

System Zdalnego dostępu VPN w oparciu o sprzęt i oprogramowanie opisane poniżej.

Koncentrator VPN (z funkcjonalnością Firewall i IPS) 2 szt.

1. Urządzenie o konstrukcji niemodularnej zapewniające:

- Wydajność przy pracy jako firewall co najmniej 1,2Gb/s (IPv4 i IPv6).
- Wydajność przy pracy jako firewall dla ruchu multi-protocol co najmniej 600Mb/s.
- Wydajność przy pracy z włączoną funkcjonalnością firewall i systemu wykrywania włamań (IPS) co najmniej 400 Mb/s.
- Obsługę co najmniej 250.000 jednoczesnych połączeń.
- Możliwość zestawiania co najmniej 15.000 połączeń na sekundę.
- Wydajność nie mniejszą niż 500.000 pakietów na sekundę dla pakietów 64-bajtowych.

2. Urządzenie musi zapewniać co najmniej 250 Mb/s dla szyfrowania VPN algorytmami 3DES/AES.

3. Urządzenie musi pozwalać na obsługę jednocześnie co najmniej 250 tuneli IPsec.

4. Urządzenie musi posiadać co najmniej 6 interfejsów Gigabit Ethernet 10/100/1000BASE-T oraz możliwość rozbudowy o dodatkowe 6 portów miedzianych Gigabit Ethernet 10/100/1000BASE-T lub 6 portów Gigabit Ethernet definiowanych wkładkami SFP.

5. Urządzenie musi obsługiwać ramki Ethernet typu Jumbo (9216 bajtów).

6. Urządzenie musi obsługiwać co najmniej 100 VLANów.

7. Urządzenie musi pozwalać na wirtualizację konfiguracji poprzez wirtualne firewalle/konteksty. Wymagana jest obsługa co najmniej 2 wirtualnych kontekstów Firewall oraz możliwość rozszerzenia ilości obsługiwanych wirtualnych kontekstów firewall do co najmniej 5.

8. Urządzenie musi umożliwiać grupowanie VLANów w trybie pracy jako transparent firewall (Firewall warstwy 2) – minimum 4 grup po 4 VLANy (funkcjonalność możliwa do uruchomienia dla IPv4 i IPv6).

9. Urządzenie musi posiadać co najmniej 8 GB pamięci RAM i 8 GB pamięci Flash.

10. Urządzenie musi umożliwiać dostęp administracyjny do interfejsu zarządzania w oparciu o role (RBAC).
11. Urządzenie musi posiadać co najmniej 1 dedykowany interfejs zarządzający GigabitEthernet (Out-of-Band management).
12. Urządzenie musi posiadać co najmniej 2 porty USB z możliwością obsługi systemu plików na kluczach USB.
13. Urządzenie musi posiadać port konsoli.
14. Urządzenie musi pozwalać na realizację modelu wdrożenia w wysokiej dostępności dla IPv4 i IPv6 w trybach
 - Active-Standby
 - Active-Active
15. Urządzenie musi być zasilane prądem zmiennym 230V.
16. Urządzenie musi mieć możliwość montażu w szafie Rack 19". Wysokość urządzenia nie może być większa niż 1RU.
17. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
18. Rozwiązanie musi umożliwiać pracę firewalla w trybie warstwy 3 (routed) i warstwy 2 (transparentnym).
19. Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się z usługą katalogową Microsoft Active Directory
20. Rozwiązanie musi zapewnić mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
 - Hypertext Transfer Protocol (HTTP)
 - File Transfer Protocol (FTP)
 - Simple Mail Transfer Protocol (SMTP)
 - Domain Name System (DNS)
 - H.323
 - Session Initiation Protocol (SIP)
 - Lightweight Directory Access Protocol (LDAP)
 - Internet Control Message Protocol (ICMP)
 - Network File System (NFS)

21. Rozwiązanie musi zapewniać mechanizmy pozwalające na blokowanie aplikacji tunelowanych z użyciem portu 80 w tym:
- blokowanie komunikatorów internetowych
 - blokowanie aplikacji typu peer-to-peer
22. Urządzenie musi zapewniać obsługę protokołów routingu dynamicznego OSPF oraz RIPv2
23. Urządzenie musi zapewniać obsługę ruchu multicast w tym
- Protokoły routingu multicast (PIM)
 - IGMP
 - definiowanie list kontroli dostępu dla ruchu multicast
24. Urządzenie musi zapewniać obsługę ruchu z adresacją IPv6
- pracę w sieci z adresacją IPv6
 - definiowanie list kontroli dostępu dla ruchu IPv6
 - inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń
 - Hop-by-Hop Options,
 - Routing (Type 0),
 - Fragment,
 - Destination Options,
 - Authentication,
 - Encapsulating Security Payload
 - zarządzanie urządzeniem poprzez SSHv2, HTTPS w sieci IPv6
25. Urządzenie musi obsługiwać protokoły IKE i IKEv2.
26. Urządzenie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPsec z IKEv2 dla dostępu zdalnego w oparciu o klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat).
27. Urządzenie musi obsługiwać współpracę z serwerami certyfikatów (CA) oraz posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS.
28. Urządzenie musi posiadać funkcjonalność sondy IPS (Intrusion Prevention System). Sonda IPS musi realizować co najmniej następujące funkcje:
- Umożliwiać pracę w trybie IPS (In-line);

- Umożliwiać identyfikację, klasyfikację i powstrzymywanie ruchu zagrażającego bezpieczeństwu organizacji w tym:
 - robaki sieciowe
 - adware
 - spyware
 - wirusy sieciowe
 - trojany
 - nadużycia aplikacyjne
 - wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii
 - posiadać wbudowane co najmniej 5000 sygnatur ataków
 - umożliwiać definicje reakcji z dokładnością do jednej sygnatury
 - umożliwiać grupowanie sygnatur ataków
 - umożliwiać tworzenie zdarzeń opisanych przez naruszenie kilku niezależnych sygnatur ataku
 - umożliwiać określenie znaczenia ataku na podstawie kilku zmiennych w szczególności: znaczenia atakowanego systemu, znaczenia naruszonej sygnatury oraz prawdopodobieństwa ataku.
 - umożliwiać indywidualne (przez administratora) definiowanie poziomu zagrożenia dla sygnatury
 - zapewniać mechanizm notyfikacji administratora o zaistniałym ataku (co najmniej przez e-mail)
 - umożliwiać zarządzanie przez linię komend, graficznie przez przeglądarkę internetową oraz powinna być dostępna dedykowana aplikacja;
 - umożliwiać zdefiniowanie co najmniej 4 wirtualnych sensorów
29. Urządzenie musi posiadać możliwość wyeksportowania konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
30. Urządzenie musi być zarządzane przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia oraz z wykorzystaniem interfejsu komend (CLI).
31. Wymagane jest aby oferowane urządzenia były w pełni kompatybilne, w zakresie obsługiwanych funkcjonalności VPN z obecnie posiadanym przez Zamawiającego systemem zdalnego dostępu pracującym w oparciu o oprogramowanie Cisco IOS

(koncentrator VPN) i oprogramowania klienckiego (Cisco VPN Client) zainstalowanego na stacjach użytkowników pracujących w sieci PAŻP.

32. Urządzenie musi być fabrycznie nowe, nie używane wcześniej w innych projektach. Nie dopuszcza się rozwiązań typu „refurbish” itp.

33. Dostarczany sprzęt musi być objęty 36-miesięcznym (3 lata) serwisem opartym na bezpośrednim serwisie producenta urządzenia świadczonym w reżimie 8x5xNBD (czas naprawy 8h, 5 dni w tygodniu, naprawa w następnym dniu roboczym). W ramach w/w serwisu należy zapewnić subskrypcję sygnatur IPS na okres 36 miesięcy.

System (oprogramowanie) do uwierzytelnienia, autoryzacji i rozliczania dostępu do urządzeń sieciowych. - 2 licencje.

1. System musi wspierać protokół RADIUS zgodnie z dokumentami
 - RFC 2138—Remote Authentication Dial In User Service (RADIUS)
 - RFC 2139—RADIUS Accounting
 - RFC 2865—Remote Authentication Dial In User Service (RADIUS)
 - RFC 2866—RADIUS Accounting
 - RFC 2867—RADIUS Accounting for Tunnel Protocol Support
 - RFC 2868—RADIUS Attributes for Tunnel Protocol Support
 - RFC 2869—RADIUS Extensions
2. System musi umożliwiać konfigurację dodatkowych atrybutów RADIUS Vendor Specific Attributes (VSA) niezdefiniowanych w domyślnych słownikach.
3. System musi wspierać co najmniej następujące protokoły uwierzytelniania: PAP/ASCII, EAP-MD5 oraz CHAP.
4. System musi wspierać protokół TACACS+
5. System musi wspierać zaawansowane funkcje protokołu TACACS+ a w tym:
 - zmianę haseł użytkowników za pomocą TACACS+
 - definicję dodatkowych atrybutów, które mogą być użyte w odpowiedziach autoryzacji
 - wspierać inne usługi (services) niż shell
 - umożliwiać przekazywanie (relay) zapytań protokołu TACACS+ do zdalnych serwerów AAA i przekazywanie odpowiedzi do urządzeń sieciowych.

- Metody uwierzytelnienia MSCHAP i CHAP
 - Możliwość podstawienia wartości atrybutu TACACS+ wartością innego atrybutu z jednego z dostępnych w dynamicznych słownikach dla konfiguracji profili dostępu do powłoki (shell profiles).
6. System musi umożliwiać wykonanie procesu uwierzytelnienia w oparciu o następujące repozytoria użytkowników:
- wewnętrzna baza użytkowników
 - Active Directory Windows AD 2003, 2008 oraz 2008 R2
 - dostępne przez LDAP/LDAPS
 - RSA Secure ID Server
 - RADIUS OTP zgodnie z RFC 2865
7. Wewnętrzne repozytorium użytkowników musi umożliwiać:
- ustawienie polityki wygasania hasła
 - śledzenie historii zmian hasła w celu zapobiegania ponownego użycia identycznego hasła
 - zmianę hasła użytkownika przy pomocy formularza webowego
 - wyłączenie konta użytkownika jeżeli data jest poza skonfigurowanym przedziałem czasowym lub gdy użytkownik przekroczył maksymalną ilość nieudanych logowań
8. System musi pozwalać na sekwencyjne wykorzystanie kolejnego repozytorium do uwierzytelnienia użytkownika, jeśli:
- użytkownik nie został odnaleziony w repozytorium
 - repozytorium w sekwencji nie jest dostępne
 - system nie może połączyć się z repozytorium
9. System musi umożliwiać ograniczenie ilości jednoczesnych sesji per użytkownik.
10. System musi umożliwiać zarządzanie za pomocą graficznego interfejsu użytkownika dostępnego przez co najmniej następujące przeglądarki internetowe:
- Mozilla Firefox w wersji co najmniej 4.x dla Linux RedHat, MAC OS 10.5 oraz Microsoft Windows XP/Vista/7.
 - Internet Explorer w wersji co najmniej 8.0

11. System musi umożliwiać zapewnienie zaawansowanego bezpieczeństwa dostępu do interfejsu administracyjnego realizując co najmniej następujące funkcje:

- konfigurację polityki wygasania hasła i wyłączenie konta administratora na podstawie nieaktywności lub nieudanych prób logowania
- konfigurację listy adresów IP, z których administratorzy mają dostęp do interfejsu administracyjnego
- konfigurację certyfikatu serwera dla dostępu przy pomocy protokołu HTTPS z możliwością wygenerowania żądania wystawienia certyfikatu (CSR)
- przypisanie ról określających prawa dostępu do określonych elementów interfejsu administracyjnego (Role Based Access Control)

12. System musi umożliwiać tworzenie raportów dla potrzeb zarządzania zawierających:

- listę administratorów systemu wraz z przypisanymi do każdego z nich przywilejami
- listę aktywnych sesji RADIUS
- listę zmian haseł przez wewnętrznych użytkowników systemu
- listę prób logowania administratorów systemu wraz z kontami, które zostały wyłączone
- listę operacji przeprowadzonych w systemie przez administratorów i samodzielnie przez system

13. System musi wspierać możliwość wykonywania operacji tworzenia, odczytu, uaktualniania i usuwania obiektów konfiguracji przy pomocy skryptów.

14. System musi umożliwiać konfigurację kopii zapasowej konfiguracji (backup) za pomocą interfejsu graficznego zarządzania z opcją natychmiastowego backupu na żądanie i opcją zaplanowania backupu w przyszłości.

15. System musi umożliwiać wykonanie inkrementalnej kopii zapasowej systemu, gdzie pełna kopia zapasowa wykonywana jest tylko za pierwszym razem.

16. System musi umożliwiać kopiowanie plików do i z systemu w sposób bezpieczny.

17. System musi wspierać protokół SNMP dla realizacji usługi logowania zdarzeń.
Wymagane jest wsparcie dla agenta w trybie read-only dla SNMPv1 i SNMPv2c.
18. System musi wspierać co najmniej następujące bazy MIB protokołu SNMP: SNMPv2-MIB, RFC1213-MIB (MIB II), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, CISCO-CDP-MIB oraz ENTITY-MIB.
19. System musi umożliwiać powiadamianie o zdarzeniach przy pomocy protokołu syslog.
20. System musi umożliwiać pracę w klastrze typu active-standby.
21. Zmiany konfiguracji wykonywane w interfejsie administracyjnym aktywnego węzła klastra active-standby muszą automatycznie replikować się na węzeł zapasowy.
22. System należy dostarczyć z licencjami umożliwiającymi instalację dwóch wirtualnych instancji systemu pracujących w klastrze active-standby pod kontrolą hypervisora VMware ESXi w wersji 4.1 lub 5.0.
23. Zamawiający zobowiązuje się dostarczyć zasoby serwerowe, na których zostaną uruchomione wirtualne instancje systemu. Dla jednej instancji wirtualnej systemu Zamawiający może dedykować nie więcej zasobów niż:
 - 2 procesory
 - 4GB pamięci RAM
 - 750 GB przestrzeni dyskowej
 - 1 karta sieciowa

Oprogramowanie należy dostarczyć wraz z 3 letnim kontraktem serwisowym uprawniającym w reżimie 8x5xNBD do korzystania ze wsparcia technicznego producenta systemu oraz dostępu do aktualizacji (np. z wersji x.1 do x.2).

Certyfikat SSL wystawiony przez publiczne CA, na pojedynczą domenę internetową, ważny przez 3 lata, rozpoznawany domyślnie przez przeglądarki internetowe takie jak: Internet Explorer 8, Firefox, Chrome oraz systemy mobilne takie jak Android i Apple iOS. - 1 szt.

Szkolenie autoryzowane przez producenta sprzętu, w zakresie administracji i konfiguracji usług zdalnego dostępu (VPN) dla 3 osób, zawierające min. następujące zagadnienia szkoleniowe:

- Tworzenie bezpiecznych zapór sieciowych.
- Budowa bezpiecznych wirtualnych sieci prywatnych z użyciem protokołu IPSec.
- Zaawansowane funkcje protokołu IPSec wykorzystywane w sieciach VPN.
- Implementacja funkcjonalności PKI.
- Bezpieczny dostęp do infrastruktury sieciowej z wykorzystaniem dostępnych rozwiązań SSL VPN.
- Diagnostyki i analiz stanu pracy połączeń VPN.
- Metodologii diagnostyki problemów związanych z działaniem połączeń VPN.
- Wysoka dostępność i niezawodność połączeń VPN.
- Konfiguracja połączeń VPN typu site-to-site.
- Konfiguracja zaawansowanych funkcjonalności dla sieci VPN typu site-to-site.
- Konfiguracja połączeń VPN typu remote access.
- Konfiguracja zaawansowanych funkcjonalności dla połączeń typu remote access.
- Konfiguracja rozwiązania SSL VPN: Clientless.
- Konfiguracja rozwiązania SSL VPN: Thin Client.
- Zaawansowane metody uwierzytelniania dla rozwiązań SSL VPN.

Usługi wdrożenia:

W ramach niniejszego kontraktu Wykonawca będzie zobowiązany do:

- Dostawy na swój koszt sprzętu i oprogramowania do siedziby Zamawiającego.
- Instalacji i konfiguracji Sprzętu z wykorzystaniem pełnej funkcjonalności typu Failover oraz konfiguracji zdalnego dostępu typu IPSEC oraz ClientLess VPN (WebVPN) w oparciu o autoryzacje i autentykacje na podstawie certyfikatów.
- Instalacji Oprogramowania oraz jego konfiguracji i integracji z posiadanym przez Zamawiającego środowiskiem Windows Active Directory.
- Migracji konfiguracji i ustawień z obecnie pracującego w PAŻP systemu VPN zbudowanego w oparciu o klientów Cisco VPN client ver. 5.x i oprogramowanie Cisco IOS do nowego systemu zdalnego dostępu będącego przedmiotem Zamówienia.
- Testów funkcjonalnych całego systemu.