PKP INTERCITY
SPÓŁKA AKCYJNA
BIURO TELEINFORMATYKI
Al. Jerozolimskie 142A
02-305 Warszawa

NR BST-P5/076/44/2021

Warszawa, dnia 20-09-2021 r.

Z A P Y T A N I E O I N F O R M A C J Ę

Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej w poniższym zakresie.

Przedmiotem zamówienia jest rozbudowa posiadanego środowiska zabezpieczającego sieć Zamawiającego o funkcjonalność VPN. Zamawiający eksploatuje rozwiązanie bazujące na Firewallach PaloAlto.

Opis przedmiotu zapytania:

Zadanie będące przedmiotem niniejszego zapytania polega na:

1.Zapewnieniu nowych funkcjonalności poprzez dostarczenia trzech pakietów funkcjonalności VPN w skład każdego wchodzą: urządzenie PA-3250 oraz pakiety subskrypcji Threat Prevention, GlobalProtect w całości objęte wsparciem producenta oferowanego rozwiązania.

2. Dostawy dokumentacji powykonawczej zainstalowanych urządzeń

3. Dostawa okablowania umożliwiającego połączenie urządzeń

4. Szkolenia

Wykonawca zapewni autoryzowane szkolenia dotyczące:

- wdrażanego rozwiązania dla 5 pracowników Zamawiającego
- zarządzania ciągłością działania ISO22301 dla 5 pracowników

Architektura

System koncentratorów VPN zwany dalej jako SKV musi być wdrożony dla dwóch fizycznych lokalizacji DataCenter (DC1, DC2) w architekturze 2+1:

DC1 - pełna redundancja w ramach lokalnego klastra wysokiej dostępności (tzw. High Availability) złożonego z dwóch urządzeń

DC2 - pojedyncze urządzenie zapewniające zarówno większą skalowalność w zakresie terminowania połączeń od użytkowników zdalnych w przypadku pracy normalnej jak również pełniące rolę zapasową w przypadku niedostępności DC1

SKV musi zostać wyskalowany do obsługi co najmniej 4 tysięcy jednoczesnych użytkowników zdalnych dla pracy normalnej definiowanej jako pełna dostępność DC1 i DC2, co należy rozumieć jako możliwość jednoczesnego zestawienia 4 tysięcy jednoczesnych tuneli w oparciu o protokoły IPSec i/lub SSL oraz dedykowane oprogramowanie klienta VPN na stacji końcowej.

SKV musi zapewniać jego bezproblemowe dalsze skalowanie poprzez instalację dodatkowych komponentów sprzętowych lub wirtualnych (w ramach prywatnych lub publicznych chmur DC),

pozwalających na zwiększenie ilości jednoczesnych tuneli VPN jako rozbudowa początkowej architektury (np. 2+1+1).

Urządzenia wchodzące w skład systemu SKV muszą zostać zintegrowane z posiadanym centralnym systemem zarządzania Panorama firmy Palo Alto Networks w zakresie:

- administrowania konfiguracją i politykami bezpieczeństwa
- aktualizacji oprogramowania i regularnych poprawek producenta
- logowania i raportowania
- redystrybucji informacji o zidentyfikowanych użytkownikach, ich mapowaniu do adresów IP oraz liście urządzeń poddanych kwarantannie (np. z powodu wykrycia infekcji stacji złośliwym oprogramowaniem lub komunikacji C2)

Zamawiający oświadcza, iż posiada odpowiednie licencje w ramach rozwiązania Panorama.

Sprzęt

SKV musi być zbudowany w oparciu jako specjalizowane urządzenia zabezpieczeń sieciowych (firewall), każdy z redundancją zasilania oraz sprzętową separacją zasobów (CPU, pamięć, dysk) w zakresie modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta (appliance).

Każdy firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla inspekcji firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 3 Gbit/s dla aktywnej kontroli zagrożeń w ruchu sieciowym (w tym kontrola aplikacji, antywirus, antyspyware, IPS, blokowanie plików oraz logowanie) oraz nie mniej niż 3 Gbit/s przepustowości połączeń IPSec VPN.

Każdy firewall musi być wyposażony w interfejsy robocze (inspekcyjne) w liczbie co najmniej 12 miedzianych portów Ethernet o negocjowanej przepustowości 10/100/1000Mbps oraz 8 portów o przepustowości 1Gbps/10Gbps zależnej od użytego interfejsu SFP lub SFP+.

Interfejsy sieciowe firewall muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Pracując 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. Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a firewall musi umożliwiać pracę we wszystkich wymienionych trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.

Firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.

Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie (HA) 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.

Oferowane urządzenia muszą być wyposażone w dedykowane interfejsy fizyczne do zestawienia klastra wysokiej dostępności (HA). Konfiguracja dwóch urządzeń jako klastra odpornego na awarie w trybach Active-Passive oraz Active-Active nie może zatem powodować zmniejszenia ilości wymaganych w zapytaniu, fizycznych interfejsów do inspekcji ruchu. Przedmiotem oferty jest również dedykowany kabel HA, do zestawienia klastra firewall-i w DC1.

Firewall musi posiadać wbudowany twardy dysk SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być również dostępne lokalnie na urządzeniu zabezpieczeń bez konieczności zakupu zewnętrznych urządzeń, oprogramowania ani licencji.

Funkcje bezpieczeństwa

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).

Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).

Firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

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. 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 9 Gbit/s.

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, kontrola i blokowanie aplikacji w modułach innych jak firewall (np. w silniku IPS lub innym module/profilu UTM).

Firewall musi wykrywać co najmniej 3500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

Firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

Firewall musi zapewniać możliwość segmentacji aplikacji na standardowych dla nich portach usług w obrębie pojedynczej reguły polityki firewall, tj. musi istnieć możliwość takiej konfiguracji pojedynczej reguły firewall, która zezwoli na działanie kilku aplikacji, wyłącznie jeśli nawiązanie połączenia następuje na port właściwy dla danej aplikacji, np. jeśli pojedyncza reguła zezwala na ruch SMTP i DNS, to SMTP nie może być dozwolone na porcie 53 (właściwym dla DNS), a DNS na porcie 25 (właściwym dla SMTP). Konstrukcja pojedynczej reguły bezpieczeństwa musi zatem pozwalać na jednoczesne uwzględnienie wielu aplikacji (lub grup aplikacji) wraz z ich domyślnie wykorzystywanym numerem portu TCP/UDP co znacznie podnosi optymalizację ilości zarządzanych reguł polityki bezpieczeństwa.

Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AntySpyware, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AntySpyware, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

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.

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.

Firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL/TLS) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. Musi być 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 antywirus i antyspyware), filtracja plików, danych i URL.

Firewall musi posiadać osobny/oddzielny zestaw polityk (względem głównych reguł bezpieczeństwa) do definicji rodzaju czy kategorii ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji.

Firewall musi umożliwiać deszyfrację ruchu SSL/TLS w zakresie:

- inspekcji bezpośrednio na urządzeniu

- przesłania w postaci rozszyfrowanej do innych rozwiązań zewnętrznych (np. system DLP) i ponownego zaszyfrowania

- wysyłania kopii zdeszyfrowanego ruchu SSL na wskazany interfejs urządzenia.

Firewall musi zapewniać również inspekcję szyfrowanej komunikacji SSH (Secure Shell).

Firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu 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, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

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.

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. Po odczytaniu zawartości pola XFF z nagłówka http firewall musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

Firewall musi umożliwiać dynamiczną modyfikację nagłówka HTTP o dane dotyczące użytkownika oraz domeny, w oparciu o posiadane informacje przypisania adresu IP do użytkownika w ramach danej sesji. Modyfikacja nagłówka powinna wynikać wprost ze skonfigurowanej reguły bezpieczeństwa dla konkretnej domeny z żądania HTTP (nagłówek HOST). Musi być możliwość nadpisania predefiniowanego pola nagłówka (np. X-Authenticated-User) jak również dołączenia własnego nagłówka (np. X-Custom-Header) z wartościami: użytkownik/domena.

Firewall powinien być wyposażony w mechanizm dynamicznej zmiany polityki bezpieczeństwa, dla użytkownika z wykrytą anomalią w ruchu lub uzasadnionym podejrzeniem kompromitacji konta, celem automatycznego przerwania ataku. Mechanizm taki powinien działać w oparciu o dynamiczne przypisanie takiego użytkownika do grupy źródłowej skojarzonej z inną, bardziej restrykcyjną regułą bezpieczeństwa. Taka zmiana powinna być:

- Wyzwalana zewnętrznie (np. poprzez interfejs API)
- Odwracalna (zdjęcie ograniczeń po ustąpieniu ryzyka)

- Automatycznie zatwierdzana (bez dodatkowej konieczności ręcznego zatwierdzania konfiguracji firewall, co bezpośrednio wpływa na opóźnienie odpowiedzi na atak)
- Widoczna w logach

Firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

Firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolujący ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur antywirus musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny z centralnego systemu zarządzania.

Firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

Firewall musi posiadać modułu wykrywania i blokowania ataków intruzów IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny z centralnego systemu zarządzania.

Firewall musi posiadać moduł antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur antyspyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny z centralnego systemu zarządzania.

Firewall musi posiadać moduł antyspyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja antyspyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta, w tym poprzez import sygnatur w formatach SNORT oraz Suricata z centralnego systemu zarządzania.

Firewall musi wykrywać i blokować ruch/zapytania do domen uznanych za złośliwe poprzez weryfikację bezpośrednio na urządzeniu lokalnej bazy o pojemności co najmniej 100 tysięcy sygnatur DNS.

Firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

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.

Firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

Firewall musi wykonywać statyczną i dynamiczną translację adresów NAT w oparciu o osobny, względem polityk bezpieczeństwa, zestaw reguł. Funkcjonalność NAT musi pozwalać na wykorzystanie adresów dynamicznych w oparciu o obiekty typu FQDN.

Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

Firewall musi pozwalać na budowanie polityk uwierzytelniania określających rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.

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. Przykładowo firewall musi pozwalać na integrację w środowisku wirtualnym VMware ESXi w taki sposób, aby mógł on 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 rekonfiguracji polityk bezpieczeństwa firewalla.

VPN

Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać zaawansowane funkcjonalności:

a. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS, Google Android.Wymagana jest dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-14), Google Android (6-11), Microsoft Windows 10 UWP

b. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 7,8,8.1,10; Windows 10 UWP; MacOS 10.11-10.15,11; Linux CentOS 7.0-7.7, 8.0, 8.3; RedHat 7.0-7.7, 8.3-8.4; Ubuntu 14.04-20.04;

c. Możliwość zestawiania połączeń zdalnego dostępu VPN za pomocą IPv6

d. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows

e. Dla podłączających się stacji/laptopów Windows i MacOS możliwość pomijania ruchu do tunelu zdalnego dostępu VPN dla specyficznych procesów aplikacji, domen, aplikacji video.

f. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)

Klient dostępu zdalnego VPN, co najmniej dla systemów klasy Windows, musi zbierać informacje o systemie operacyjnym, zainstalowanych poprawkach OS, aktualności lokalnego oprogramowania antywirusowego, stanie host firewall-a i szyfrowania dysku, wpisach w rejestrze OS i uruchomionych na stacji procesach. Musi być możliwość zarówno monitorowania pozyskanych informacji jak również ich wykorzystania jako elementu klasyfikacji w polityce dostępowej VPN.

Klient dostępu zdalnego VPN musi umożliwiać identyfikację urządzenia użytkownika zdalnego w sposób jednoznaczny tj. przy wykorzystaniu jego atrybutu sprzętowego typu numer seryjny urządzenia. Na tej podstawie (a nie na podstawie samego tylko adresu IP) musi być możliwość dodania zainfekowanego złośliwym oprogramowaniem urządzenia końcowego, do listy kwarantanny co powoduje definitywne zablokowanie jego dostępu do zasobów firmowych (bez względu na adres IP, z którego się łączy).

Firewall musi również 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).

Autentykacja dostępu zdalnego VPN do zasobów firmowych musi bazować na co najmniej dwóch metodach, określonych na etapie wdrożenia SKV, w tym co najmniej LDAP + certyfikat użytkownika/urządzenia lub kody SMS (RADIUS).

Wymagania zarządzanie

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.

Firewall musi posiadać koncept konfiguracji kandydackiej którą można edytować na urządzeniu na poziomie API, GUI oraz CLI bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany te zostaną zaakceptowane i sprawdzone przez administratora systemu. Musi być możliwa modyfikacja konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie, jak również zatwierdzanie i cofanie zmian, których są autorami. Rozwiązanie

musi automatycznie tworzyć kopie i przechowywać co najmniej 100 ostatnio używanych konfiguracji wraz ze znacznikiem czasu, które można w dowolnym momencie przywrócić.

Firewall musi być wyposażony w interfejs API, który odwzorowuje wszystkie funkcje interfejsów CLI oraz GUI, celem zapewnienia otwartości systemu pod kątem innych integracji oraz automatyzacji.

Firewall musi dokładnie logować wszystkie zdarzenia związane z próbami nawiązania zdalnego połączenia VPN w ramach oddzielnej kategorii logów w celu ich łatwego przeszukiwania i identyfikacji potencjalnych problemów, celem przyspieszenia pomocy użytkownikom.

Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). Firewall musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach oraz ich uwierzytelnianie za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos (konfigurowalnych również jako sekwencja uwierzytelniająca np. baza lokalna, LDAP i RADIUS

Firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa, polityki PBR (policy based routing) oraz polityki QoS wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur.

Firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa, w szczególności selektywne wysyłanie logów bazując na ich atrybutach oraz generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia (np. automatyczne utworzenie zgłoszenia w zewnętrznym systemie helpdesk po wystąpieniu zdefiniowanego typu logu/zdarzenia).

Firewall musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach oraz aktywności zdalnych połączeń VPN.

Firewall musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, w szczególności raportów o próbach połączeń zdalnych VPN użytkowników i urządzeń, 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.

Firewall musi automatycznie zweryfikować spójność konfiguracji polityk bezpieczeństwa z punktu widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook” potrzebne jest dodatkowo użycie aplikacji „SSL”, a administrator nie uwzględni tej aplikacji w polityce, to algorytm powinien ostrzec o tym fakcie administratora zarówno w momencie tworzenia oraz zatwierdzania nowej polityki. Bezpośrednio z okna powiadomienia administratora o wykryciu zależności pomiędzy aplikacjami, powinna istnieć efektywna i szybka możliwość edycji takiej reguły. Z poziomu

GUI musi być możliwość analizy wykorzystania polityk bezpieczeństwa pod kątem wykrywanych w politykach aplikacji oraz na ciągłe monitorowanie innych, nowych aplikacji pod kątem ich dodania lub wykluczenia z ruchu.

Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

Wymagania dla dostawy urządzeń i wsparcia serwisowego:

1. Urządzenia muszą być fabrycznie nowe, muszą pochodzić z autoryzowanego kanału dystrybucji producenta i być objęte serwisem producenta na terenie RP.
2. Sprzęt powinien być oznaczony znakami producenta i powinien posiadać deklarację CE.
3. Miejsce realizacji przedmiotu zapytania:
    i. Dostawa, instalacja i konfiguracja powinna być przeprowadzona w miejscu wskazanym przez Zamawiającego (do 35 km od siedziby Zamawiającego),
4. Urządzenia powinny być podłączone do sieci Zamawiającego we współpracy z administratorami Zamawiającego.
5. Urządzenia powinny być dostarczone z najnowszym i zalecanym przez producenta oprogramowaniem oraz wszystkimi niezbędnymi licencjami.
6. Zamawiający powinien mieć wgląd w stronę producenta i mieć możliwość pobrania aktualizacji oprogramowania przez okres wsparcia serwisowego.
7. Wsparcie serwisowe powinno być w realizowane w dni robocze w trybie 8x5xNBD na zasadach określonych przez producenta oferowanego rozwiązania.

Terminy składania pytań oraz udzielenie informacji:

W odpowiedzi na niniejsze zapytanie prosimy przesłać:

1. Szacowanego czasu dostawy przedmiotu zapytania do Zamawiającego, w tym:
    a. Termin dostawy urządzeń i subskrypcji
    b. Termin przygotowania i przekazania Zamawiającemu dokumentacji technicznej
2. Zakres wsparcia dla oferowanego rozwiązania
3. uzupełniony formularz cenowy według wzoru w poniższej tabeli.

Termin składania informacji cenowych upływa **w dniu 29.09.2021 r. o godz. 15.00** (ewentualne pytania prosimy kierować do dnia 24.09.2021 r. do godziny 15:00). Odpowiedź proszę przesłać w formie e-mail na adres: it@intercity.pl

Formularz cenowy . .

Poniższe pozycje wypełnia Oferent:

L.P.	Nazwa/Model		Ilość	Cena netto za 1 szt./ 1 pracownika [w przypadku szkoleń] w zł	Wartość netto w zł
1	Dostawa, instalacja i konfiguracja pakietów funkcjonalności VPN	Urządzenie PA-3250	3		
2		Subskrypcja Threat Prevention na okres 36 miesięcy	3		
3		Subskrypcja Global Protect na okres 36 miesięcy	3		
4	Wsparcie producenta oferowanego rozwiązania na okres 36 miesięcy		36 miesięcy	…….. zł za wsparcie na okres 12 miesięcy / 1 szt.	…….. zł za wsparcie na okres 36 miesięcy / 3 szt.
5	Dokumentacja		n/d	n/d	
6	Komplet niezbędnego okablowania		n/d	n/d	
7	Komplet szkoleń		5	…….. zł za komplet szkoleń / osobę.	…….. zł za komplet szkoleń / 5 osób.
				Suma	

Szacowany czas dostawy urządzeń i subskrypcji w ramach realizacji przedmiotu zapytania:

……..

Szacowany czas przygotowania i przekazania Zamawiającemu dokumentacji technicznej:

……..

„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.