Podniesienie poziomu cyberbezpieczeństwa poprzez zakup urządzeń do zabezpieczenia brzegu sieci oraz wewnętrznej segmentacji sieci wraz z niezbędnym oprogramowaniem do analizy ruchu sieciowego.

|  |  |  |
| --- | --- | --- |
|  | Nazwa | Ilość [szt.] |
|  | Urządzenie do zabezpieczenia brzegu sieci oraz wewnętrznej segmentacji sieci | 4 |
|  | Wkładki SFP+ kompatybilne z dostarczanymi urządzeniami | 10 |
|  | System do uwierzytelniania logowania do urządzania sieciowego opisanego w poz. 1 na 100 użytkowników wraz ze wsparciem | 1 |
|  | Rozbudowa posiadanego przez Zamawiającego systemu do zbierania i analizy logów FortiAnalyzer o numerze seryjnym: FAZ-VM0000069622  (licencja na dodatkowe 30GB logów/dzień).  - dostarczane urządzenia muszą być włączone do użytkowanego systemu analizy logów. | 1 |

**Opis pozycji 1:**

|  |  |
| --- | --- |
| Zakup urządzenia do zabezpieczenia brzegu sieci oraz wewnętrznej segmentacji sieci – wymagane parametry: | Posiadanie wymaganego parametru TAK/NIE (zaznaczenie odpowiedzi NIE powoduje odrzucenie oferty) |
| * Liczba portów: |  |
| * Interfejs GE RJ45 minimum 10 |  |
| * Interfejs SFP 1 Gbps minimum 8 |  |
| * Interfejs 10GE SFP+ o niskim opóźnieniu pakietów (Low Latency) minimum 4 |  |
| * Interfejs 10GE SFP+ minimum 4 |  |
| * Interfejs zarządzający GE RJ45 |  |
| * Port USB minimum 1 |  |
| * Port konsolowy RJ45 |  |
| * Redundantne zasilacze minimum 2 sztuki |  |
| * Możliwość pracy w klastrze Active-Active |  |
| * Opóźnienie pakietów przez firewalla niższe niż 4,5μs |  |
| * Przepustowość silnika IPS minimum 12Gbps |  |
| * Przepustowość NGFW minimum 10 Gbps |  |
| * Przepustowość ochrony przed zagrożeniami minimum 9 Gbps |  |
| * Przepustowość zapory sieciowej dla IPv4 minimum (1518 / 512 / 64 byte, UDP) 79,5 / 78,5 / 70 Gbps |  |
| * Przepustowość zapory sieciowej (pakietów na sekundę) więcej niż 105 Mpps |  |
| * Ilość aktywnych sesji TCP więcej niż 7,8mln |  |
| * Ilość polityk bezpieczeństwa możliwych do skonfigurowania więcej niż 5tys |  |
| * Silniki bezpieczeństwa obsługiwane przez urządzenie: |  |
| * IPS |  |
| * Antivirus |  |
| * DNS Filtering |  |
| * WEB Filtering |  |
| * Application Control |  |
| * File Filter |  |
| * WAF (Web Application Firewall) |  |
| * SSL Inspection w czasie rzeczywistym również dla TLS 1.3 |  |
| * System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego oraz zapewnienie podstawowej ochrony przed atakami typu DDOS, DOS |  |
| * Przepustowość silnika SSL Inspection minimum 8Gbps |  |
| * Przepustowość silnika kontroli aplikacji (HTTP 64K) minimum 28 Gbps |  |
| * Obsługa SSL-VPN oraz IPSEC VPN |  |
| * Przepustowość SSL-VPN więcej niż 3,6Gbps |  |
| * Przepustowość szyfrowania IPsec VPN minimum 55Gbps |  |
| * Ilość aktywnych użytkowników SSL-VPN minimum 5tys |  |
| * Tunele VPN IPsec: Wsparcie dla IKE v2, obsługa AES 128 i 256, protokół DH minimum grupa 14 |  |
| * Obsługa SD-WAN: dynamiczny routing przy konfiguracji równoważenia obciążenia łączy |  |
| * Obsługa protokołów routingu dynamicznego takich jak BGP, OSPF, RIP. |  |
| * Traffic-Shaping – możliwość konfiguracji QOS (Quality of Service) |  |
| * Wbudowany Load Balancer |  |
| * Możliwość translacji adresów NAT, PAT |  |
| * Parametry techniczne urządzenia: |  |
| * Zasilanie: 100–240V AC, 50/60Hz |  |
| * Temperaturowy zakres pracy: od 0°C do 40°C |  |
| * Pracy przy wilgotność powietrza: od 5% do 90% |  |
| * Przepływ powietrza: przód-tył |  |
| * Urządzenie montowane do szafy RACK |  |
| * Licencje zapewniające działanie wyżej opisanych funkcjonalności |  |
| * Wsparcie 3-letnie świadczone co najmniej w trybie 8/5 bezpośrednio przez producenta i/lub przy współpracy z autoryzowanym partnerem producenta |  |
| * Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty |  |
| * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |  |
| * Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |  |
| * Wykonawca wraz z dostawą przełączników przedstawi oświadczenie producenta przełączników, które będzie potwierdzało, że przełączniki objęta są gwarancją na terenie Polski zgodną z wymaganiami Zamawiającego. Oświadczenie to musi zawierać informację o nr seryjnych przełączników, nr katalogowych przełączników, dane wykonawcy oraz dane klienta końcowego |  |
| * Wykonawca wraz z dostawą przełączników przeprowadzi wdrożenie obejmujące: |  |
| * + Konfiguracja klastra Active-Active na brzegu sieci, konfiguracja na każdym z urządzeń po jednym z operatorów ISP (routing BGP) wraz z odpowiednimi politykami WAN oraz politykami bezpieczeństwa. Migracja oraz odpowiednia konfiguracja wskazanych przez Zamawiającego Vlanów do wcześniej skonfigurowanego klastra. |  |
| * + W drugim etapie migracja konfiguracji oraz wszystkich polityk bezpieczeństwa z aktualnie posiadanego przez Zamawiającego klastra urządzeń Fortigate 501e na nowo zakupione urządzenia. Podłączenie sieciowe z przełącznikami rdzeniowymi za pomocą protokołu LACP. |  |
| * + Inżynier realizujący wdrożenie musi posiadać certyfikat techniczny wydany przez producenta urządzeń. |  |
|  |  |
| **Opis pozycji 3:** |  |
| System musi obsługiwać co najmniej: |  |
| • Uwierzytelnianie dla 100 użytkowników. |  |
| • 200 tokenów dla uwierzytelniania dwuskładnikowego. |  |
| • 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). |  |
| • Możliwość zdefiniowania co najmniej 10 grup użytkowników, |  |
| • 10 lokalnych centrów certyfikacji (CA). |  |
| • Możliwość wygenerowania 500 certyfikatów dla użytkowników. |  |
| • Uwierzytelnianie dla 2000 użytkowników w oparciu o dedykowaną aplikację (agenta), |  |
|  |  |
| Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: |  |
| * Lokalną, wbudowaną bazę użytkowników. |  |
| * Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. |  |
| * Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. |  |
| * Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. |  |
| * Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: |  |
| * + poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), |  |
| * + czasu ważności hasła, |  |
| * Konfigurowalną politykę blokowania kont, która będzie uwzględniać: |  |
| * + ilość nieudanych logowań, |  |
| * + czas blokowania konta, |  |
| * + okres nieaktywności, po którym konto jest blokowane. |  |
| * Możliwość odzyskiwania haseł: |  |
| * + z wykorzystaniem adresu email, |  |
| * + z wykorzystaniem pytania pomocniczego. |  |
| * Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować: |  |
| * + wbudowany serwer RADIUS, |  |
| * + integrację z zewnętrznymi serwerami RADIUS – praca jako klient. |  |
| * Obsługę protokołu LDAP, w tym zakresie system musi oferować: |  |
| * + wbudowany serwer LDAP, |  |
| * + możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). |  |
| * Obsługę protokołu SAML - Identity Provider (IdP) proxy. |  |
| * Realizację funkcji SSO (Single Sign On) w oparciu o: |  |
| * + integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny, |  |
| * + dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows, |  |
| * + kontekst użytkownika przesyłany z serwera RADIUS, |  |
| * + informacje uzyskiwane poprzez protokół Syslog, |  |
|  |  |
| Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż: |  |
| * Obsługę dla tokenów sprzętowych (hardware): |  |
| * + wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. |  |
| * Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. |  |
| * Dla tokenów na system iOS i Android wymaga się: |  |
| * + aktywacji z centralnego systemu uwierzytelniania (seed provisioning), |  |
| * + możliwości konfiguracji ilości generowanych cyfr (6 lub 8), |  |
| * + generowania kodu (cyfr) co 30 lub 60 sekund, |  |
| * + możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), |  |
| * + ochrony dostępu poprzez konfigurowalny kod PIN, |  |
|  |  |
|  |  |
| System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: |  |
| * Obsługa wbudowanego CA (Certificate Authority). |  |
| * Obsługa CA pośredniczących (Intermediate CA). |  |
| * Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. |  |
| * Możliwość pobrania wygenerowanych certyfikatów. |  |
| * Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. |  |
| * Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. |  |
| * Możliwość generowania certyfikatów typu wildcard. |  |
| * Realizacja CRL (Certificate Revocation List). |  |
| * Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). |  |
| * Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
|  |  |
|  |  |
| Zarządzanie |  |
| * Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. |  |
| * System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. |  |
| * Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. |  |
| * Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |

Serwis, szkolenia i usługi

Wymaga się aby dostawa obejmowała również serwis producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.