Załącznik nr 1a do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy postępowania o udzielenie zamówienia publicznego na:

„Wyposażenie serwerowni Centrum Komiksu i Narracji Interaktywnej”
Numer postępowania: 206/DIM/PN/2020

Zadanie 1

Dostawa urządzeń klasy UTM wraz z wdrożeniem, konfiguracją i uruchomieniem

Spis treści

I. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa urządzeń klasy UTM wraz z wdrożeniem, konfiguracją i uruchomieniem. Zakresem zamówienia objęte są urządzenia klasy UTM (2 urządzenia) do zabezpieczenia połączeń sieci LAN do sieci Internet oraz z sieci Internet do sieci LAN wraz z wdrożeniem, konfiguracją i uruchomieniem.

II. Wdrożenie

Czynności wdrożeniowe obejmują wykonanie co najmniej następujących czynności:

1. Analiza środowiska sieci L2/L3
2. Analiza obecnej konfiguracji urządzeń posiadanych przez Zamawiającego
3. Przygotowanie projektu wdrożenia
4. Migracja konfiguracji do nowych urządzeń z uwzględnieniem zmian
5. Aktualizacja oprogramowania na nowych urządzeniach do rekomendowanej przez producenta wersji oprogramowania
6. Konfiguracja i testy klastra HA nowych urządzeń umieszczonych w dwóch serwerowniach
7. Audyt poprawności konfiguracji, zgodnie z wymaganiami Zamawiającego
8. Weryfikacja poprawności przeniesienia konfiguracji
9. Wykonanie planu przepięcia urządzeń
10. Przepięcie urządzeń, monitoring i wsparcie w ciągu 7 dni od dnia dokonania czynności przepięcia
11. Konfiguracja funkcjonalności ochrony antywirusowej
12. Konfiguracja funkcjonalności ochrony IPS
13. Konfiguracja funkcjonalności kontroli aplikacji
14. Konfiguracja funkcjonalności DLP lub tożsamej do wymagań
15. Konfiguracja funkcjonalności ochrony usług wystawianych do sieci Internet
16. Konfiguracja funkcjonalności kontroli przepustowości pasma
17. Konfiguracja funkcjonalności dostępu do sieci z wykorzystaniem SSL VPN
18. Konfiguracja funkcjonalności rozszywania SSL dla ruchu wyjściowego do Internetu
19. Wykonanie dokumentacji powykonawczej

III. Minimalne wymagania techniczne - Urządzenia UTM

III.1 Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Nie dopuszcza się, aby poszczególne elementy, wchodzące w skład systemu bezpieczeństwa, pochodziły od różnych producentów. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu,

Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 co najmniej w zakresie:

- Firewall
- Ochrony w warstwie aplikacji
- Protokołów routingu dynamicznego

III.2 Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach umowy system musi zostać dostarczony w postaci redundantnej.
3. System klastrowania musi pozwalać na dalszą rozbudowę do 4 urządzeń pracujących w trybie Active-Active.
4. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
5. Monitoring stanu realizowanych połączeń VPN Site-to-Site oraz Client-to-Site.
6. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

III.3 Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB oraz zapisanie/odczytanie konfiguracji urządzenia.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania 1024 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie redundantne AC.
5. System firewall powinien być wyposażony w co najmniej jeden dysk SSD o pojemności nie mniejszej niż 200GB.

III.4 Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 65.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla ruchu Enterprise Mix.
3. Przepustowość Firewall z włączoną funkcją Threat Prevention : nie mniej niż 1.8 Gbps dla ruchu Enterprise Mix.
4. Wydajność szyfrowania VPN IPSec dla pakietów opisanych RFC 3511, 2544, 2647, 1242 przy zastosowaniu algorytmu o mocy nie mniejszej niż AES128 – SHA1: nie mniej niż 2.57 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Mix - minimum 4,5 Gbps.

Wyniki wydajności skanowania muszą być podane dla testów gdzie skanowana jest cała sesja.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami NGFW (FW, IPS, Application Control) - minimum 3.7 Gbps. Wyniki wydajności skanowania muszą być podane dla testów gdzie skanowana jest cała sesja.

III.5 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:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
2. Kontrola Aplikacji
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS, SMBv3
5. Ochrona przed atakami - Intrusion Prevention System
6. Kontrola stron WWW
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP
8. Zarządzanie pasmem (QoS, Traffic shaping)
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (Zarządzanie zawartością danych, DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych w ramach połączeń VPN typu client-to-site
11. Analiza ruchu szyfrowanego protokołem SSL
12. Analiza ruchu szyfrowanego protokołem SSH

III.6 Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

III.7 Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać co najmniej:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługę protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh
   - 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.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać co najmniej:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.
   - Pracę w trybie Tunnel - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.

III.8 Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę co najmniej:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
3. System musi umożliwiać sterowaniem ruchem dla co najmniej 2 łączy WAN poprzez reguły PBR (Policy Base Routing), w których można wykorzystać zdefiniowane reguły z polityki bezpieczeństwa na FW.

III.9 Zarządzanie pasmem

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

III.10 Inspekcja ruchu szyfrowanego

1. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
2. 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. Każda polityka bezpieczeństwa może posiadać odrębny zestaw polityk deszyfracji SSL.

3. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
4. Nie dopuszczalne jest, aby system do deszyfracji SSH używał jednego globalnego klucza deszyfrującego. Takie podejście będzie uznane za potencjalną dziurę bezpieczeństwa i nie będzie zaakceptowane.

III.11 Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR, 7-zip.
3. System inspekcji antywirusowej powinien wspierać analizę dla ruchu http, https, smtp, imap, pop3, ftp, cifs, SMBv3 (multi-channel), kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

III.12 Ochrona typu Sandbox

1. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do chmurowego lub lokalnego systemu typu „SandBox" plików różnych typów (exe, dll, pdf, Ms-Offfice, jar, flash, rar, MacOSX, Linux, JScript, PowerShell, Shell Scripts, VBScript). System „SandBox" musi pochodzić od tego samego producenta.
2. System zabezpieczeń firewall musi posiadać funkcję, zatrzymania pliku na urządzeniu do momentu wydania werdyktu przez system typu „SandBox". Nie dopuszczalne jest, aby plik transportowany z Internetu do użytkownika miałby możliwość pojawienia się na urządzeniu bez otrzymania werdyktu o pliku.
3. Integracja z chmurowym systemem typu „SandBox" musi pozwalać administratorowi na podjęcie decyzji o podziale typów plików, przesyłanych do chmurowych lub lokalnych systemów typu „SandBox". System „SandBox" musi pochodzić od tego samego producenta.
4. System zabezpieczeń firewall współpracujący z systemem „SandBox" musi posiadać wsparcie dla przechwytywanych plików większych niż 10Mb (Megabajt). Nie dopuszczalne jest ograniczanie wspieranej wielkości plików poniżej 10Mb.

III.13 Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrona IPS musi być wykonywana dla całej sesji. Nie dopuszcza się rozwiązań określających bezpieczeństwo sesji poprzez szczątkową analizę ruchu podczas ustanawiania sesji.
3. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

4. Baza sygnatur ataków powinna zawierać minimum 10000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora bezpośrednio na urządzeniu.
5. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
6. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
7. System powinien posiadać mechanizm automatycznego dodawania adresu IP do czarnej listy (z ang. Black list) w przypadku spełnienia warunku naruszenia zasad bezpieczeństwa wykrytych przez moduł IPS/IDS.
8. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injection, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
9. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
10. 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. Blackhole DNS).
11. Ochrona IPS musi udostępniać mechanizmy dodawania oraz aktywowania nowych definicji pobranych z aktualizacji IPS.
12. Ochrona IPS musi dostarczać mechanizm wykluczania elementów sieciowych na bazie źródła, celu, serwisu oraz kombinacji tych trzech elementów.

III.14 Kontrola aplikacji

1. System musi zapewniać funkcję kontroli aplikacji, która powinna umożliwiać kontrolę ruchu, na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. System musi zapewniać bazę kontroli aplikacji, która powinna zawierać minimum 7500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
6. Rozwiązanie musi dostarczać narzędzia do tworzenia dodatkowych definicji aplikacji.

III.15 Kontrola przepływu danych

1. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików w obu kierunkach, nie mniej niż: bat, cab, dll, doc, szyfrowany zip, docx, xlsx, pptx, pdf, jpg,

jpeg, exe, com, dll, drv, pif, qts, qtx, sys, scr, vbx, vxd, gif, png, tiff, asf, wmv, wma, mp3, 7f, mdb, accdb, dbf, db, ras, bmp, xpm, psd, ps, dwg, rtf, rar, gz, tgz, tar.gz, tar.z, bz2, tar.bz2, tbz2, tb2, jar, lha, lzh, arc, kgb, xy, reg, rpm, arj, bh, zoo, cpio, ace, deb, avi, wmf, rm, rv, emf, pbm, pgm, ppm, gem, xml, doc, ppt, xls, swf, mov, mp4, mpeg, flv, dwf, mkv, js, css, wav, pak, tar, mdg, oft, eml, pst, odt, ott, ods, ots, odg , otg, odp, otp, odi, oti, ico, wks, wk1, wk2, wk3, wk4, wk5, 123, dxf, hwp, one, webp, Zip (compressed using BZip2), Zip (compressed using Deflate64), Zip (compressed using LZMA), Zip (compressed using PPMD), html, xhtml, phtml, htm. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka, a nie na podstawie rozszerzenia.

2. Kontrola przepływu danych musi odbywać się dla całego ruchu.
3. Musi być możliwe tworzenie oddzielnych reguł kontroli ruchu bezpieczeństwa dla zadanej aplikacji.
4. Rozwiązanie musi dostarczać mechanizmy tworzenia definicji nowych typów plików.

III.16 Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy adresów URL, pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW, powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: Malicious Sites (lub inne będące źródłem złośliwego oprogramowania), Phishing, Spam.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. System zabezpieczeń firewall powinien posiadać funkcję ochrony przed atakami wykorzystującymi protokół DNS, m.in. przesyłanie wykradzionych danych lub komunikacja z serwerem C&C przez DNS (DNS tuneling).

III.17 Zarządzanie tożsamością użytkowników – uwierzytelnianie użytkowników w ramach sesji

1. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z MS Active Directory, MS Exchange, Citrix, LDAP i serwerami Terminal Services). 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. W przypadku użytkowników pracujących w środowisku terminalowym, a tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
2. 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 sesję, w przypadku gdy

analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

3. Urządzenie musi posiadać funkcjonalność współdzielenia tożsamości między systemami firewall pochodzącymi od tego samego producenta, jednakże zarządzanymi poprzez odrębne domeny zarządzania.
4. System Firewall musi umożliwiać weryfikację tożsamości użytkowników co najmniej 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.
5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

III.18 Zarządzanie Systemem Firewall

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalną konfiguracją z wykorzystaniem protokołów: HTTPS oraz SSH oraz muszą być zarządzane poprzez centralny system zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego Wykonawca zobowiązany będzie udostępnić dokumentację na żądanie Zamawiającego, w trakcie trwania okresu gwarancji.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, hping, hping2, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

III.19 Serwer zarządzania – wymagania ogólne

1. System zarządzania musi być dostarczony jako osobny element w celu zcentralizowania prac nad politykami bezpieczeństwa.
2. Serwer zarządzania musi mieć możliwość zarządzania minimum dwoma punktami wymuszania polityki bezpieczeństwa (zapora sieciowa).
3. Serwer zarządzania musi umożliwiać jednoczesną pracę wielu administratorów - w tym także jednoczesną pracę w ramach pojedynczej polityki bezpieczeństwa.

4. Serwer zarządzania musi zapewniać możliwość tworzenia wielu różnych polityk bezpieczeństwa oraz umożliwiać ich przypisanie do poszczególnych zapór sieciowych zarządzanych z poziomu serwera.
5. Serwer zarządzania musi umożliwiać tworzenie modułowej polityki bezpieczeństwa. System musi umożliwiać współdzielenie modułów (zestawów reguł polityki bezpieczeństwa) pomiędzy różnymi politykami bezpieczeństwa.
6. Serwer zarządzania musi posiadać mechanizmy automatycznej weryfikacji spójności i niesprzeczności implementowanej polityki bezpieczeństwa przed zainstalowaniem jej na zaporze sieciowej.
7. Serwer zarządzania musi posiadać mechanizmy pozwalające na weryfikację poprawności działania nowej wersji polityki bezpieczeństwa po jej uruchomieniu na zaporze sieciowej oraz możliwość automatycznego powrotu do poprzedniej wersji w przypadku stwierdzenia nieprawidłowości na bazie zestawu testów utworzonych przez administratora - np. brak dostępu do wybranych usług powstały w wyniku błędu administratora
8. Serwer zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa, a także opcję cofnięcia konfiguracji do wybranej wersji.
9. Serwer zarządzania musi zapewniać możliwość uwierzytelniania administratorów za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych.
10. Serwer zarządzania musi zapewniać możliwość definiowania szczegółowych zestawów uprawnień dla poszczególnych administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkownikami).
11. Serwer zarządzania musi posiadać mechanizmy zapewniające rozliczalność zmian konfiguracyjnych wykonanych przez poszczególnych administratorów w formie generowania i przechowywania logów audytowych. Logi muszą zawierać minimum informacje o tożsamości administratora oraz czasie i zakresie wykonywanych zmian.
12. Serwer zarządzania musi posiadać mechanizmy centralnego zarządzania licencjami dla wszystkich komponentów wchodzących w skład systemu bezpieczeństwa (serwery logów, serwer korelacji zdarzeń i raportowania, zapory sieciowe).
13. Serwer zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych zapór sieciowych takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa.
14. Serwer zarządzania musi dostarczać mechanizmy pozwalające na graficzne prezentowanie statystyk ruchu sieciowego, przetwarzanego przez zarządzane zapory sieciowe. Dostępne statystyki powinny obejmować minimum informacje o najczęściej wykorzystywanych usługach sieciowych, najczęstszych źródłach transmisji,

najczęstszych adresach docelowych, aktywnych i nieaktywnych tunelach IPSec VPN (Site-to-site oraz Remote Access).

15. Serwer zarządzania musi posiadać dedykowane API umożliwiające automatyzację czynności administracyjnych. Mechanizm API powinien umożliwiać minimum wykonanie następujących czynności:
    - tworzenie, edycja oraz usuwanie obiektów sieciowych i usług
    - tworzenie, modyfikowanie oraz usuwanie reguł polityki bezpieczeństwa oraz reguł NAT
    - instalacja polityki bezpieczeństwa
    - zarządzania kontami administratorów systemu
16. Serwer zarządzania musi posiadać wbudowane mechanizmy pozwalające na implementację rozwiązania wysokiej dostępności (HA), w ramach której możliwe jest dodanie zapasowego serwera zarządzania oraz uruchomienie automatycznej synchronizacji konfiguracji polityk bezpieczeństwa.
    UWAGA: Dostarczenie zapasowego serwera zarządzania nie jest wymagane w ramach postępowania.
17. Serwer zarządzania musi zapewniać zintegrowane zarządzanie zagrożeniami w czasie rzeczywistym, w tym: rejestrowanie, monitorowanie, logowanie zdarzeń, zarządzanie zagrożeniami oraz kontrolę zgodności z regulacjami. Musi istnieć możliwość identyfikacji i analizy zagrożeń w czasie rzeczywistym wykorzystując logi bieżące jak i logi historyczne. Musi istnieć możliwość wyszukiwania określonych wartości w całej bazie danych zdarzeń (bez potrzeby definiowania wyszukiwanych atrybutów).
18. Musi istnieć możliwość grupowania wyników wyszukiwania według poszczególnych atrybutów (typ incydentu, zasoby, nazwa użytkownika).
19. Musi istnieć możliwość zarządzania wieloma domenami. Musi istnieć możliwość utworzenia co najmniej 5 domen administracyjnych na podstawie położenia geograficznego, jednostki biznesowej lub funkcji bezpieczeństwa (licencja musi być częścią oferty).
20. Musi istnieć możliwość zwiększenia liczby domen administracyjnych w przyszłości do co najmniej 200.
21. Serwer zarządzania musi obsługiwać interfejs API dla zapewnienia automatyzacji pracy z systemem.
22. Wykonawca musi zapewniać, aby nowe wersje formatów logów były regularnie aktualizowane przez producenta urządzenia.
23. Musi istnieć możliwość analizy typu Forensics (kliknięcie na linę czasu, wykres graficzny lub mapę powinno skutkować tzw. drill-down do poziomu pakietów).
24. Logi muszą być przesyłane poprzez uwierzytelniony i szyfrowany tunel.
25. Serwer zarządzania musi zostać dostarczony z co najmniej 3 letnim wsparciem technicznym producenta.

III.20 Serwer zarządzania - widoki i raporty

1. Wszystkie widoki i raporty muszą być konfigurowalne.

2. Musi istnieć zdolność definiowania filtrów, dodawania / usuwania / dostosowywania komponentów i stron.
3. Musi istnieć możliwość tworzenia własnych widżetów, widoków i raportów lub korzystania z dowolnego predefiniowanego raportu.
4. Musi istnieć możliwość personalizowania raportów pod kątem ról, takich jak: specjalista ds. bezpieczeństwa, inżynier sieciowy, kadra kierownicza.
5. Musi istnieć możliwość dodawania niestandardowych lub predefiniowanych widoków do raportów.
6. Musi zawierać raporty i kontrole zgodności z regulacjami dla co najmniej 300 praktyk i wymogów bezpieczeństwa.
7. Musi zawierać ujednolicony widok dla wszystkich aspektów monitorowania.
8. Musi istnieć możliwość tworzenia niestandardowych widoków odzwierciedlających i wyświetlających tylko informacje istotne dla organizacji.
9. Musi graficznie wyświetlać inną kategorię zdarzeń w postaci interaktywnych pasków, wykresów kołowych i czasowych.
10. Musi istnieć możliwość tworzenia filtrów bazując na parametrach zdarzenia takich jak: aplikacja, źródłowy i docelowy IP, usługa, typ zdarzenia, istotność ataku, kraj pochodzenia itd.
11. Musi obsługiwać automatycznie generowanie raportów według harmonogramu (codziennie, co tydzień i co miesiąc). Musi także umożliwiać administratorowi określenie daty i godziny, w której system raportowania zacznie generować zaplanowany raport.
12. Musi obsługiwać następujące formaty raportów: PDF i Excel.

III.21 Serwer zarządzania - logi, zdarzenia, korelacja

1. Serwer zarządzania musi posiadać możliwość korelacji logów pochodzących ze wszystkich urządzeń w celu zidentyfikowania podejrzanej aktywności, śledzenia trendów oraz anomalii; wszystko to musi być dostępne z wykorzystaniem jednego interfejsu użytkownika.
2. Wszystkie logi bezpieczeństwa i zdarzenia muszą być skorelowane.
3. Wszystkie logi oraz powiązane zdarzenia muszą być indeksowane.
4. Musi istnieć możliwość tworzenia niestandardowych reguł korelacji zdarzeń bezpieczeństwa.
5. Serwer zarządzania musi zapewniać obsługę przechowywania zdarzeń, przetwarzania i korelację logów z urządzeń firm trzecich, z wykorzystaniem co najmniej Syslog i SNMP.
6. Musi istnieć możliwość definicji poziomu istotności poszczególnych zdarzeń na podstawie reguł korelacji.
7. Serwer zarządzania musi obsługiwać automatyczną reakcję na określone zdarzenie bezpieczeństwa - minimalne działanie: wyślij wiadomość e-mail, SNMP trap, uruchom skrypt.
8. Musi istnieć możliwość graficznego tworzenia „parsera” logów w przypadku ich niestandardowego formatu.

9. Musi istnieć możliwość „skoku” bezpośrednio od zdarzenia do reguły w polisie bezpieczeństwa, która dane zdarzenie wygenerowała; wszystko musi być wykonane z użyciem jednego interfejsu użytkownika.
10. Musi istnieć możliwość natychmiastowego powiadomienia administratora w wyniku wystąpienia określonych zdarzeń i logów.
11. Serwer zarządzania musi umożliwiać definiowanie i zapisywania niestandardowych filtrów użytkownika dla każdego zdarzenia.
12. Musi istnieć możliwość definicji globalnych wyjątków związanych ze zdarzeniami; musi istnieć możliwość dostosowywania alarmów, aby wykluczyć zdarzenia według źródła, celu i usługi.
13. Musi istnieć możliwość grupowania zdarzeń w celu ich analizy.
14. Serwer zarządzania musi zapewniać predefiniowane raporty: godzinowy, dzienny, tygodniowy i miesięczny. Raport musi zawierać co najmniej: najczęstsze źródło, cel, usługi, zdarzenia, najczęstsze cele i odpowiadające im zdarzenia, najczęstsze usługi i odpowiadające im zdarzenia.

IV. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 lub równoważny dla funkcji Firewall.
- ICSA lub równoważny dla funkcji IPS lub NSS Labs w kategorii NGFW.

Zamawiający zastrzega sobie, na etapie realizacji umowy, możliwość wezwania Wykonawcy do przedstawienia ww. certyfikatów.

V. Serwisy i licencje

W ramach umowy powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować co najmniej kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analizę typu Sandbox, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres trwania umowy.

VI. Gwarancja oraz wsparcie techniczne

System musi być objęty serwisem gwarancyjnym producenta przez okres trwania umowy, polegającym co najmniej 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.
Przez naprawę rozumie się całkowite usunięcie usterki.
Wykonawca musi zapewnić wsparcie techniczne podczas eksploatacji systemu w liczbie 5 godzin w miesiącu przez cały okres trwania umowy.