ORPEG
OŚRODEK ROZWOJU
POLSKIEJ EDUKACJI ZA GRANICĄ

Warszawa, dnia 26 listopada 2024 r.

ZAPYTANIE OFERTOWE

I. <u>Przedmiot zamówienia:</u> Dostawa urządzeń UTM

II. Opis Przedmiotu zamówienia:

1. <u>Definicje:</u>
   1.1. Urządzenie UTM – wszystkie pozycje stanowiące przedmiot zamówienia
   1.2. oferta równoważna – oferta zgodna z informacjami zawartymi w specyfikacji sprzętu
2. <u>Miejsce dostawy:</u>
   2.1. Ośrodek Rozwoju Polskiej Edukacji za Granicą, ul. Wołoska 5, 02-675 Warszawa, do pomieszczeń znajdujących się na 4 piętrze. W budynku znajdują się windy. Dostawa w godzinach 7-15.
3. <u>Termin realizacji zamówienia:</u> do 15 dni od dnia podpisania umowy.
4. Wykaz zamawianych urządzeń UTM stanowi załącznik nr 1 do niniejszego zapytania ofertowego.
5. Wykonawca zobowiązany jest dostarczyć urządzenia UTM w oryginalnych opakowaniach producenta.
6. Oferowane produkty nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć.
7. Wsparcie techniczne producenta:
   7.1. Całodobowy dostęp do ekspertów technicznych, szybką reakcję na zgłoszenia serwisowe oraz możliwość wymiany sprzętu w trybie 24x7.
   7.2. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu urządzenia.
8. Wykonawca przekaże Zamawiającemu szczegółowe instrukcje obsługi i konserwacji dla każdej właściwej jednostki dostarczonego urządzenia UTM (może być w wersji elektronicznej).
9. Wykonawca przed podpisaniem umowy dostarczy deklarację zgodności CE oferowanego sprzętu.
10. Dostarczone urządzenia UTM muszą spełniać wszystkie wymogi bezpieczeństwa oraz zużycia energii obowiązujące w prawie polskim.
11. Dostarczone urządzenia UTM muszą spełniać kryteria środowiskowe.
12. Warunki gwarancji:
    1) Minimalne okresy gwarancji zostały wskazane w wykazie znajdującym się w niniejszym załączniku. Za dzień rozpoczęcia biegu terminu gwarancji uważa się dzień podpisania przez obie strony protokołu odbioru dostarczonego sprzętu.
    2) Zamawiający oczekuje gwarancji producenta sprzętu.
    3) Serwis urządzeń musi być realizowany na terenie Polski przez producenta lub autoryzowanego partnera Serwisowego Producenta.
    4) Serwis świadczony w siedzibie Zamawiającego.
    5) Czas reakcji serwisu – najpóźniej w pierwszym dniu roboczym następującym po dniu zgłoszenia awarii, o ile zgłoszenie nastąpi do godziny 17:00. W przypadku złożenia zgłoszenia po godzinie 17 za dzień zgłoszenia przyjmuje się dzień następny po dniu przesłania zgłoszenia.
13. Wykonawca zobowiązany jest wskazać w ofercie nazwę sprzętu (typ, producent, model), który oferuje.

III. Kryteria oceny ofert:

cena 100%, co oznacza, że jako najkorzystniejsza uznana zostanie oferta z najniższą ceną spośród ważnych ofert.

IV. Wynagrodzenie:

Informacje dotyczące wynagrodzenia znajdują się w załączniku nr 3 do zapytania ofertowego.

V. Wykaz dokumentów, jakie należy załączyć do oferty:

1. Formularz ofertowy – stanowiący załącznik nr 2 do zapytania ofertowego.
2. W przypadku, gdy Wykonawcę reprezentuje pełnomocnik – pełnomocnictwo.

VI. Opis sposobu przygotowania ofert:

1. Oferta obejmie przedmiot zamówienia i musi być sporządzona w oparciu o warunki niniejszego zapytania.
2. Oferta musi spełniać następujące wymogi:
   2.1. Oferta ma być napisana w języku polskim, na komputerze, ręcznie długopisem lub nieścieralnym atramentem pod rygorem jej nieważności;
   2.2. Oferty nieczytelne nie będą rozpatrywane;
   2.3. Formularz oferty oraz wszystkie załączniki muszą być podpisane na każdej zapisanej stronie przez osobę(y) upoważnioną(e) do reprezentowania firmy (podpis i pieczątka imienna lub czytelny podpis lub tylko podpis kwalifikowany w przypadku podpisania elektronicznego oferty), zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze sądowym lub innym dokumencie, właściwym dla formy organizacyjnej firmy Wykonawcy;
   2.4. Upoważnienie do reprezentowania Wykonawcy należy dołączyć do oferty (oryginał lub kopia poświadczona notarialnie);
   2.5. W przypadku, gdy Wykonawcę reprezentuje Pełnomocnik, do oferty musi być załączone pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy;
   2.6. Zaleca się, aby wszystkie zapisane strony oferty były ponumerowane kolejnymi numerami;
   2.7. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane i datowane własnoręcznie przez osobę podpisującą ofertę;
   2.8. Wszelkie koszty związane z przygotowaniem oraz złożeniem oferty ponosi Wykonawca;

VII. <u>Informacja o obowiązywaniu Procedury zgłoszeń wewnętrznych w Ośrodku Rozwoju Polskiej Edukacji za Granicą („Ośrodek")</u>

Informujemy, że na podstawie art. 24 ust. 1 ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. z 2024 r. poz. 928) dalej „ustawa'', w Ośrodku obowiązuje Procedura zgłoszeń wewnętrznych wprowadzona zarządzeniem nr 141/2024 Dyrektora Ośrodka Rozwoju Polskiej Edukacji za Granicą z 25 września 2024 r. w sprawie wprowadzenia Procedury zgłoszeń wewnętrznych w Ośrodku Rozwoju Polskiej Edukacji za Granicą zwana dalej „Procedurą"

W wypełnieniu obowiązku z art. 24 ust. 6 ustawy informujemy , że w związku z przyjętą Procedurą, mają Państwo prawo zgłoszenia naruszenia prawa polegającego na działaniu lub zaniechaniu niezgodnym z prawem lub mającym na celu obejście prawa, we wszystkich dziedzinach wskazanych w art. 3 ust. 1 ustawy:

Zgłoszeń można dokonywać za pomocą następujących środków komunikacji:

1) w postaci elektronicznej na adres e-mail: naruszenia@orpeg.pl;
2) w postaci pisemnej na adres korespondencyjny Ośrodka: Dyrektor Ośrodka Rozwoju Polskiej Edukacji za Granicą, 02-675 Warszawa ul. Wołoska 5 z dopiskiem: nie otwierać – zgłoszenie sygnalisty;
3) telefonicznie pod dedykowany numer: +48 22 622 37 92, +48 22 622 37 93, w dni robocze, w godzinach 8-16;
4) osobiście, na wniosek sygnalisty złożony za pośrednictwem jednego z kanałów, o których mowa w pkt 1-3, podczas bezpośredniego spotkania zorganizowanego w terminie 14 dni od dnia otrzymania wniosku.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Informujemy, że Państwa dane osobowe przekazane w związku ze zgłoszeniem dokonanym w trybie ustawy nie podlegają ujawnieniu nieupoważnionym osobom, chyba że ujawnienie takie następuje za wyraźną zgodą sygnalisty, bądź ich ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa. Procedura zgłoszeń wewnętrznych dostępna jest w Biuletynie Informacji Publicznej Ośrodka w zakładce Sygnaliści/ zgłoszenia wewnętrzne.
https://bip.orpeg.pl/zgloszenia-wewnetrzne/

VIII. Miejsce i termin składania ofert:

1. Ofertę należy nadsyłać **do 3 grudnia 2024 r. do godziny 10:00** na adres Ośrodka Rozwoju Polskiej Edukacji za Granicą, ul. Wołoska 5, 02-675 Warszawa z dopiskiem „Dostawa urządzeń UTM" lub na adres e-mail: bartlomiej.barlakowski@orpeg.pl .
2. Oferty złożone po terminie składania ofert nie będą rozpatrywane. Decyduje data skutecznego dostarczenia oferty do Zamawiającego a nie data nadania oferty.
3. Oferty oraz wszelkie oświadczenia i zaświadczenia składane w trakcie postępowania są jawne, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane. W tym przypadku powinien ją oznaczyć w sposób niebudzący wątpliwości, iż stanowi ona zastrzeżoną tajemnicę przedsiębiorstwa np. w odrębnym opakowaniu oznaczonym napisem „TAJEMNICA PRZEDSIĘBIORSTWA. NIE UDOSTĘPNIAĆ INNYM UCZESTNIKOM POSTĘPOWANIA" lub równoważnym.

IX. Z wyłonionym w trakcie postępowania Wykonawcą zostanie podpisana umowa na druku Zamawiającego. Istotne postanowienia umowy stanowią załącznik nr 3 do zapytania ofertowego.

X. **UWAGA:** Zamawiający zastrzega sobie:

- w przypadku, gdy najkorzystniejsza oferta przekroczy cena kwotę przeznaczona przez Zamawiającego na realizacje przedmiotu zamówienia zmniejszenie zamówienia o wybrane przez siebie pozycje tak by ostateczne zamówienie nie przekroczyło kwoty przewidzianej przez Zamawiającego na realizacje przedmiotu zamówienia lub negocjowanie z Wykonawcą, który złoży najkorzystniejszą ofertę ceny łącznej zamówienia
- prawo odstąpienia lub unieważnienia postępowania o udzielenie zamówienia publicznego na każdym etapie; z tytułu unieważnienia postępowania Oferentom nie przysługuje żadne roszczenie wobec Zamawiającego,
- zmiany lub uzupełnienia zapytania ofertowego,
- poprawy oczywistych omyłek pisarskich

Pytania można kierować do: Bartłomiej Barlakowski, e-mail: bartlomiej.barlakowski@orpeg.pl .

Barbara Teresa Talik

Elektronicznie podpisany przez Barbara Teresa Talik
Data: 2024.11.26 12:53:20 +01'00'

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Zamawiający wskazuje minimalne wymagania wobec poszczególnych pozycji stanowiących przedmiot zamówienia.

Urządzenie UTM - 2 sztuki wraz z gwarancja producenta i kontrolą aplikacji, IPS, antywirus, analizą typu Sandbox cloud, antyspam, web filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Opis przedmiotu zamówienia:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę 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 7 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach systemu ochrony są 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.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 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.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników 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.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
    - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
    - Certyfikat ISO 9001 podmiotu serwisującego.

Wymagania dodatkowe

1. Spełnienie wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), uzyskania dokumentu pochodzącego od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

2. Uzyskanie dokumentu - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Załącznik nr 2 do zapytania ofertowego

FORMULARZ OFERTOWY

Dane Wykonawcy (imię i nazwisko lub firma): .....

Siedziba/adres zamieszkania Wykonawcy .....

NIP..... REGON.....

tel. ..... fax.....

www..... e-mail .....

Do: Nazwa i siedziba Zamawiającego:
Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa

Składamy ofertę na: Dostawa urządzeń UTM

CENA BRUTTO za realizację przedmiotu zamówienia
..... zł (słownie: .....),

Kwota NETTO za realizację przedmiotu zamówienia
..... zł (słownie: .....),

w tym VAT w stawce ……% lub cena brutto ……. zł (słownie:…… złotych).

FORMULARZ CENOWY

Lp.	Przedmiot – zgodnie z załącznikiem nr 1 zapytania ofertowego	Kwota jednostkowa netto	Vat %	Cena jednostkowa brutto	Liczba sztuk	Kwota łączna netto	Kwota łączna vat	Kwota łączna brutto
1	Urządzenie UTM (wraz z gwarancją i licencjami na okres 60 miesięcy)				2			

OPIS OFEROWANEGO SPRZĘTU

	PRODUCENT	**MODEL**	**TYP (wariant)**	**Opis ofertowanych parametrów***
Urządzenie UTM (2 sztuki) wraz z licencjami				

*należy odnieść się minimum do parametrów wskazanych przez zamawiającego w załączniku nr 1 do zapytania ofertowego

1. Składając ofertę na wykonanie przedmiotu zamówienia oświadczamy, że zapoznaliśmy się z treścią zapytania ofertowego i nie wnosimy do niego zastrzeżeń oraz , że zamówienie zostanie wykonane zgodnie z warunkami wskazanymi w zapytaniu ofertowym. Oświadczamy także, że wyrażamy zgodę na zawarcie umowy zgodnie z istotnymi postanowieniami umowy stanowiącymi załącznik nr 3 do zapytania ofertowego.
2. Oświadczamy, ze naszym pełnomocnikiem dla potrzeb niniejszego Zamówienia jest:

……

…… *(wypełniają jedynie przedsiębiorcy składający wspólną ofertę)*

3. Uważamy się za związanych niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.
4. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr_____ do nr _____.

Do oferty załączam następujące dokumenty:

1) ……..
2) ……..

……..

…… .....

/miejscowość, data/ /podpis Wykonawcy /osoby uprawnionej do reprezentacji/

*niepotrzebne skreślić

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Załącznik nr 3 do zapytania ofertowego

ISTOTNE POSTANOWIENIA UMOWY

UMOWA nr /2024/ORPEG

zawarta w dniu ……. grudniu 2024 roku w Warszawie pomiędzy:

Skarbem Państwa - Ośrodkiem Rozwoju Polskiej Edukacji za Granicą z siedzibą Warszawie, przy ul. Wołoskiej 5, 02 – 675 Warszawa, NIP 521-29-08-445 zwanym dalej „**ZAMAWIAJĄCYM**", reprezentowanym przez:

Panią ……..

a

……. REGON …… NIP ……, zwanym dalej „**Wykonawcą"**

zwanych dalej łącznie **STRONAMI**

§ 1

1. Przedmiotem umowy jest zakup i dostawa …….zwanego dalej także urządzeniem UTM lub przedmiotem dostawy, zgodnie z opisem przedmiotu zamówienia, stanowiącym załącznik nr 1 do niniejszej umowy oraz ofertą Wykonawcy z dnia …….. 2024 r., stanowiąca załącznik nr 2 do niniejszej umowy.
2. Wykonawca zobowiązuje się dostarczyć urządzenia UTM w terminie do 14 dni od dnia podpisania umowy
3. Wykonawca dostarczy urządzenia UTM na własny koszt we własnym zakresie. Dostawa nastąpi w godzinach 7:00-15, w dniu ustalonym przez Wykonawcę z Zamawiającym.
4. Wykonawca ponosi odpowiedzialność za wady i szkody powstałe w czasie transportu urządzeń UTM do miejsca przeznaczenia oraz jego wnoszenia.
5. Wykonawca przekaże Zamawiającemu przedmiot dostawy na podstawie protokołu odbioru, zawierającego minimum :
   1) liczbę porządkową,
   2) dla urządzeń UTM:
      a) rodzaj,
      b) model,
      c) nazwę producenta,
      d) numer seryjny,
      e) liczba
   3) liczba wykupionych gwarancji producenta,
   4) oraz datę dostawy i oznaczenie stron,
6. W przypadku stwierdzenia podczas odbioru wadliwości urządzeń UTM w całości lub części Zamawiający może odmówić odbioru urządzeń UTM.
7. W chwili odbioru urządzeń UTM przez przedstawiciela Zamawiającego własność sprzętu przechodzi na Zamawiającego.
8. Sprzęt dostarczony przez Wykonawcę musi być fabrycznie nowy, niewykazujący śladów użytkowania, posiadać ponadto posiadać wszelkie niezbędne atesty, o ile obowiązujące przepisy prawa wymagają przedstawienia ww. atestów.
9. Za datę dostarczenia urządzeń UTM uważa się dzień jego odbioru przez przedstawiciela Zamawiającego, bez zastrzeżeń.
10. Zamawiający zobowiązuje się do:
    1) przystąpienia do czynności odbioru urządzeń UTM, niezwłocznie po dostarczeniu go przez Wykonawcę,

o ile będzie on spełniać wymogi określone w „opisie przedmiotu zamówienia” stanowiącym załącznik nr 1 do niniejszej umowy i nie będzie obciążony wadami,

2) podpisania protokołu zdawczo – odbiorczego lub zgłoszenie uwag w terminie do 7 dni od dnia dostarczenia przedmiotu zamówienia.
3) zapłaty na rzecz Wykonawcy wynagrodzenia umownego za zrealizowany przedmiot umowy.

11. Podpisanie protokołu odbioru sprzętu przez Zamawiającego nie ogranicza jego uprawnień wynikających z gwarancji i rękojmi za wady urządzeń UTM i zrealizowanych instalacji oraz uprawnień do żądania zapłaty kar umownych i odszkodowań wynikających z postanowień umowy.

§ 2

1. Wykonawca oświadcza, że posiada wszelkie kwalifikacje, uprawnienia, doświadczenie niezbędne do wykonania umowy oraz zobowiązuje się do jej wykonania z zachowaniem należytej staranności wymaganej w stosunkach tego rodzaju.
2. Wykonawca oświadcza, iż urządzenia UTM posiada i w dacie dostawy posiadać będzie wszelkie atesty, certyfikaty i dopuszczenia wymagane na terenie Polski oraz spełnia i w dacie dostawy spełniać będzie wymogi wynikające z przepisów obowiązującego prawa.
3. W przypadku powierzenia przez Wykonawcę wykonania przedmiotu umowy osobom trzecim w całości lub w części, Wykonawca odpowiada za działania i zaniechania tych osób, jak za własne działania lub zaniechania.
4. Wykonawca ponosi pełną odpowiedzialność, za jakość i terminowość prac, które wykonuje przy pomocy podwykonawców.
5. Wykonawca zobowiązuje się do zachowania w poufności wszystkich informacji uzyskanych przez niego w związku z zawarciem umowy. Wykonawca ponosi pełną odpowiedzialność za zachowanie w poufności ww. informacji przez podmioty, o których mowa w ust. 2 i 3.
6. Wykonawca jest zobowiązany do udzielania Zamawiającemu, na jego żądanie, wszelkich wiadomości o przebiegu realizacji umowy przez Wykonawcę.
7. Wykonawca jest zobowiązany niezwłocznie na piśmie, informować Zamawiającego o wszelkich okolicznościach, które mogą mieć wpływ na realizację postanowień Umowy, w szczególności o przewidywanym opóźnieniu jej wykonania, wraz z podaniem przyczyny.
8. Wykonawca zobowiązuje się wykonać przedmiot niniejszej umowy z należytą starannością, według swojej najlepszej wiedzy i umiejętności, wykorzystując w tym celu wszystkie posiadane możliwości i doświadczenie oraz mając na względzie ochronę interesów Zamawiającego.

§ 3

1. Strony zgodnie ustalają, że za prawidłowe i kompletne wykonanie przedmiotu umowy, o którym mowa w §1 cena wynosi z podatkiem VAT: …….. zł (słownie: ……), w tym podatek VAT w stawce ..... Szczegółowa kalkulacja cen jednostkowych znajduje się w ofercie Wykonawcy, stanowiącej załącznik nr 2 do umowy.
2. Wypłata nastąpi w terminie do 14 dni od dnia dostarczenia do Zamawiającego prawidłowo wystawionej faktury. Faktura zostanie wystawiona i dostarczona do Zamawiającego nie później niż pierwszego dnia roboczego następującego po dniu podpisania przez obie strony protokołu odbioru. Protokół zostanie podpisany przez przedstawiciela Wykonawcy i …….. lub osobę zastępującą.
3. Zapłata wskazanego wyżej wynagrodzenia na rzecz Wykonawcy nastąpi przelewem na rachunek bankowy Wykonawcy wskazany na fakturze .
4. Przez dzień zapłaty rozumie się dzień obciążenia rachunku bankowego Zamawiającego.
5. Wykonawcy nie przysługują żadne inne roszczenia o dodatkowe wynagrodzenie, nieprzewidziane w umowie, ani roszczenia o zwrot kosztów poniesionych w związku z wykonaniem umowy.

§ 4

1. Na przedmiot dostawy Wykonawca udziela Zamawiającemu gwarancji, jakości na okres nie krótszy niż:
   a) Urządzenie UTM wraz z licencjami ……..=≥ 60 miesięcy

   począwszy od dnia sporządzenia miedzy stronami protokołu, o którym mowa w § 1 ust. 5 umowy.
2. Wykonawca zagwarantuje Zamawiającemu gwarancję producenta.
3. Naprawy gwarancyjne muszą być świadczone przez autoryzowany serwis producenta Sprzętu.
4. Termin gwarancji udzielony przez Wykonawcę biegnie od daty podpisania protokołu odbioru urządzeń UTM przez przedstawiciela Zamawiającego.
5. Zamawiający zgłasza do Wykonawcy lub bezpośrednio do producenta wadliwie działający urządzenia UTM podczas jego eksploatacji, w czasie trwania gwarancji.
6. Zamawiający zastrzega sobie prawo zgłaszania do Wykonawcy wadliwego działania Sprzętu podczas jego eksploatacji, w czasie trwania gwarancji, telefonicznie: …… lub e-mailem: ……. Zgłoszenie do Wykonawcy, awarii Sprzętu pocztą elektroniczną uważać się będzie za doręczone. Zgłoszenie, w miarę możliwości, będzie zawierać opis uszkodzenia.
7. Ewentualne naprawy gwarancyjne Sprzętu, zgłoszone do Wykonawcy, będą odbywały się w miejscu instalacji Sprzętu, zgodnie z wymogami gwarancyjnymi określonymi w opisie przedmiotu zamówienia
8. W przypadku awarii dysków twardych Zamawiający otrzyma nowy dysk, a uszkodzony pozostanie własnością Zamawiającego. Zamawiający wymaga, aby opcja ta była wykupiona u producenta sprzętu.
9. Serwis świadczony w siedzibie Zamawiającego
10. Czas reakcji serwisu – najpóźniej w pierwszym dniu roboczym następującym po dniu zgłoszenia awarii, o ile zgłoszenie następy do godziny 17:00. W przypadku złożenia zgłoszenia po godzinie 17 za dzień zgłoszenia przyjmuje się dzień następny po dniu przesłania zgłoszenia.
11. Na wymienione części Wykonawca przekaże gwarancję o takiej długości, jaką daje producent części, jednak nie krótszą niż termin gwarancji danego urządzeń UTM.
12. Wykonawca na żądanie Zamawiającego, dokona wymiany urządzenia UTM na nowe, wolne od wad, o parametrach identycznych lub lepszych, niż określone w opisie przedmiotu zamówienia i ofercie Wykonawcy w przypadkach, gdy:
    1) w okresie gwarancyjnym nastąpi trzykrotna naprawa urządzenia UTM lub jedna jego istotna naprawa (rozumiana, jako naprawa o wartości nie mniejszej niż 30% wartości naprawianego urządzeń UTM),
    2) naprawa urządzenia UTM z powodu wad nieusuwalnych jest technicznie niemożliwa,
13. Gwarancje, o których mowa w ust. 1 nie mogą zawierać następujących warunków:
    1) ograniczać okresu gwarancji poprzez uwzględnienie naturalnego zużycia elementów wchodzących w skład zamawianego urządzenia UTM,
    2) postanowień niekorzystnych dla Zamawiającego lub powodujących jego obciążenie dodatkowymi kosztami związanymi z dostawą urządzeń UTM, a także zawierać dodatkowych warunków współpracy z Wykonawcą,
    3) postanowień o innych płatnych działaniach nie ujętych w umowie,
    4) postanowień dotyczących ponoszenia przez Zamawiającego opłat z tytułu przygotowania urządzeń UTM przekazywanego do serwisu.
    5) postanowień ograniczających naprawę urządzeń UTM z uwagi na wartość usunięcia wady.
14. O ile producent sprzętu określonego w przedmiocie dostawy wydaje odrębne dokumenty gwarancyjne, Wykonawca ma obowiązek dostarczyć wypełnione i zarejestrowane, wymagane, dokumenty gwarancyjne producenta urządzeń UTM, które nie mogą być mniej korzystne niż warunki określone w niniejszej umowie w zakresie gwarancji. W razie utraty dokumentu gwarancyjnego Zamawiający nie traci uprawnień z tytułu gwarancji, jeżeli okaże za pomocą innego dokumentu (protokołu odbioru, faktura) istnienie zobowiązań z

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

tytułu gwarancji, jakości.

15. Wszystkie dodatkowe koszty związane ze świadczeniem usługi serwisu gwarancyjnego ponosi Wykonawca.
16. Wykonawca zobowiązuje się każdorazowo informować Zamawiającego o zmianie siedziby w czasie trwania okresu gwarancyjnego.

§ 5

1. Zamawiający ma prawo naliczyć Wykonawcy kary umowne:
   1) Za niewykonanie lub nienależyte wykonanie przedmiotu umowy - karę umowną w wysokości 0,5 % łącznego wynagrodzenia brutto, o którym mowa w § 3 ust. 1 umowy za każdy przypadek naruszenia umowy.
   2) W razie zwłoki w dostarczeniu urządzeń UTM Wykonawca zobowiązany jest zapłacić Zamawiającemu karę umowną w wysokości 0,5 % kwoty brutto, o której mowa w § 3 ust. 1 umowy, za każdy rozpoczęty dzień zwłoki, licząc od terminu, o którym mowa w § 1 ust. 2 do dnia odbioru urządzeń UTM bez zastrzeżeń przez przedstawiciela Zamawiającego.
   3) W przypadku zwłoki w wykupieniu przez Wykonawcę gwarancji producenta Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,25% kwoty brutto, o której mowa w § 3 ust. 1 umowy, za każdy rozpoczęty dzień zwłoki, licząc od dnia następnego po dniu dostarczenia Zamawiającemu przedmiotu zamówienia przez Wykonawcę.
   4) W przypadku niewykonania lub nienależytego wykonania umowy przez Wykonawcę, odstąpienia Wykonawcy od umowy, bądź odstąpienia od umowy przez Zamawiającego z przyczyn dotyczących Wykonawcy z wyłączeniem przypadku określonego w § 6 ust. 1 pkt. 2, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20% ceny brutto, o której mowa w § 3 ust. 1.
2. Kary umowne podlegają sumowaniu.
3. Wykonawca wyraża zgodę na potrącenie kar z należnego mu wynagrodzenia, bez dodatkowych wezwań do zapłaty.
4. Zamawiający ma prawo do żądania od Wykonawcy odszkodowania przewyższającego wysokość zastrzeżonej kary umownej na zasadach ogólnych w przypadku, gdy wielkość szkody przekracza wysokość zastrzeżonej kary umownej.
5. Strony nie odpowiadają za niewykonanie lub nienależyte wykonanie umowy, będące następstwem działania siły wyższej. Dla celów niniejszej umowy określa się, iż siłą wyższą jest zdarzenie nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia i przewidzenia.
6. W przypadku naliczenia przez Zamawiającego kar umownych, Wykonawca nie może pomniejszyć należnego mu wynagrodzenia na wystawionej fakturze o kwotę naliczonych kar umownych

§ 6

1. Zamawiający zastrzega sobie prawo do odstąpienia od umowy w razie zaistnienia przynajmniej jednej z wymienionych okoliczności:
   1) niewykonywania lub nienależytego wykonywania umowy przez Wykonawcę,
   2) zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, czego nie można było przewidzieć chwili zawarcia Umowy.
   3) dostarczony urządzenia UTM nie odpowiada parametrom określonym w opisie przedmiotu zamówienia,
   4) Wykonawca wykonuje przedmiot umowy wadliwie lub w sposób sprzeczny z umową, niezgodnie z uzgodnieniami lub zaleceniami Zamawiającego i pomimo wezwania do zmiany sposobu wykonania i wyznaczenia mu w tym celu odpowiedniego terminu nie wywiązuje się należycie z umowy.
   5) opóźnienie w realizacji umowy w odniesieniu do terminu wskazanego w § 1 ust. 2 wyniesie 5 dni

kalendarzowych od terminu o którym w § 1 ust.2 umowy.

2. Zamawiający może odstąpić od umowy bez wyznaczania dodatkowego terminu.
3. Oświadczenie Zamawiającego o odstąpieniu od umowy wymaga formy pisemnej i powinno być złożone w terminie 5 dni od ujawnienia okoliczności stanowiących podstawę dla odstąpienia od Umowy

§ 7

1. Osobami odpowiedzialnymi za prawidłową realizację niniejszej umowy są:
   1) po stronie Zamawiającego: …….. tel. …….. adres e-mail ……
   2) po stronie Wykonawcy …….. Tel. ……, e-mail: ……
2. Wszelkie powiadomienia i informacje, które Strony są zobowiązane sobie przekazywać w związku z zawarciem umowy, wymagają formy pisemnej i Strony zobowiązują się do ich doręczania przez pocztę na adresy:
   1) w przypadku ww. korespondencji pochodzącej od Wykonawcy adresem właściwym dla doręczeń Zamawiającego jest adres: ul. Wołoska 5, 02-675 Warszawa
   2) w przypadku ww. korespondencji pochodzącej od Zamawiającego adresem właściwym dla doręczeń Wykonawcy jest adres: ……
3. Zmiana osób wyznaczonych do bezpośrednich kontaktów i nadzoru nad prawidłowym wykonywaniem umowy oraz zmiana danych adresowych nie stanowi zmiany umowy i nie wymaga zawarcia aneksu. Strony zobowiązują się do wzajemnego powiadamiania o każdej zmianie osób, o których mowa w ust. 1 i adresu, o którym mowa w ust. 2. W razie zaniedbania tego obowiązku korespondencję wysłaną pod dotychczasowy adres uważa się za skutecznie doręczoną.

§ 8

Wykonanie umowy nie wiąże się z przetwarzaniem danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119 z 04.05.2016 r., dalej RODO) dla których Administratorem Danych Osobowych jest Zamawiający. Zamawiający oświadcza, iż realizuje obowiązki Administratora danych osobowych określone w przepisach RODO w zakresie danych osobowych Wykonawcy, w sytuacji gdy jest on osoba fizyczną w tym prowadzącą działalność gospodarczą, a także danych kontaktowych osób które Wykonawca wskazał ze swojej strony do realizacji umowy.

§ 9

1. Do umowy nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (,na podstawie art. 2 ust.1 pkt. 1 w zw. z art. 30.4 tej ustawy.
2. Wykonawca oświadcza, że znany jest mu fakt, iż treść niniejszej umowy, a w szczególności danego go identyfikujące, przedmiot umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej która podlega udostępnieniu w trybie przedmiotowej ustawy.
3. Wszelkie zmiany umowy z wyjątkiem odrębnych postanowień umowy, wymagają formy pisemnej pod rygorem nieważności.
4. Strony umowy stwierdzają, że zapoznały się z umową i dokonały interpretacji jej poszczególnych postanowień, w celu wyeliminowania ewentualnych, mogących powstać w przyszłości sporów na tle jej wykonania.
5. Poza innymi przypadkami wymienionymi w umowie Strony zastrzegają sobie możliwość dokonania zmiany postanowień umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w przypadku zajścia okoliczności, na które Strony nie miały wpływu, w tym tzw. „siły wyższej", a skutkujących

– bezpośrednio lub pośrednio – znacznym utrudnieniem lub uniemożliwieniem spełnienia świadczeń Stron w sposób określony przy podpisaniu umowy, o ile wyżej wymienione okoliczności mają charakter obiektywny.

6. Przez siłę wyższą rozumie się zdarzenie, którego przyczyny leżą poza kontrolą danej Strony, są nagłe i zewnętrzne, w tym między innymi takie przyczyny jak: wojna, embargo, akty normatywne lub decyzje administracji państwowej, zdarzenia losowe, powódź, pożar, strajki, epidemie lub pandemie chorób. Wystąpienie siły wyższej rozpatrywane będzie tak w skali kraju, jak w skali poszczególnych jednostek administracyjnych kraju, na których wystąpiły opisane wyżej zjawiska.
7. Strony umowy zobowiązują się do wzajemnego powiadamiania o zaistnieniu siły wyższej i dokonania stosownych ustaleń celem wyeliminowania możliwych skutków działania siły wyższej. Powiadomienia, o którym mowa należy dokonać pisemnie lub w inny dostępny sposób, niezwłocznie po fakcie wystąpienia siły wyższej. Do powiadomienia należy dołączyć dowody na poparcie zaistnienia siły wyższej. Nie można powoływać się na siłę wyższą w przypadku braku zawiadomienia zarówno o zaistnieniu jak i o ustaniu okoliczności siły wyższej, jak również nie przedstawienia dowodów, o których mowa powyżej.
8. Strony umowy zgodnie ustalają, że Wykonawca bez zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności nie może dokonać na rzecz osoby trzeciej cesji żadnych praw i roszczeń lub przeniesienia obowiązków wynikających z zamówienia na rzecz osoby trzeciej bez uprzedniej zgody Zamawiającego.
9. Umowa zostaje zawarta z dniem podpisania przez obie strony.
10. Klauza informująca o obowiązywaniu Procedury zgłoszeń wewnętrznych w Ośrodku Rozwoju Polskiej Edukacji za Granicą stanowi załącznik nr 3 do umowy,
11. W sprawach nieuregulowanych niniejszą umową obowiązują odpowiednie przepisy prawa a w szczególności ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny
12. Wszelkie spory powstałe na tle zawarcia jak i wykonania umowy Strony zobowiązują się rozstrzygać w sposób polubowny. Ewentualne spory Strony poddają sądowi powszechnemu właściwemu ze względu na siedzibę Zamawiającego.
13. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego i jeden dla Wykonawcy.

1. Załączniki:
   1) Opis przedmiotu zamówienia stanowiący załącznik nr 1 do umowy.
   2) Kopia oferty z dnia …… r. stanowiąca załącznik nr 2 do umowy.
   3) Klauzula informująca o obowiązywaniu Procedury zgłoszeń wewnętrznych w Ośrodku Rozwoju Polskiej Edukacji za Granicą. załącznik nr 3

ZAMAWIAJĄCY WYKONAWCA

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Załącznik nr 1 do umowy nr ……./2024/ORPEG z dnia …….. …….. 2024 r.

ZAPYTANIE OFERTOWE

XIII. Przedmiot zamówienia: Dostawa urządzeń UTM

XIV. Opis Przedmiotu zamówienia:

27. Definicje:
    27.1. Urządzenie UTM – wszystkie pozycje stanowiące przedmiot zamówienia
    27.2. oferta równoważna – oferta zgodna z informacjami zawartymi w specyfikacji sprzętu
28. Miejsce dostawy:
    28.1. Ośrodek Rozwoju Polskiej Edukacji za Granicą, ul. Wołoska 5, 02-675 Warszawa, do pomieszczeń znajdujących się na 4 piętrze. W budynku znajdują się windy. Dostawa w godzinach 7-15.
29. Termin realizacji zamówienia: do 15 dni od dnia podpisania umowy.
30. Wykaz zamawianych urządzeń UTM stanowi załącznik nr 1 do niniejszego zapytania ofertowego.
31. Wykonawca zobowiązany jest dostarczyć urządzenia UTM w oryginalnych opakowaniach producenta.
32. Oferowane produkty nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć.
33. Wsparcie techniczne producenta:
    33.1. Całodobowy dostęp do ekspertów technicznych, szybką reakcję na zgłoszenia serwisowe oraz możliwość wymiany sprzętu w trybie 24x7.
    33.2. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu urządzenia.
34. Wykonawca przekaże Zamawiającemu szczegółowe instrukcje obsługi i konserwacji dla każdej właściwej jednostki dostarczonego urządzenia UTM (może być w wersji elektronicznej).
35. Wykonawca przed podpisaniem umowy dostarczy deklarację zgodności CE oferowanego sprzętu.
36. Dostarczone urządzenia UTM muszą spełniać wszystkie wymogi bezpieczeństwa oraz zużycia energii obowiązujące w prawie polskim.
37. Dostarczone urządzenia UTM muszą spełniać kryteria środowiskowe.
38. Warunki gwarancji:
    13) Minimalne okresy gwarancji zostały wskazane w wykazie znajdującym się w niniejszym załączniku. Za dzień rozpoczęcia biegu terminu gwarancji uważa się dzień podpisania przez obie strony protokołu odbioru dostarczonego sprzętu.
    14) Zamawiający oczekuje gwarancji producenta sprzętu.
    15) Serwis urządzeń musi być realizowany na terenie Polski przez producenta lub autoryzowanego partnera Serwisowego Producenta.
    16) Serwis świadczony w siedzibie Zamawiającego.
    17) Czas reakcji serwisu – najpóźniej w pierwszym dniu roboczym następującym po dniu zgłoszenia awarii, o ile zgłoszenie nastąpi do godziny 17:00. W przypadku złożenia zgłoszenia po godzinie 17 za dzień zgłoszenia przyjmuje się dzień następny po dniu przesłania zgłoszenia.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

39. Wykonawca zobowiązany jest wskazać w ofercie nazwę sprzętu (typ, producent, model), który oferuje.

Załącznik nr 1 do zapytania ofertowego

Zamawiający wskazuje minimalne wymagania wobec poszczególnych pozycji stanowiących przedmiot zamówienia.

Urządzenie UTM - 2 sztuki wraz z gwarancja producenta i kontrolą aplikacji, IPS, antywirus, analizą typu Sandbox cloud, antyspam, web filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Opis przedmiotu zamówienia:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę 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 7 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

5. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
6. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
7. Monitoring stanu realizowanych połączeń VPN.
8. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

4. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.
5. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
6. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

8. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

9. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
10. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
11. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
14. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

14. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
15. Kontrola Aplikacji.
16. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
17. Ochrona przed malware.
18. Ochrona przed atakami - Intrusion Prevention System.
19. Kontrola stron WWW.
20. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
21. Zarządzanie pasmem (QoS, Traffic shaping).
22. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
23. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
24. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
25. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
26. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

8. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
9. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
10. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
11. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
12. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
13. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
14. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).

- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

3. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19, 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.
    - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
    - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
    - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
    - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
4. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
    - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

8. Routingu statycznego.
9. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
10. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
11. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
12. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
13. BFD (Bidirectional Forwarding Detection).
14. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Funkcje SD-WAN

3. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
4. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

5. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
6. System daje możliwość określania pasma dla poszczególnych aplikacji.
7. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
8. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

11. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
12. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
13. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
14. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
15. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
16. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
17. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
18. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
19. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
20. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

9. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
10. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
11. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
12. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
13. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
14. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
15. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
16. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

Kontrola aplikacji

7. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
8. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
9. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
10. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
11. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
12. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

10. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
11. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
12. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
13. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
14. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
15. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
16. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
17. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
18. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

5. System Firewall umożliwia weryfikację tożsamości użytkowników 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.
6. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
7. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
8. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

10. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
11. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

12. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
13. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
14. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
15. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
17. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
18. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

7. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
8. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
9. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
10. Możliwość włączenia logowania per reguła w polityce firewall.
11. System zapewnia możliwość logowania do serwera SYSLOG.
12. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

2. System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
    - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
    - Certyfikat ISO 9001 podmiotu serwisującego.

Wymagania dodatkowe

3. Spełnienie wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), uzyskania dokumentu pochodzącego od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami,

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl

technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4. Uzyskanie dokumentu - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Załącznik nr 2 do umowy nr ……./2024/ORPEG z dnia …….. …….. 2024 r.

Ośrodek Rozwoju Polskiej Edukacji za Granicą
ul. Wołoska 5, 02-675 Warszawa | tel. +48 22 622 37 92 | +48 22 622 37 93 | e-mail: orpeg@orpeg.pl | www.orpeg.pl