTES), XG 86 Webserver Protection - (SKU: XS8B2CTAA), XG 86 Email Protection - (SKU: XM8B2CTAA)	Lokalizacja 1, Lokalizacja 2
1	Zyxel USG60W	LIC-BUN for USG60 & USG60W, Filtering/Anti-Virus Bitdefender	Hala serwisowa (Siedziba Główna)

		Signature/SecuReporter Premium License, LIC-BUN for USG60 & USG60W, Content Filtering/Anti-Virus Bitdefender Signature/SecuReporter Premium License	
--	--	---	--

4. 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.
5. **Wymagania ogólne:**
- a. **Zarządzanie i raportowanie:**
 - i. System musi umożliwiać centralne zarządzanie wszystkimi funkcjami bezpieczeństwa z jednej konsoli administracyjnej lub z konsoli na poziomie lokalizacji.
 - ii. Powinien oferować szczegółowe raportowanie i monitorowanie zdarzeń bezpieczeństwa oraz możliwość generowania niestandardowych raportów.
 - b. **Wysoka dostępność i odporność na awarie (dotyczy 2 szt. Firewall działające w klastrze active-active)**
 - i. System powinien wspierać konfiguracje wysokiej dostępności (HA) i zapewniać nieprzerwane działanie w przypadku awarii jednego z komponentów.
 - ii. Wymagana jest funkcja automatycznego przełączania na zapasowe urządzenie w przypadku awarii.
 - c. **Integracja z istniejącą infrastrukturą:**
 - i. System musi być kompatybilny z istniejącymi rozwiązaniami sieciowymi i bezpieczeństwa.
 - ii. Powinien oferować API do integracji z systemami zarządzania bezpieczeństwem informacji (SIEM) oraz innymi narzędziami monitorowania.
 - iii. Obsługiwać pliki JSON oraz Syslog w celu przekazywania danych do centralnego serwera logów.
 - d. **Aktualizacje i wsparcie techniczne:**
 - i. Dostawca musi zapewnić regularne aktualizacje oprogramowania w celu zachowania najwyższego poziomu bezpieczeństwa.
 - ii. Wymagane jest również zapewnienie wsparcia technicznego w trybie 24/7, w tym szybka reakcja na zgłoszenia serwisowe i incydenty bezpieczeństwa.
 - e. **Polityki bezpieczeństwa i zgodność:**

- i. System musi umożliwiać definiowanie i egzekwowanie zaawansowanych polityk bezpieczeństwa zgodnych z obowiązującymi standardami i przepisami.
 - ii. Powinien wspierać mechanizmy audytowania i logowania działań administracyjnych oraz zdarzeń sieciowych.
- f. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów:
 - i. Routera z funkcją NAT
 - ii. Transparentnym
 - iii. Monitorowania na porcie SPAN (Switched Port Analyzer)
- g. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum dwóch oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:
 - i. Routingu
 - ii. Firewalla
 - iii. IPSec VPN
 - iv. Antywirusa
 - v. IPS
 - vi. Kontroli Aplikacji
- h. Powinna istnieć możliwość dedykowania co najmniej trzech administratorów do poszczególnych instancji systemu,
- i. System musi wspierać IPv4 oraz IPv6 w zakresie:
 - i. Firewall
 - ii. Ochrony w warstwie aplikacji
 - iii. Protokołów routingu dynamicznego

II. Szczegółowe wymagania

1. Redundancja, monitoring i wykrywanie awarii

- a. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active. Wymagane jest istnienie funkcji synchronizacji sesji firewall.
- b. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
- c. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- d. Monitoring stanu realizowanych połączeń VPN.
- e. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
- f. Raportowanie ruchu sieciowego, ilości wywołań, połączeń odrzuconych i zaakceptowanych.
- g. Wysyłanie na maila i SMS informacji o zaistniałych zagrożeniach/zdarzeniach zdefiniowanych przez administratora, lub dostarczenie oprogramowania pozwalającego spełnić ten zapis.

2. Interfejsy, Dysk, Zasilanie:

2.1 Siedziba Główna

- a. System realizujący funkcję Firewall musi dysponować minimum:
 - 16 portami Gigabit Ethernet RJ-45.
 - 8 gniazdami SFP 1 Gbps.
 - 2 gniazdami SFP+ 10 Gbps.
- b. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- c. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- d. System musi być wyposażony w zasilanie AC.

2.2 Lokalizacja 1 i 2

- a. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 5 portami Gigabit Ethernet RJ-45.
- b. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- c. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- d. System jest wyposażony w zasilanie AC.

2.3 Hala serwisowa

- a. System realizujący funkcję Firewall dysponuje musi dysponować minimum:
 - 5 portami Gigabit Ethernet RJ-45.
 - Ponadto system realizujący funkcje firewall jest wyposażony w interfejs radiowy WiFi pracujący w standardach 802.11 a/b/g/n/ac. Jeżeli takiego interfejsu nie posiada, koniecznym jest zastosowanie urządzenia Access Point pracującego w w.w. standardach radiowych wraz z systemem centralnego zarządzania siecią WiFi (kontrolerem).
- b. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- c. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- d. System jest wyposażony w zasilanie AC.

3. Parametry wydajnościowe:

3.1 Siedziba Główna

- a. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
- b. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.

- c. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
- d. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
- e. 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 2.5 Gbps.
- f. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
- g. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

3.2 Lokalizacja 1 i 2 i Hala serwisowa

- a. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
- b. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
- c. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
- d. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
- e. 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 Gbps.
- f. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
- g. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

4. 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:

- a. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
- b. Kontrola Aplikacji.
- c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
- e. Ochrona przed atakami - Intrusion Prevention System.
- f. Kontrola stron WWW.
- g. Inspekcja ruchu SSL/TSL.
- h. Śledzenie połączeń: FTP, IRC, PPTP, TFTP.
- i. Zarządzanie pasmem (QoS, Traffic shaping).
- j. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- k. 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 dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. (Zamawiający posiada klucze YubiKey 5 NFC (jeżeli można je zastosować dostawa nie dotyczy) oraz korzysta z Microsoft Authenticator).

- l. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
- m. Analiza ruchu szyfrowanego protokołem SSH.
- n. 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.
- o. Rozwiązanie posiadać będzie 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).
- p. Wbudowane mechanizmy zapobiegające włamaniom i atakom (DoS, DDoS, skanowanie portów).
- q. Ochrona przed atakami Zero-day.
- r. Automatyczna aktualizacja listy blokowanych stron pobierana z pliku .txt z zewnętrznego hosta.
- s. Automatyczne tworzenie kopii konfiguracji zabezpieczonej hasłem na zasobie zewnętrznym.
- t. Możliwość tworzenia profili: harmonogramów godzin, dostępow, limitów użytkownika Internetu, limitów danych, odszyfrowywania połączeń IPsec.
- u. Możliwość tworzenia list: hostów IP, grup hostów IP, hostów MAC, hostów FQDN, grup hostów FQDN, grup lokalizacyjnych, usług, grup usług.
- v. Możliwość tworzenia list ACL dla użytkowników, grup, połączeń VPN.

5. Polityki, Firewall

- a. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- b. 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.
- c. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- d. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
- e. Tworzenie reguł firewalla dla określonych połączeń/typów połączeń (VPN, LAN, WAN, DMZ).
- f. Tworzenie reguł NAT oraz przekierowań.
- g. 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:

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- OpenStack
- VMware NSX

6. Połączenia VPN

- a. 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.
 - Obsługa tunelów GRE lub tuneli IpSecVPN z GRE.
 - Obsługa dedykowanych tunelów z Microsoft Azure lub IpSec IKEv2.
 - Wbudowane mechanizmy automatycznego przełączania połączenia VPN w przypadku braku dostępności łącza (failover group).
- b. 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 (dla definiowanych użytkowników lub grup), które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
- c. Wbudowane mechanizmy automatycznego przełączania połączenia VPN w przypadku braku dostępności łącza (failover group).

7. Routing i obsługa łączy WAN

- a. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
 - Routingu statycznego.

- Policy Based Routing.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- Możliwość konfiguracji routingu (static, OSPF, BGP, multicast).

8. Funkcje SD-WAN

- a. System powinien umożliwić wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
- b. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

9. Zarządzanie pasmem

- a. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- b. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
- c. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware

- a. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- b. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- c. 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.
- d. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
- e. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

11. Ochrona przed atakami

- a. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- b. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- c. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- d. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- e. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

- f. 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.
- g. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12. Kontrola aplikacji

- a. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- b. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- c. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- d. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- e. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- f. Kontrola aplikacji z możliwością monitorowania używania aplikacji.

13. Kontrola WWW

- a. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- b. 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.
- c. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
- d. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- e. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
- f. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- g. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
- h. Blokowanie i ochrona stron www z możliwością tworzenia polis dostępowych/kategorii oraz dostosowywaniem akcji (blokowanie, ostrzeżenie, informacja).

14. Uwierzytelnianie użytkowników w ramach sesji

- a. 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.
- b. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
- c. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
- d. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

15. Zarządzanie

- a. 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.
- b. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- c. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
- d. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- e. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- f. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- g. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
- h. Możliwość tworzenia administratorów oraz przypisywania im ról.
- i. Dostęp do urządzenia przez SSH, HTTPS, dedykowany portal.
- j. Obsługa dostępu klientów VPN z podziałem na uprawnienia z obsługą urządzeń z systemami Windows, MacOS, Android, Linux.
- k. Wysyłanie na maila i SMS informacji o zaistniałych zagrożeniach/zdarzeniach lub dostarczenie narzędzie pozwalających na realizację tego.
- l. Możliwość ręcznego ustawienia portu dostępowego do urządzenia oraz portu dostępu do portalu użytkownika.
- m. Możliwość ustawienia kontroli złożoności hasła dostępowego do klienta VPN dla użytkowników.
- n. Automatyczna aktualizacja bibliotek urządzenia wraz z możliwością zarządzania wersją firmware'u urządzenia.
- o. Blokowanie wysyłania informacji poufnych w tle z już zainfekowanych komputerów.

16. Logowanie

- a. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania).
- b. 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.
- c. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- d. Musi istnieć możliwość logowania do serwera SYSLOG w formacie m.in. JSON.

17. Serwisy i licencje

- a. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować na okres 36 miesięcy:
 - Kontrola Aplikacji,
 - IPS,
 - Analiza typu Sandbox,
 - Antyspam,
 - Web Filtering,
 - bazy reputacyjne adresów IP/domen.

18. Gwarancja oraz wsparcie

- a. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.

19. Szkolenie administratorskie

Szkolenie administratorskie powinno zawierać omówienie takich obszarów jak:

- a. Wprowadzenie do firewalli:
 - Podstawowe pojęcia i definicje (firewall, strefa DMZ, NAT, filtracja pakietów, stanowa inspekcja).
 - Znaczenie i rola firewalli w ochronie sieci.
- b. Architektura i komponenty systemu:
 - Przegląd architektury typowego rozwiązania firewall.
 - Opis komponentów systemu firewall i ich roli (interfejsy, reguły, polityki).
 - Schematy sieciowe i topologie z uwzględnieniem firewalli.
- c. Instalacja i konfiguracja:
 - Wymagania systemowe i przygotowanie środowiska.
 - Procedury instalacji sprzętowego i programowego firewalla.
 - Podstawowa konfiguracja firewalli (adresacja IP, interfejsy sieciowe, strefy bezpieczeństwa).

- d. Konfiguracja polityk bezpieczeństwa:
 - Tworzenie i zarządzanie politykami bezpieczeństwa.
 - Ustawienia reguł pozwalających, blokujących i monitorujących ruch sieciowy.
 - Konfiguracja filtracji pakietów, filtrowanie aplikacji, inspekcja protokołów.
- e. Zarządzanie użytkownikami i dostępem:
 - Konfiguracja kont użytkowników i uprawnień administratorów.
 - Mechanizmy autoryzacji i uwierzytelniania.
 - Zarządzanie rolami i dostępem do konsoli zarządzania firewall.
- f. Monitorowanie i logowanie:
 - Narzędzia do monitorowania ruchu sieciowego i działania firewalla.
 - Analiza logów i generowanie raportów dotyczących aktywności i incydentów.
 - Konfiguracja systemów ostrzegania i powiadamiania o incydentach.
- g. Zarządzanie zagrożeniami i incydentami:
 - Identyfikacja, analiza i reagowanie na zagrożenia oraz incydenty bezpieczeństwa.
 - Tworzenie i wdrażanie procedur zarządzania incydentami.
 - Integracja firewalla z systemami SIEM (Security Information and Event Management).
- h. Aktualizacje i utrzymanie systemu:
 - Procedury aktualizacji oprogramowania i sygnatur bezpieczeństwa.
 - Regularne przeglądy i testy konfiguracji firewalli.
 - Tworzenie kopii zapasowych i planowanie odzyskiwania danych.
- i. Zaawansowane funkcje i optymalizacja:
 - Wykorzystanie zaawansowanych funkcji firewalli nowej generacji (NGFW) takich jak IDS/IPS, filtrowanie URL, inspekcja SSL/TLS.
 - Optymalizacja wydajności firewalla.
 - Integracja z innymi systemami bezpieczeństwa (VPN, proxy, DLP).
- j. Symulacje i scenariusze:
 - Ćwiczenia praktyczne z konfiguracji, monitorowania i reagowania na zagrożenia.
 - Scenariusze symulacji ataków i incydentów bezpieczeństwa.
- k. Wsparcie techniczne i rozwiązywanie problemów:
 - Procedury identyfikacji i rozwiązywania najczęstszych problemów.
 - Korzystanie z dokumentacji, forum wsparcia i kontaktu z pomocą techniczną.