1. Wymagania ogólne dla NGFW – sztuk 1.

1) Firewall musi być dostarczony w postaci dedykowanego rozwiązania sprzętowo-programowego – tzw. appliance.
2) Minimalne wymagania wydajnościowe:
   a. 8,5 Gbps przepustowości Firewall/kontroli aplikacji;
   b. 3 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
   c. 4,5 Gbps dla IPsec VPN;
   d. 900 000 jednoczesnych sesji;
   e. 90 000 nowych połączeń na sekundę;
   f. 1500 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
   g. 5 wirtualnych routerów posiadających odrębne tabele routingu;
   h. Minimum 5 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.
   i. minimum 100 stref bezpieczeństwa;
   j. Lokalna przestrzeń pamięci co najmniej o pojemności 120GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi)

3) Minimalne parametry sprzętowe oferowanego urządzenia:
   a. Wysokość maksymalnie 1U wraz z zestawem montażowym do szafy RACK 19”;
   b. 8 portów 1-GigabitEthernet RJ45 (dopuszcza się uzyskanie tych portów poprzez zastosowanie portów 1 GigabitEthernet SFP obsadzonych modułami z RJ45)
   c. 4 porty 1G/2,5G/5G lub 4 porty 1G/10G RJ45
   d. 4 porty 10 GigabitEthernet SFP+ obsługujące moduły optyczne SR oraz LR
   e. 6 porty 1 GigabitEthernet SFP obsługujące moduły optyczne SX oraz LX
   f. 1 port 1-GigabitEthernet RJ45 lub 10-GigabitEthernet RJ45 wyłącznie do celów zarządzania (dopuszcza się uzyskanie tego portu poprzez zastosowanie portów SFP / SFP+ obsadzonych modułami z RJ45)
   g. Urządzenie musi posiadać port (10GE lub szybsze) dla celów połączenia urządzeń w klaster (high availability). Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.

h. Porty 10 GigabitEthernet SFP+ mają być obsadzone 4szt wkładkami LR 10Gbs 1310nm LC DDM SMF

i. Porty 1 GigabitEthernet SFP mają być obsadzone 6szt wkładkami SFP 1.25Gbps LX 1310nm LC DDM SMF

III. Wymagania funkcjonalne dla rozwiązań NGFW

UWAGA: Wszystkie wymienione poniżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.

Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

Cechy NGFW

1) Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 4000 aplikacji predefiniowanych przez Producenta.
2) Transparentne ustalenie tożsamości użytkowników
3) Realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:
    a) Intrusion Prevention System (IPS),
    b) Antywirus (AV),
    c) Anty-Spyware / Anty-Malware ,
    d) Kategoryzacja URL i filtracja URL
    e) ochrona DNS,
    f) sandbox lokalny lub chmurowy tego samego producenta
4) Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory
5) System musi zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji

Silniki detekcyjne i ochronne NGFW

1) Bazy sygnatur IPS, AV, Anty-Spyware (lub innego silnika, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, regularnie aktualizowane w sposób automatyczny.

2) Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.

3) Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.

4) Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa. Nie dopuszcza się by IPS i AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego, gdzie administrator nie ma możliwości konfiguracji jaka część ruchu będzie podlegała inspekcji i w jakim zakresie.

5) Wykrywanie aktywności sieci typu Botnet.

6) Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.

7) Funkcja filtrowania ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron.

   a) Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp)

   b) Ocena strony musi obejmować określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie).

   c) Musi być zapewniona możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta z możliwością konfiguracji, gdzie własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.

8) Funkcja ochrony przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem

   a) możliwość przesyłania do systemu sandbox (tego samego producenta co firewall) plików zdefiniowanych przez administratora (co najmniej exe, dll, java, MS Office, pdf). Zamawiający dopuszcza by odbywało się to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy

b) możliwość aktualizacji systemu firewall o nowo wykryte (w Sandbox) zagrożenia. Aktualizacje muszą być dystrybuowane niezwłocznie i na bieżąco, to znaczy bezpośrednio po ich wykryciu przez producenta. Nie jest dopuszczalne aby aktualizacje systemu firewall odbywały się w trybie regularnych uaktualnień publikowanych przez producenta np. co 24 godziny.

c) administrator musi posiadać dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również posiadać możliwość manualnego wysłania pliku (np. poprzez upload przez stronę www) do sandboxa.

d) dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym firewallem

e) Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 20 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery).

f) Jednoczesna analiza 20 próbek/plików musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie przez firewall czy manualnie przez administratora czy też będzie to mieszana grupa plików pochodząca zarówno bezpośrednio z firewalla, jak też od administratorów

9) Podstawowa ochrona DNS co najmniej w zakresie:

a) wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 10 milionów wpisów.

b) możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

Deszyfracja ruchu

1) Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:

a. Realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 1,2 Gbps inspekcji TLS dla sesji http 64K,

b. Jest wyposażone w co najmniej 2 interfejsy 10GigabitEthernet SFP+

c. Musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla.

d. W przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.

Obsługa VPN oraz funkcji sieciowych

1) Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.

2) Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.

a. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 1500 tuneli/użytkowników.

b. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS

c. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla.

d. Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 5000 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 10000.

3) Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4;

4) Obsługa 4094 VLAN zgodnych z 802.1q.

5) Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.

6) Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.

7) Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.

8) Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

Uwierzytelnienie i ustalanie tożsamości użytkowników

1) Transparentne ustalenie tożsamości w oparciu o:

a. integrację z kontrolerem domeny Active Directory;

b. integrację z serwerami LDAP;

c. integrację z serwerami terminalowymi;

d. integrację bazującej na informacji z logów SYSLOG lub RADIUS pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX;

2) Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.

3) MInimalne wymagane mechanizmy uwierzytelnienia administratorów NGFW:

   a. baza lokalna

   b. zewnętrzna usługa katalogowa dostępna po LDAPS;

   c. RADIUS lub TACACS+.

Zarządzenie urządzeniami NGFW

1) Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora – bez konieczności korzystania z centralnych narzędzi zarządzania.

2) Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.

3) Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

IV. Interpretacja parametrów wydajnościowych NGFW

1) Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwoli na:

   a. wykrycie aplikacji,

   b. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.

2) Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware - rozwiązanie pozwoli na

   a. wykrycie aplikacji,

   b. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,

   c. inspekcje IPS całego ruchu,

d. inspekcję antywirusową całego ruchu,

e. inspekcję antymalware/AntySpyware całego ruchu,

f. przesyłanie plików do sandboxa lokalnego i/lub chmurowego,

g. przechwytywanie i blokowanie plików określonego typu.

h. Logowanie zdarzeń

Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

3) Charakterystyka ruchu sieciowego dla interpretacji parametrów wydajnościowych.

Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na oferowanym firewallu zakładają, iż będą to parametry wskazane przez producentów w dokumentacji (lub testach) jako inspekcja http z wielkością sesji 64KB lub mniejszą wartością np. http 44KB, 40KB – zależnie od tego jaki parametr sesji http przyjął producent urządzenia firewall do określenia jego parametrów.

W przypadku gdy Wykonawca zaproponuje urządzenie, którego wydajność nie będzie wskazana w oficjalnej i publicznie dostępnej dokumentacji wówczas jest on zobowiązany do dodatkowego potwierdzenia spełnienia wymagań wydajnościowych. Zamawiający wymaga, aby potwierdzenie zostało dostarczone w postaci wyników testów przeprowadzonych przez publiczny ośrodek badawczo-rozwojowy w Polsce z wykorzystaniem dedykowanych testerów ruchu – IXIA lub Spirent lub Agilent.

V. WYMAGANIA LICENCYJNE

1) Całość rozwiązania będzie pochodziła od jednego producenta.

2) W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 36 miesięcy.

3) Dla systemu firewall należy dostarczyć usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla następujących funkcji:

   a. Aktualizacje bazy aplikacji;

b. Aktualizacje baz sygnatur IPS;

c. Aktualizacje baz sygnatur AV;

d. Możliwość współpracy z systemem sandbox;

e. Aktualizacji baz dla podstawowej ochrony DNS;

f. realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN);

Warunki Gwarancyjne

1. gwarancja producenta oparta o świadczenia gwarancyjne producenta sprzętu Wykonawcy przez okres minimum 36 miesięcy
2. . 36 miesięczny serwis gwarancyjny od daty odbioru sprzętu.
3. Serwis gwarancyjny świadczony w miejscu instalacji sprzętu przez Wykonawcę
4. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin
5. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 1 dnia roboczego od momentu zgłoszenia usterki w trybie 8x5xnbd.
6. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku.
7. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę).