ZAŁĄCZNIK NR 5 DO SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem Zamówienia jest dostarczenie systemu bezpieczeństwa typu firewall wraz z oprogramowaniem do zarządzania, logowania i raportowania i niezbędną infrastrukturą techniczną, zapewnienie subskrypcji i serwisu w Porcie Lotniczym Gdańsk Sp. z o.o.

Przedmiot zamówienia obejmuje dostawę:

a) urządzeń typu next-generation firewall firmy Palo Alto Networks, numer katalogowy PAN-PA-5220-AC – 2 sztuki
b) wsparcie techniczne i serwis producenta w/w urządzeń obejmujący naprawę lub wymianę sprzętu, usuwanie usterek w oprogramowaniu systemowym oraz aktualizacje tego oprogramowania przez okres 3 lat od podpisania przez Zamawiającego Protokołu Odbioru Systemu – PAN-SVC-BKLN-5220 - 2 sztuki
c) subskrypcji Threat Prevention do w/w urządzeń na okres 3 lat od podpisania przez Zamawiającego Protokołu Odbioru Systemu, numer katalogowy PAN-PA-5220-TP--HA2 – 2 sztuki
d) subskrypcji PANDB URL filtering do w/w urządzeń na okres 3 lat od podpisania przez Zamawiającego Protokołu Odbioru Systemu, numer katalogowy PAN-PA-5220-URL4-HA2 – 2 sztuki
e) subskrypcji WildFire do w/w urządzeń na okres 3 lat od podpisania przez Zamawiającego Protokołu Odbioru Systemu, numer katalogowy PAN-PA-5220-WF-HA2 – 2 sztuki
f) subskrypcji Globalprotect do w/w urządzeń na okres 3 lat , numer katalogowy PAN-PA-5220-GP-HA2 – 2 sztuki
g) oprogramowania Panorama central management w wersji do 25 urządzeń, numer katalogowy PAN-PRA-25
h) serwisu wsparcia dla oprogramowania Panorama, Partner Enabled Premium Support na okres 3 lat od podpisania przez Zamawiającego Protokołu Odbioru Systemu, numer katalogowy PAN-SVC-BKLN-PRA-25

<u>Opis wymagań technicznych i funkcjonalnych dotyczący firewalli</u>

Wymagania ogólne

1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance).
2. System zabezpieczeń firewall musi zapewniać wewnętrzne wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym.
3. System zabezpieczeń firewall musi umożliwiać działanie w następujących trybach pracy
    a. routera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (tzn. w warstwie 2 modelu OSI),
    c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych

adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
   d. w trybie pasywnego nasłuchu (sniffer).
4. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).
5. System zabezpieczeń firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active.
6. System zabezpieczeń firewall w dostarczanej konfiguracji musi obsługiwać nie mniej niż 10 wirtualnych systemów. Każdy system wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
   a. tablic routingu przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.
   b. Polityk bezpieczeństwa obejmujących
      i. System IPS
      ii. System ochrony antymalware/antyspyware
      iii. System ochrony antywirus
   c. Koncentratorów VPN dla zdalnego dostępu
7. Dostarczane urządzenia muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
8. Urządzenia muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
9. Urządzenia i inne świadczenia Wykonawcy składające się na przedmiot zamówienia oraz Wykonawca muszą spełniać wszystkie wymogi określone prawem.

Wymagania dot. Platformy

1. System zabezpieczeń firewall musi być wyposażony w co najmniej następujące interfejsy sieciowe
   a. 4 miedziane porty Ethernet 100/1G/10G,
   b. 16 portów 1G/10G SFP/SFP+,
   c. 4 porty 40G QSFP+.
2. System zabezpieczeń firewall musi być wyposażony w co najmniej jeden port konsoli
3. System zabezpieczeń firewall musi być wyposażony w co najmniej jeden port zarządzający Out-of-Band 10/100/1000
4. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
5. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 20 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,
6. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 8,9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-

spyware, IPS i web filtering)

7. System zabezpieczeń firewall musi obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 133 000 połączeń na sekundę.
8. System zabezpieczeń firewall musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 10Gbps.
9. System zabezpieczeń firewall musi posiadać wbudowane w obudowę co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V.

Podstawowe wymagania funkcjonalne

1. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
2. Polityka zabezpieczeń firewall musi uwzględniać
    a. strefy bezpieczeństwa,
    b. adresy IP klientów i serwerów,
    c. protokoły i usługi sieciowe,
    d. aplikacje,
    e. kategorie URL,
    f. użytkowników aplikacji,
    g. reakcje zabezpieczeń,
    h. rejestrowanie zdarzeń i alarmowanie
    i. zarządzanie pasmem w sieci w oparciu o
        i. priorytet,
        ii. pasmo gwarantowane,
        iii. pasmo maksymalne,
        iv. oznaczenia DiffServ
3. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
4. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
5. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.
6. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne

definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.

7. System zabezpieczeń firewall musi wykrywać co najmniej 2400 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
8. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
9. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antymalware, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
10. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
11. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
12. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
13. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
14. System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta musi być traktowana jako stanowiąca automatyczne wyjątki od ogólnych reguł deszyfracji.
15. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH

Wymaganie dotyczące identyfikacji użytkowników

1. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci
2. System zabezpieczeń firewall musi zapewniać integrację z
    a. Active Directory,
    b. Ms Exchange,

c. Citrix,
d. LDAP
e. serwerami Terminal Services
f. Radius (w szczególności system CERB)

3. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
4. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.
5. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

Wymagania dot. warstwy sieci

1. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
2. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
3. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
4. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
5. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
6. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania

definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.

a. Polityki definiujące powinny umożliwiać wykorzystanie
    i. adresów źródłowych,
    ii. adresów docelowych,
    iii. użytkowników,
    iv. numerów portów usług
    v. kategorie URL.
b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia
    i. RADIUS,
    ii. TACACS+,
    iii. LDAP,
    iv. Kerberos,
    v. SAML 2.0.

7. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
8. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników lub grupy użytkowników.
9. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

Wymagania dotyczące zaawansowanych systemów ochrony

1. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
2. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
3. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
4. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
5. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek

komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

6. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
7. System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. __
8. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
9. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
10. System zabezpieczeń firewall musi posiadać moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
11. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja antymalware lub antyspyware uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
12. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur antymalware lub antyspyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
13. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
14. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
15. System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
16. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP

hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

17. System zabezpieczeń firewall musi umożliwiać (np. w ramach modułu filtracji stron WWW) zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
18. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
19. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
20. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
21. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".
22. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
23. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

Wymagania dotyczące zarządzania

1. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
2. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania

wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

3. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
4. System zabezpieczeń firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmiany w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. W innych systemach wirtualnych
5. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
6. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
7. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
8. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
9. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
10. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się aby do tego celu konieczny był zakup zewnętrznych urządzeń, oprogramowania ani licencji.
11. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
12. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
13. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
14. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
15. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
16. System zabezpieczeń firewall musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:

a. ruchu sieciowym,
b. aplikacjach,
c. zagrożeniach
d. filtrowaniu stron www.

17. System zabezpieczeń firewall musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
18. System zabezpieczeń firewall musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
19. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Wymagania dotyczące wsparcia technicznego

1. Pomoc techniczna musi być świadczona w języku polskim. Wsparcie musi być świadczone w wersji premium.
2. W ramach wsparcia technicznego Wykonawca zapewni utrzymywanie, aktualizacje oraz udostępnianie Zamawiającemu oprogramowania za pośrednictwem strony internetowej wsparcia.
3. W ramach wsparcia technicznego Zamawiający musi mieć dostęp 24/7/365 do specjalistów produktowych z możliwością kontaktu telefonicznego, e-mail, poprzez narzędzia web i forum społecznościowe.
4. W ramach wsparcia technicznego Zamawiający będzie miał dostęp do instrukcji produktowych, przewodników technicznych, notatek serwisowych oraz FAQs. Wsparcie techniczne będzie obejmowało także subskrypcje do aktualizacji serwisowych, łaty programowe i aktualizacje właściwości oraz wsparcie platformy sprzętowej.
5. W ramach wsparcia technicznego Wykonawca zapewni Zamawiającemu weryfikację i usuwanie błędów oprogramowania zgłaszanych przez Zamawiającego.
6. Elementem wsparcia jest także usługa wymiany sprzętu - dostawa na następny dzień.
7. Określa się następujące czasy reakcji na zgłoszenia:
   Priorytet 1 - krytyczny <1h – awaria skutkująca całkowitą niesprawnością systemu, która krytycznie wpływa na środowisko produkcyjne Zamawiającego
   Priorytet 2- wysoki 2h – awaria skutkująca częściową niesprawnością systemu, mająca negatywny wpływ na środowisko produkcyjne Zamawiającego
   Priorytet 3- średni 3h – awaria systemu nie mająca negatywnego wpływu na środowisko produkcyjne Zamawiającego
   Priorytet 4 - niski 8h pracujących – awarie nie mające negatywnego wpływu na działalność prowadzoną przez Zamawiającego; ten czas reakcji ma również zastosowanie do udzielania Zamawiającemu informacji, porad, przesyłania dokumentacji

Przez godziny pracujące rozumie się godziny od 7:00 do 18:00 w dniach od poniedziałku do piątku, z wyjątkiem dni ustawowo uznanych za wolne od pracy.

System zarządzania, logowania i raportowania PANORAMA

Wymagania ogólne

1. Wraz z systemem zabezpieczeń firewall konieczne jest dostarczenie centralnego systemu zarządzania.
2. System zarządzania, logowania i raportowania musi obsługiwać docelowo nie mniej niż 25 firewalli.
3. System zarządzania, logowania i raportowania musi obsługiwać przestrzeń dyskową do przechowywania logów o pojemności nie mniejszej niż 2 TB.
4. System zarządzania, logowania i raportowania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie.
5. System zarządzania, logowania i raportowania musi posiadać taki sam Graficzny Interfejs Użytkownika (GUI) jak zarządzane firewalle.
6. System zarządzania, logowania i raportowania musi umożliwiać import obecnej konfiguracji używanych firewalli.
7. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
8. System zarządzania, logowania i raportowania musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
9. System zarządzania, logowania i raportowania musi umożliwiać dedykowane narzędzia dla łatwego przeszukiwania skorelowanych logów zebranych z zarządzanych firewalli.
10. System zarządzania, logowania i raportowania musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
11. System zarządzania, logowania i raportowania musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
12. System zarządzania, logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”.
13. System zarządzania, logowania i raportowania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) i globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).
14. System zarządzania, logowania i raportowania musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie

ustawień sieciowych, wykorzystanie tych samych obiektów).

15. System zarządzania, logowania i raportowania musi umożliwiać tworzenie raportów na podstawie zbudowanych kontenerów.
16. System zarządzania, logowania i raportowania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
17. System zarządzania, logowania i raportowania musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.
18. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
19. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek.
20. System zarządzania, logowania i raportowania musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli.
21. System zarządzania, logowania i raportowania musi pozwalać na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu konsoli zarządzającej.
22. System zarządzania, logowania i raportowania musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
23. System zarządzania, logowania i raportowania musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne).
24. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
25. System zarządzania, logowania i raportowania musi informować o zmianach konfiguracji systemu.
26. System zarządzania, logowania i raportowania musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem.
27. System zarządzania, logowania i raportowania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.
28. System zarządzania, logowania i raportowania musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak, aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone.
29. System zarządzania, logowania i raportowania musi być dostarczony jako tzw. wirtualny appliance do uruchomienia jako maszyna wirtualna w środowisku Vmware

Wymagania dotyczące wsparcia technicznego

30. Pomoc techniczna musi być świadczona w języku polskim. Wsparcie musi być świadczone w wersji premium.
31. W ramach wsparcia technicznego Wykonawca zapewni utrzymywanie, aktualizacje oraz udostępnianie Zamawiającemu oprogramowania za pośrednictwem strony internetowej wsparcia.
32. W ramach wsparcia technicznego Zamawiający musi mieć dostęp 24/7/365 do

specjalistów produktowych z możliwością kontaktu telefonicznego, e-mail, poprzez narzędzia web i forum społecznościowe.

33. W ramach wsparcia technicznego Zamawiający będzie miał dostęp do instrukcji produktowych, przewodników technicznych, notatek serwisowych oraz FAQs. Wsparcie techniczne będzie obejmowało także subskrypcje do aktualizacji serwisowych, łaty programowe i aktualizacje właściwości oraz wsparcie platformy sprzętowej.
34. W ramach wsparcia technicznego Wykonawca zapewni Zamawiającemu weryfikację i usuwanie błędów oprogramowania zgłaszanych przez Zamawiającego.
35. Określa się następujące czasy reakcji na zgłoszenia:
    Priorytet 1 - krytyczny <1h – awaria skutkująca całkowitą niesprawnością systemu, która krytycznie wpływa na środowisko produkcyjne Zamawiającego
    Priorytet 2- wysoki 2h – awaria skutkująca częściową niesprawnością systemu, mająca negatywny wpływ na środowisko produkcyjne Zamawiającego
    Priorytet 3 - średni 3h – awaria systemu nie mająca negatywnego wpływu na środowisko produkcyjne Zamawiającego
    Priorytet 4 - niski 8h pracujących – awarie nie mające negatywnego wpływu na działalność prowadzoną przez Zamawiającego; ten czas reakcji ma również zastosowanie do udzielania Zamawiającemu informacji, porad, przesyłania dokumentacji

Przez godziny pracujące rozumie się godziny od 7:00 do 18:00 w dniach od poniedziałku do piątku, z wyjątkiem dni ustawowo uznanych za wolne od pracy.