**Opis przedmiotu zamówienia**

1. Sieciowe urządzenia typu Firewall do ochrony brzegowej sieci komputerowych LAN - 2 szt.
   1. Zapora sieciowa (firewall) musi być dostarczona w postaci dwóch dedykowanych urządzeń sieciowych (Appliance) umożliwiających pracę zarówno w konfiguracji Active-Passive, jak również Active-Active. Dedykowane urządzenia sieciowe muszą posiadać zainstalowane oprogramowanie, pochodzące od tego samego producenta.
   2. System zabezpieczeń funkcji firewall umożliwia ochronę sieci bez ograniczeń dla liczby adresów IP.
   3. Zapora musi umożliwiać zarządzanie za pomocą interfejsu aplikacji GUI oraz ssh.
   4. Polityka bezpieczeństwa firewall w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły i usługi sieciowe, użytkowników i serwery usług oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS).
   5. Zapora wykonuje dynamiczną i statyczną translację adresów NAT.
   6. Komunikacja pomiędzy modułem zapory sieciowej i modułem zarządzania jest szyfrowana i uwierzytelniona. (nie dotyczy jeśli moduł zarządzania jest integralną częścią zapory)
   7. Uwierzytelnianie administratorów firewall odbywa się za pomocą haseł statycznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
   8. Zapora posiada wiele metod uwierzytelniania użytkowników lokalnych i zdalnych (np. uwierzytelnianie przezroczyste gdzie firewall przechwytuje sesję i uwierzytelnia jej użytkownika, uwierzytelniania po połączeniu się z modułem firewall). Baza użytkowników jest przechowywana lokalnie na firewall lub na zewnętrznym serwerze (np. LDAP).
   9. Funkcjonalność zabezpieczeń firewall musi być rozszerzona o mechanizmy ochrony przed intruzami. Mechanizm musi zapewniać co najmniej wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan). Aktualizacja bazy sygnatur ma się odbywać poprzez sieć, automatycznie i na żądanie administratora.
   10. Funkcjonalność zabezpieczeń firewall:

- moduł kontroli aplikacji sieciowych używanych przez użytkowników wewnętrznych. Identyfikacja aplikacji ma odbywać się w oparciu o bazę danych utrzymywaną przez producenta zapory

- moduł zabezpieczeń IPS wyposażonego w mechanizmy ochrony przez intruzami

- moduł umożliwiający filtrowanie URL

- moduł ochrony antywirusowej

* 1. Funkcjonalność zabezpieczeń firewall w razie potrzeby może zostać rozszerzona również z użyciem rozwiązań innego producenta. Integracja firewall z zabezpieczeniami innego dostawcy odbywa się za pomocą dedykowanych protokołów lub dostarczonego API.
  2. Umożliwia tworzenie sieci VPN w oparciu o standard IPSec/IKE, funkcjonujące w trybie site-site oraz client-site.
  3. Uwierzytelnianie w sieci VPN odbywa się za pomocą certyfikatów cyfrowych wydawanych lokalnie oraz w razie potrzeby przez zewnętrzny urząd certyfikacji.
  4. Zabezpieczenie danych w sieci VPN odbywa się z użyciem mocnych algorytmów kryptograficznych (minimum AES-256).
  5. Zapora musi posiadać obsługę protokołów routingu dynamicznego BGP i OSPF.
  6. Zapora ma możliwość przydziału adresu IP z lokalnej puli dla zdalnego klienta VPN.
  7. Zapora musi mieć możliwość zestawienia dwóch jednoczesnych połączeń client-to-site.
  8. Zapora ma możliwość kierowania całego ruchu sieciowego od i do zdalnego klienta VPN do Internetu przez zaporę i poddania tego ruchu kontroli przez mechanizmy inspekcji uruchomione na zaporze.
  9. Zapora musi zapewniać możliwość pracy w trybie L2 (bridge), transparent oraz w trybie L3.
  10. Zapora musi posiadać moduł wykrywania intruzów IPS zapewniający wykrywanie i blokowanie ataków w czasie rzeczywistym na bazie sygnatur ataków dostarczanych przez producenta zapory.
  11. Zapora musi umożliwiać kontrolę aplikacji sieciowych używanych przez użytkowników wewnętrznych. Identyfikacja aplikacji musi się odbywać w oparciu o bazę danych aplikacji dostarczaną przez producenta rozwiązania.
  12. Zapora musi umożliwiać przeźroczyste uwierzytelnianie dla użytkowników zalogowanych do Active Directory i na podstawie tego uwierzytelniania przydział do odpowiedniej polityki bezpieczeństwa, czyli po zalogowaniu się do AD, nie jest wymagane ponowne uwierzytelnianie do firewall w celu uzyskania dostępu do zasobów sieciowych, natomiast użytkownikowi są przydzielone prawa dostępu właściwe dla użytkownika lub grupy AD.
  13. Zapora musi umożliwiać filtrowanie ruchu sieciowego pod kątem URL.
  14. Zapora musi umożliwiać wykrywanie, identyfikację i blokowanie w chronionej sieci stacji roboczych wskazujących infekcję (pobranie plików malware, komunikacją z Command&Control).
  15. Zapora musi umożliwiać kontrolę antywirusową obsługiwanego ruchu sieciowego, w czasie rzeczywistym, na podstawie bazy sygnatur wirusów.
  16. Nie ogranicza licencyjnie ilości użytkowników dla których zestawiane mogą być połączenia SSL VPN.
  17. Pojedyncze urządzenie zapory musi:

- obsługiwać nielimitowaną licencyjnie liczbę użytkowników,

- posiadać wydajność minimum 35 Gbps ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej (firewall throughput),

- posiadać wydajność minimum 9 Gbps dla ochrony NGFW (NGFW throughput – obejmujący Firewall, Application Control, IPS),

- posiadać wydajność minimum 9.6 Gbps dla ochrony IPS (IPS throughput),

- obsługiwać minimum 8 milionów jednoczesnych sesji/połączeń,

- zapewniać wydajność nawiązywania minimum 300 000 nowych połączeń na sekundę,

- posiadać co najmniej 8 fizycznych interfejsów 10/100/1000 Ethernet, minimum 8 gniazd SFP 1 Gbps oraz minimum 2 gniazda SFP+ 10 Gbps lub posiadać co najmniej 10 gniazd SFP+ 1/10 Gbps (obsługujące wkładki SFP 1Gb RJ-45). Rozwiązanie zostanie dostarczone wraz z odpowiednimi wkładkami tzn. 1Gb-SX dla gniazd SFP oraz 10Gb-SR dla gniazd SFP+,

- posiadać dedykowany dla zarządzania port, minimum port konsoli,

- posiadać minimum 2 dyski twarde o pojemności minimum 240 GB każdy,

- posiadać niezbędne komponenty do montażu w szafie rack 19”.

1.27. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

1.28. Gwarancja i wsparcie techniczne producenta w zakresie pomocy przy zgłaszaniu problemów technicznych, dostępu do bazy wiedzy, prawo pobierania poprawek, nowych wersji oprogramowania oraz subskrypcji zabezpieczeń – minimum 3 lata.

1. **System typu Sandbox.**

W ramach postępowania wymaganym jest dostarczenie rozwiązania do analizy i wykrywania zaawansowanych i nieznanych zagrożeń za pomocą technologii „sandbox”. – 1 szt.

**Architektura systemu**

Elementy systemu powinny zostać dostarczone w postaci komercyjnej platformy (lub komercyjnych platform) sprzętowej.

System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji.

System powinien umożliwiać lokalne logowanie i raportowanie.

Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń klasy NGFW (NextGeneration Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API.

Dla zapewnienia szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania.

System powinien mieć możliwość pracy w konfiguracji HA (High Availability)z podziałem obciążenia (Load Balancing).

**System operacyjny**

Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.

**Parametry fizyczne systemu**

1. System musi dysponować minimum:

* 4 portami Gigabit Ethernet RJ-45.

1. Przestrzeń dyskowa - minimum 1 x 1TB.
2. Zasilanie z sieci 230V/50Hz.

**Parametry wydajnościowe**

1. System musi zapewniać możliwość detonacji 50 000 obiektów dziennie (2000 obiektów na godzinę) lub następujące rozwiązanie: system musi pozwalać na analizę w maszynach wirtualnych min. 120 plików na godzinę i musi pozwalać na skanowanie w ruchu rzeczywistym min. 500 plików na godzinę.
2. System musi zapewniać możliwość uruchomienia min. 6 jednoczesnych instancji (jednoczesna analiza 6 różnych próbek w ramach „pełnego sandboxingu”) maszyn wirtualnych.

**Funkcje podstawowe i uzupełniające**

1. System musi umożliwiać „pełny sanboxing”, tzn. wykonanie w maszynie wirtualnej dla następujących rodzajów próbek znajdujących się w wiadomościach pocztowych: adres URL, dokumenty Microsoft Office, pliki wykonywalne (w tym języki skryptowe JavaScript, Visual Basic, bat), pliki PDF (Adobe Acrobat), pliki SWF (Adobe Flash).
2. Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.
3. Procesowanie plików o rozmiarze co najmniej 32 MB.
4. Sanboxing dla plików zarchiwizowanych (.tar, .gzip, .zip, .rar), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR).
5. Skanowanie stron www z linkami URL.
6. Czarne i białe listy dla sum kontrolnych plików.
7. Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci. Administrator powinien mieć możliwość definiowania cyklicznych raportów.
8. Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap.
9. System musi umożliwiać generowanie alertów podczas wykrywania zagrożeń i raportowanie ich za pomocą: Syslog, SNMP, SMTP.
10. System musi umożliwiać zarządzanie min. przez panel WebUI za pomocą przeglądarki internetowej.

# **Sygnatury, subskrypcje**

1. Bazy sygnatur wykorzystywanych przez funkcje skanujące powinny być systematycznie aktualizowane.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych na okres **minimum** 36 miesięcy.

**Gwarancja oraz wsparcie**

1. System musi być objęty serwisem gwarancyjnym producenta przez okres **minimum** 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.

**Gwarancja i wsparcie techniczne**

Gwarancja i wsparcie techniczne producenta w zakresie pomocy przy zgłaszaniu problemów technicznych, dostępu do bazy wiedzy, prawo pobierania poprawek, nowych wersji oprogramowania oraz subskrypcji zabezpieczeń – minimum 3 lata.

Wykonawca przeprowadzi instruktarz stanowiskowy dla 3 pracowników Zamawiającego w zakresie obsługi administracyjnej dostarczonych rozwiązań. Wykonawca zrealizuje sesję trwającą 3 dni. W sesji będzie brało udział 3 pracowników Zamawiającego.

Sesja instruktarzowa będzie prowadzona w miejscu wskazanym przez Wykonawcę.

Wszystkie koszty instruktarzu stanowiskowego pokrywa wykonawca. Dla sesji odbywającej się poza miejscem instalacji systemów Wykonawca pokrywa koszt wyżywienia oraz noclegów.

W przypadku ogłoszenia na terenie RP stanu epidemii Zamawiający dopuszcza przeprowadzenie Instruktażu stanowiskowego w trybie zdalnym tj. online za pomocą środków komunikacji elektronicznej. Szkolenie online będzie trwało 3 dni. Każda sesja instruktażowa będzie trwała minimum 6 godzin.