

Zakres usługi wdrożenia urządzeń do zabezpieczenia infrastruktury IT zamawiającego przed dostępem z zewnątrz.

Usługa obejmuje uruchomienie, podstawową konfigurację oraz przygotowanie urządzenia do pracy w środowisku klienta zgodnie z uzgodnionymi założeniami technicznymi.

1. Konfiguracja sieciowa urządzenia

W ramach konfiguracji sieciowej wykonane zostaną podstawowe ustawienia niezbędne do poprawnej pracy urządzenia w infrastrukturze klienta, w szczególności:

- konfiguracja interfejsów sieciowych,
- przypisanie adresacji IP do wskazanych interfejsów,
- konfiguracja masek sieci, bram domyślnych oraz podstawowych parametrów komunikacyjnych,
- konfiguracja routingu statycznego zgodnie z przekazaną topologią sieci,
- weryfikacja podstawowej komunikacji pomiędzy wskazanymi segmentami sieci,
- dostosowanie ustawień sieciowych do istniejącej infrastruktury klienta.

Wykonawca zobowiązany jest do samodzielnego rozpoznania środowiska technicznego Zamawiającego w ramach obowiązkowej wizji lokalnej przeprowadzonej przed złożeniem oferty. Zamawiający nie przewiduje przekazania kompletnej dokumentacji technicznej środowiska, w szczególności schematów sieci, pełnej adresacji IP, konfiguracji VLAN, bram, podsieci ani szczegółowych kierunków komunikacji.

Wszelkie informacje niezbędne do prawidłowej wyceny, doboru sposobu realizacji oraz późniejszego wdrożenia Wykonawca powinien pozyskać i zweryfikować samodzielnie podczas wizji lokalnej. Złożenie oferty oznacza, że Wykonawca zapoznał się z warunkami technicznymi środowiska Zamawiającego i uwzględnił je w cenie oraz zakresie prac.

2. Konfiguracja zapory sieciowej firewall

W ramach usługi zostanie wykonana podstawowa konfiguracja polityk bezpieczeństwa firewall zgodnie z uzgodnionymi wymaganiami klienta.

Zakres obejmuje:

- przygotowanie podstawowej struktury reguł firewall,
- konfigurację reguł dopuszczających wymagany ruch sieciowy,
- ograniczenie ruchu niepożądanego zgodnie z dobrymi praktykami bezpieczeństwa,

- uporządkowanie reguł według kierunków komunikacji lub segmentów sieci,
- weryfikację poprawności działania skonfigurowanych polityk.

Limit standardowej konfiguracji obejmuje maksymalnie **20 reguł firewall**.

Reguły powyżej wskazanego limitu mogą zostać wykonane jako prace dodatkowe, po wcześniejszym uzgodnieniu zakresu i czasu realizacji.

3. Konfiguracja NAT

W ramach wdrożenia zostanie wykonana konfiguracja translacji adresów sieciowych NAT, zgodnie z potrzebami środowiska klienta.

Zakres obejmuje:

- konfigurację podstawowych reguł NAT dla ruchu wychodzącego,
- konfigurację reguł NAT dla wskazanych usług publikowanych,
- przygotowanie translacji adresów zgodnie z wymaganiami klienta,
- weryfikację poprawności działania skonfigurowanych reguł.

Limit standardowej konfiguracji obejmuje maksymalnie **10 reguł NAT**.

Dodatkowe reguły NAT wykraczające poza powyższy limit będą traktowane jako prace dodatkowe.

4. Integracja z usługą katalogową lub baza użytkowników lokalnych

Wdrożenie obejmuje integrację urządzenia z istniejącą usługą katalogową Active Directory albo przygotowanie wewnętrznej bazy użytkowników na urządzeniu.

Zakres obejmuje jedną z poniższych opcji:

- integrację z Active Directory,
- konfigurację połączenia z kontrolerem domeny,
- konfigurację podstawowych parametrów autoryzacji,
- weryfikację poprawności komunikacji z usługą katalogową,

Zakres nie obejmuje masowego dodawania użytkowników, importu użytkowników, tworzenia grup bezpieczeństwa po stronie Active Directory ani zarządzania kontami użytkowników.

5. Konfiguracja dostawców Internetu

W ramach usługi zostanie wykonana konfiguracja połączeń WAN dla maksymalnie **2 dostawców Internetu**.

Zakres obejmuje:

- konfigurację interfejsów WAN,
- konfigurację adresacji publicznej lub prywatnej zgodnie z parametrami operatora,
- konfigurację bram operatorów,
- weryfikację dostępności Internetu,
- podstawową konfigurację pracy z jednym lub dwoma łączami,
- podstawową konfigurację routingu dla ruchu wychodzącego.

6. Konfiguracja VPN

W ramach wdrożenia zostanie wykonana podstawowa konfiguracja dostępu VPN zgodnie z przekazanymi parametrami oraz wymaganiami klienta.

6.1. IPSec Site-to-Site

Zakres obejmuje konfigurację maksymalnie **2 tuneli IPSec Site-to-Site**.

W ramach konfiguracji wykonane zostaną:

- konfiguracja parametrów tunelu IPSec zgodnie z danymi przekazanymi przez klienta,
- konfiguracja adresacji lokalnej i zdalnej,
- konfiguracja polityk dostępu dla ruchu przez tunel,
- konfiguracja podstawowego routingu dla ruchu VPN,
- uruchomienie tunelu,
- podstawowa weryfikacja zestawienia tunelu i komunikacji pomiędzy wskazanymi sieciami.

Konfiguracja tuneli realizowana jest na podstawie kompletnych danych przekazanych przez klienta, takich jak adresy publiczne peerów, sieci lokalne i zdalne, parametry IKE/IPSec, klucze współdzielone, metody szyfrowania, czasy życia i inne wymagane ustawienia.

Zakres nie obejmuje konfiguracji urządzeń po stronie zdalnej, chyba że zostanie to osobno ustalone.

6.2. Client-to-Site / SSL VPN

Zakres obejmuje konfigurację dostępu VPN dla użytkowników zdalnych, w tym:

- konfigurację funkcji Client-to-Site na urządzeniu,
- konfigurację podstawowych parametrów dostępu zdalnego,
- konfigurację jednej wzorcowej stacji klienckiej,
- uruchomienie maksymalnie jednego przykładowego połączenia SSL VPN,
- weryfikację poprawności logowania i podstawowego dostępu do wskazanych zasobów.

Zakres nie obejmuje instalacji i konfiguracji klienta VPN na wszystkich komputerach użytkowników końcowych, masowego wdrożenia oprogramowania VPN, konfiguracji GPO ani indywidualnego wsparcia dla użytkowników końcowych. Takie czynności mogą zostać zrealizowane jako prace dodatkowe.

7. Analiza logów i konfiguracja ochrony protokołów przemysłowych

W ramach wdrożenia zostanie przeprowadzona podstawowa analiza logów generowanych przez urządzenie oraz ruchu widocznego w środowisku, w celu dostosowania ochrony do charakterystyki komunikacji przemysłowej.

Zakres obejmuje:

- przegląd podstawowych logów komunikacyjnych,
- identyfikację widocznych protokołów przemysłowych,
- analizę podstawowych zdarzeń bezpieczeństwa,
- dostosowanie wybranych ustawień ochrony do obserwowanego ruchu,
- konfigurację ochrony protokołów przemysłowych zgodnie z możliwościami urządzenia,
- weryfikację, czy zastosowane ustawienia nie blokują wymaganej komunikacji produkcyjnej lub technologicznej.

Analiza ma charakter wdrożeniowy i konfiguracyjny. Nie stanowi pełnego audytu bezpieczeństwa OT/ICS, testu penetracyjnego ani szczegółowej analizy ryzyka środowiska przemysłowego.

8. Uruchomienie i konfiguracja IDS

W ramach usługi zostanie uruchomiona i skonfigurowana funkcja IDS, czyli system detekcji włamań i podejrzanych aktywności sieciowych.

Zakres obejmuje:

- aktywację funkcji IDS,
- konfigurację podstawowych profili detekcji,
- przypisanie IDS do właściwych interfejsów lub kierunków ruchu,
- dostosowanie podstawowych ustawień detekcji do charakteru środowiska,
- weryfikację generowanych zdarzeń,
- podstawową korektę konfiguracji w celu ograniczenia fałszywych alarmów na etapie uruchomienia.

Zakres obejmuje uruchomienie IDS w modelu detekcyjnym.

9. Testy i weryfikacja działania

Po zakończeniu konfiguracji wykonana zostanie podstawowa weryfikacja poprawności działania wdrożonych funkcji.

Zakres obejmuje:

- test podstawowej komunikacji sieciowej,
- test dostępu do Internetu,
- test działania reguł firewall w uzgodnionym zakresie,
- test działania wybranych reguł NAT,
- test zestawienia tuneli VPN,
- test przykładowego połączenia SSL VPN,
- weryfikację podstawowych logów systemowych i bezpieczeństwa,
- potwierdzenie działania IDS oraz ochrony protokołów przemysłowych w podstawowym zakresie.

10. Przekazanie wdrożenia

Po zakończeniu prac wdrożeniowych klient otrzyma podstawowe podsumowanie wykonanej konfiguracji.

Zakres przekazania obejmuje:

- informację o wykonanych pracach,
- zestawienie skonfigurowanych głównych funkcji,
- potwierdzenie uruchomienia urządzenia,
- wskazanie ewentualnych ograniczeń, zaleceń lub prac dodatkowych,
- przekazanie informacji niezbędnych do dalszej eksploatacji urządzenia,
- przekazanie danych dostępowych do wszystkich wdrożonych urządzeń.