Rekomendacje ustawień bezpieczeństwa dla rejestratorów NOVUS IP 6000

SPIS TREŚCI

pl

Spis treści

INFORMACJE WSTĘPNE

1.Informacje wstępne

Poniższa instrukcja opisuje rekomendowane ustawienia dla rejestratorów IP Novus serii 6000, umożliwiające w odpowiedni sposób chronić dostęp do urządzania oraz dane na nim przetwarzane.
Dostępność opisywanych funkcji zależna jest od wersji oprogramowania zainstalowanej w rejestratorze.

Obszary:

- wstępna konfiguracja
- nadawanie uprawnień / zarządzanie kontami
- polityka haseł
- konfiguracja sieciowa urządzenia
- zdalny dostęp

2.Wstępna konfiguracja

2.1. Konta i dostęp

2.1.1. Rekomendacje dotyczące dostępu do systemu

- rejestrator powinien być zlokalizowany w bezpiecznym miejscu uniemożliwiającym dostęp do niego osobom nieupoważnionym (np. serwerownia, zamykane pomieszczenie itp.)
- system powinien być aktualizowany na bieżąco pod kątem poprawek dotyczących bezpieczeństwa
- urządzenia łączące się zdalnie do systemu powinny posiadać wsparcie producenta i być na bieżąco aktualizowane
- każdy z użytkowników systemu powinien posiadać własne, imienne konto, które w łatwy sposób można powiązać z konkretną osobą
- uprawnienia w systemie powinny być nadawane poprzez członkostwo w grupach. Domyślnie w systemie skonfigurowane są trzy grupy uprawnień :
  -Administratora
  - Zaawansowane
  - Zwykły
- uprawnienia do systemu powinny być nadawane na podstawie zgody właściciela systemu bądź osoby do tego uprawnionej
- raz na pół roku powinna odbywać się weryfikacja aktywnych kont w systemie (weryfikacja powinna być wykonywana przez właściciela systemu bądź osoby do tego uprawnione)
- dostęp administracyjny powinien być nadany tylko i wyłącznie osobie odpowiedzialnej za konfigurację systemu (grupa uprawnień: „Administratora")
- wbudowane konto „root" powinno być odpowiednio zabezpieczone i wykorzystywane w nagłych przypadkach

  ◊ hasło do konta powinno zostać spisane oraz odpowiednio zabezpieczone (kartka, PenDrive bądź inne medium zlokalizowane w bezpiecznym miejscu , np. sejf)
  ◊ hasło do konta
  - losowe
  - min. 16 znaków
  - posiada minimum 2 znaki specjalne
  - zawiera minimum jedną cyfrę oraz jedną dużą literę
  - nie zawiera wyrazów słownikowych
  - nie zawiera słowa root w haśle

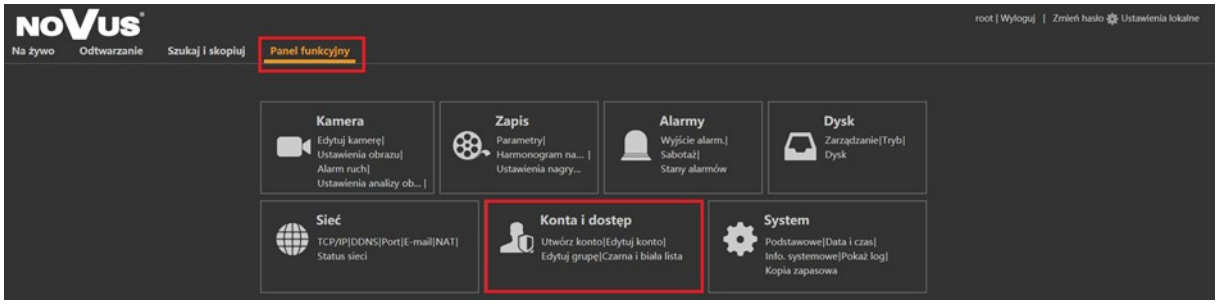
SCZEGÓŁOWA KONFIGURACJA

pl

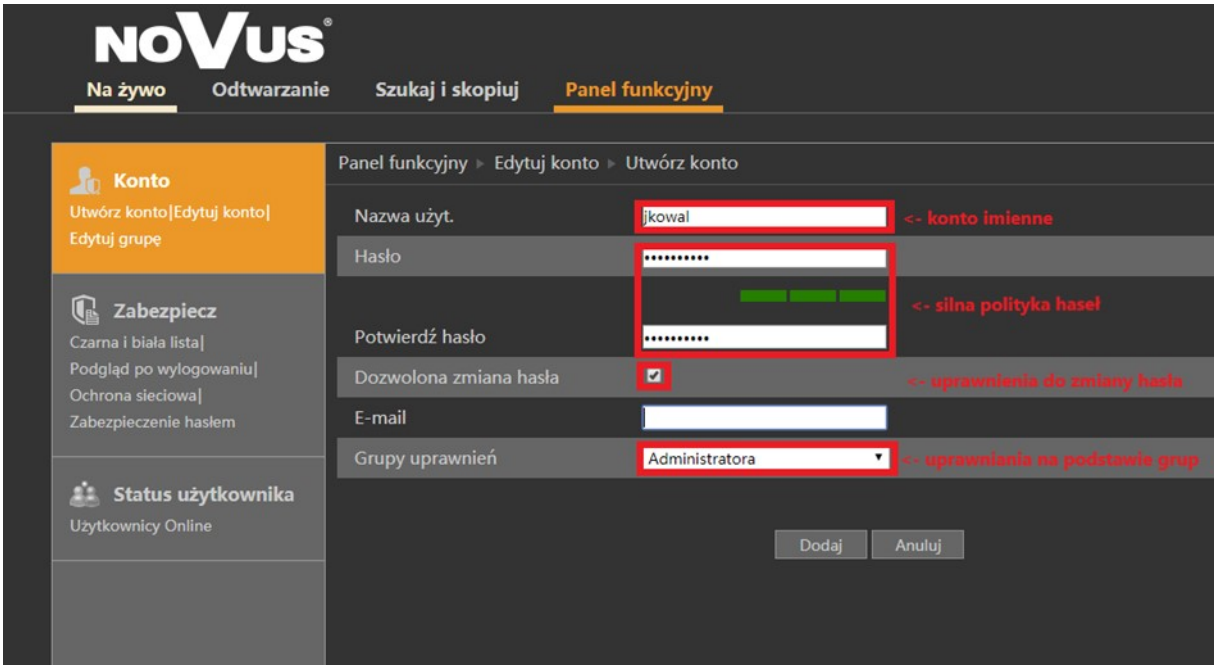
- polityka haseł oraz rekomendowane ustawienia haseł dla pozostałych kont
  - Panel funkcyjny -> Zabezpieczenia hasłem
    - Poziom: **„Silne”**
    - Data ważności: **„90 dni”**
  - polityka haseł
    - losowe
    - min. 8 znaków
    - posiada minimum 2 znaki specjalne
    - zawiera minimum jedną cyfrę oraz jedną dużą literę
    - nie zawiera wyrazów słownikowych
    - nie zawiera nazwy użytkownika w haśle
    - hasło zmieniane minimum co 90 dni

2.1.2 Szczegółowa konfiguracja

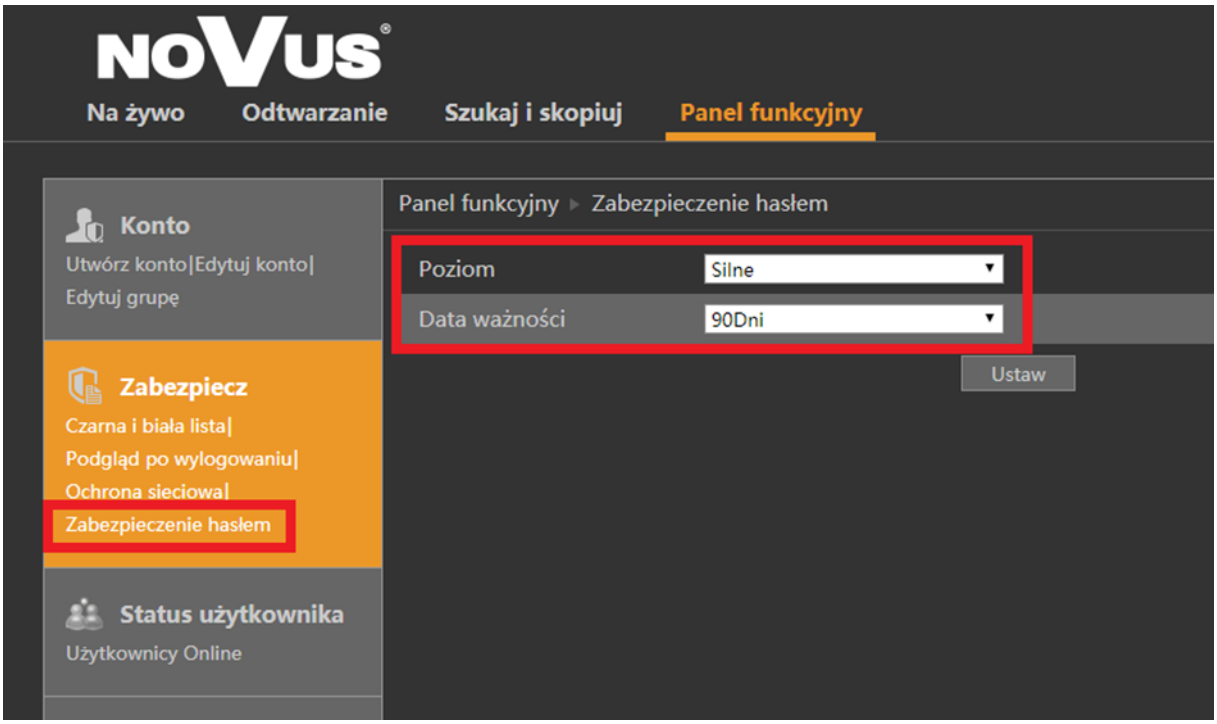
W *„Panelu funkcyjnym”* wymieramy opcję *„Konta i dostęp”*



Tworzenie nowego konta
Panel funkcyjny -> Konta i dostęp -> Utwórz konto



Ustawienia polityki haseł
Panel funkcyjny -> Konta i dostęp -> Zabezpieczenie hasłem



2.2. Konfiguracja sieciowa

2.2.1 Konfiguracji sieci LAN

Rekomendowany jest fizyczny dostęp do rejestratora IP (podłączone urządzenia peryferyjne oraz monitor). Szczególnie dotyczy to dostępu z uprawnieniami administratora w celu konfiguracji urządzenia.

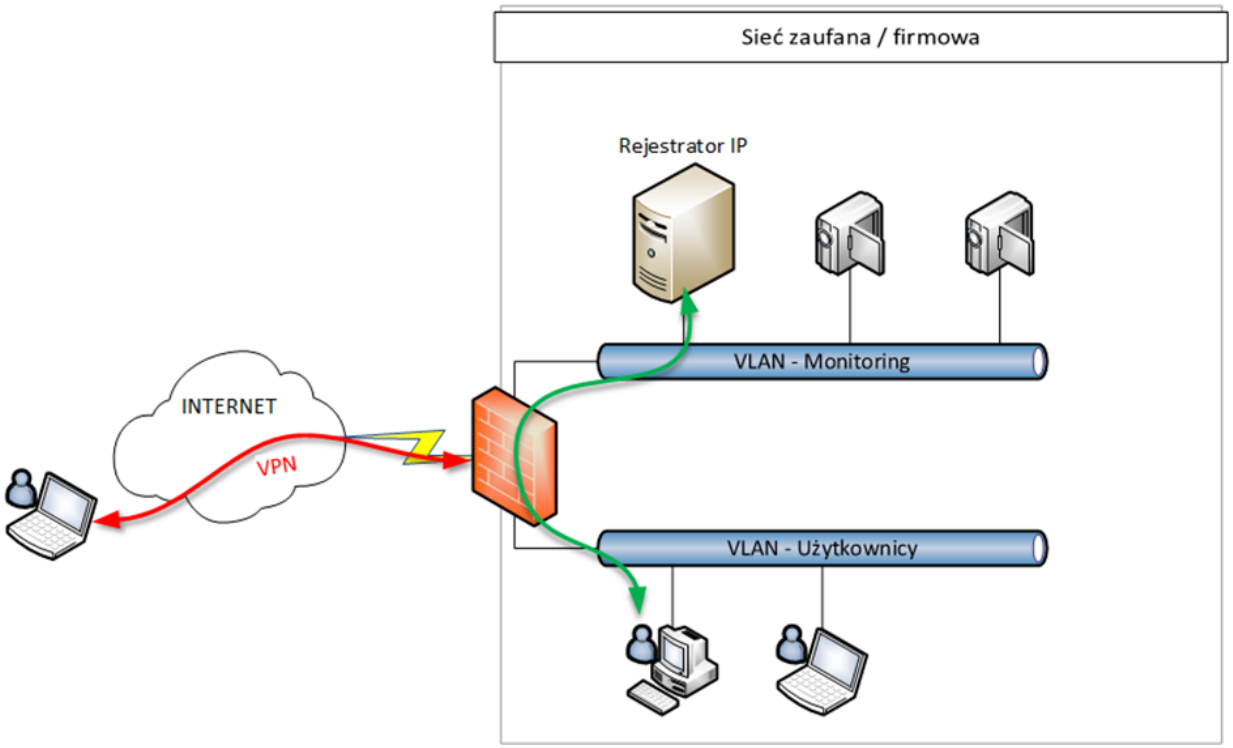
W przypadku wymaganego zdalnego dostępu

- sugerowane jest statyczne ustawienie adresu IP rejestratora
- w celu zapewnienia odpowiedniej ochrony przed nieautoryzowanym dostępem zalecane jest przygotowanie oddzielnej podsieci LAN dedykowanej tylko i wyłącznie dla systemu monitoringu
- zdalny dostęp do urządzeń znajdujących się w dedykowanej podsieci (takich jak rejestrator, kamery) powinien być zabezpieczony przez zaporę sieciową filtrującą ruch na poziomie warstwy L3 oraz L4; opis
  zdalny dostęp do rejestratora możliwy z dedykowanego urządzenia
  otwarte porty sieciowe
  - HTTP – port TCP 80
  - HTTPS – port TCP 443 (rekomendowany port komunikacji z rejestratorem)
  - Port serwera – TCP 6036
  - Port POS – TCP 9036
- ze względów bezpieczeństwa nierekomendowane jest ustawienia publicznego adresu IP na urządzeniu oraz udostępnianie go bezpośrednio z Internetu

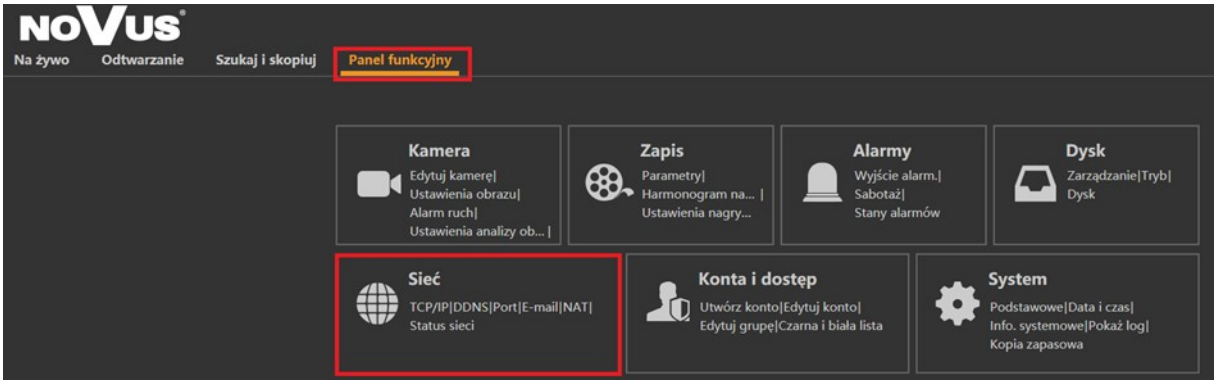
KONFIGURACJA SIECIOWA

pl

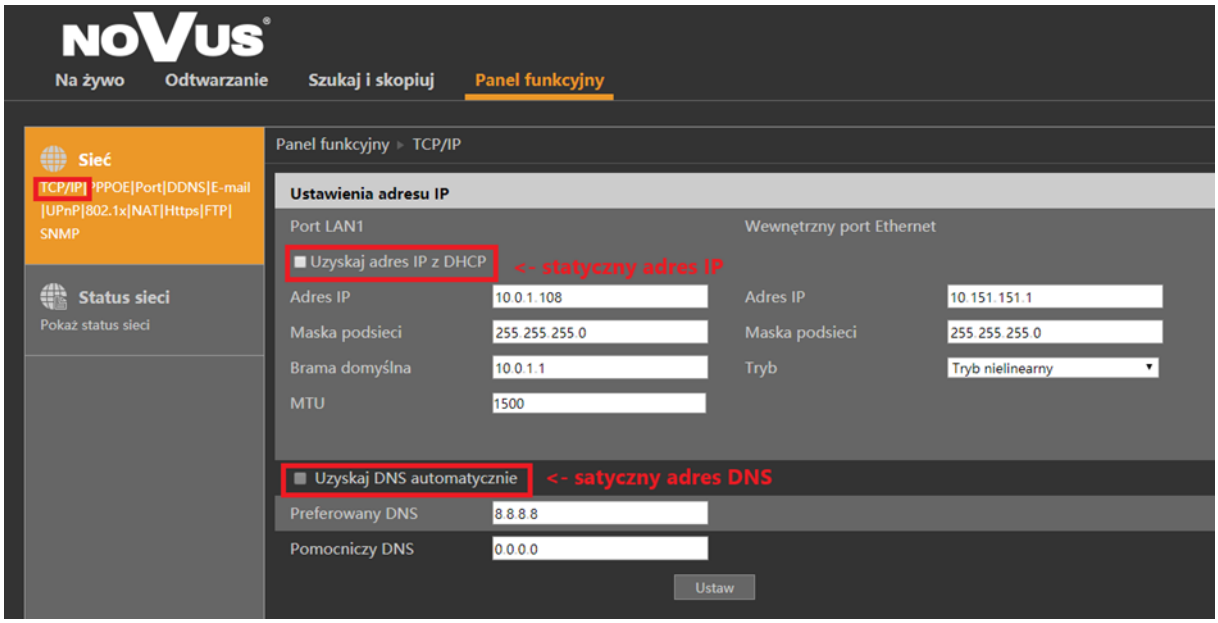
- w przypadku wymaganego dostępu do urządzenia z innej lokalizacji bądź bezpośrednio z Internetu rekomendowane jest wykorzystanie szyfrowanego tunelu VPN



Szczegółowa konfiguracja sieci
W *„Panelu funkcyjnym”* wymieramy opcję *„Sieć*

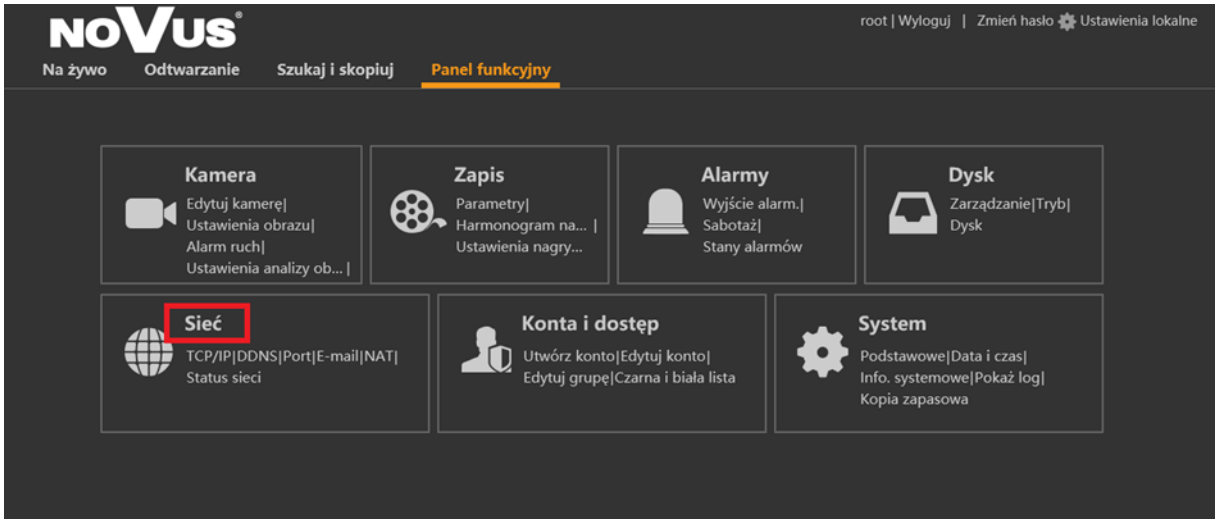


Ustawienia TCP/IP
Panel funkcyjny -> Sieć -> TCP/IP



2.2.2. Konfiguracja połączenia HTTPS

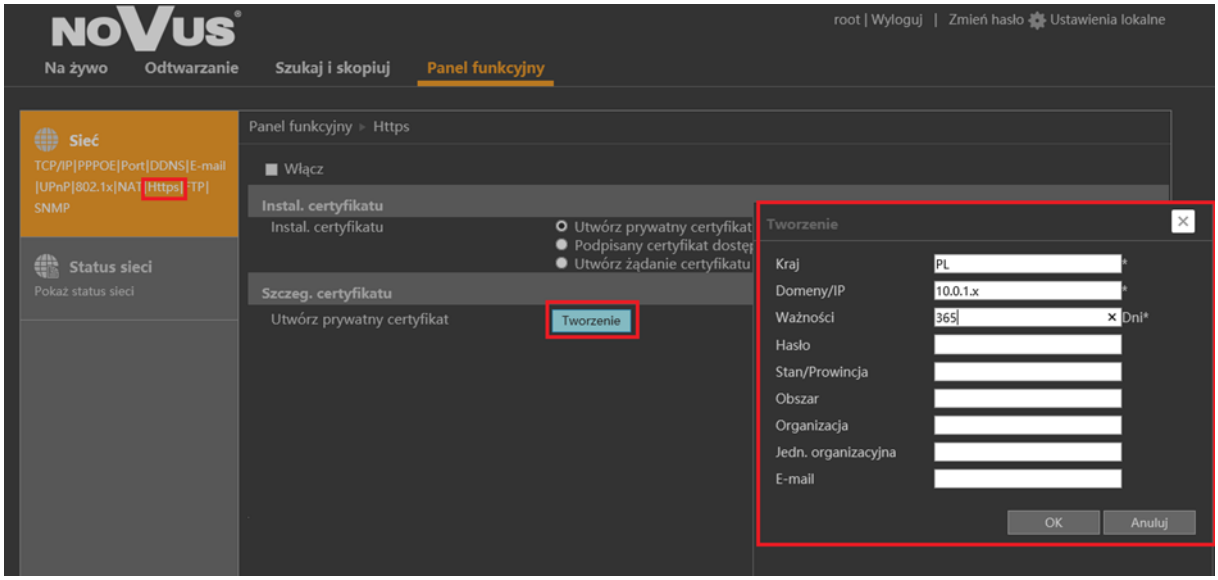
Aby uruchomić możliwość logowania się do panelu administracyjnego po HTTPS należy zalogować się z do rejestratora przez przeglądarkę i wybrać opcję *„Sieć”* -> *„HTTPS”*



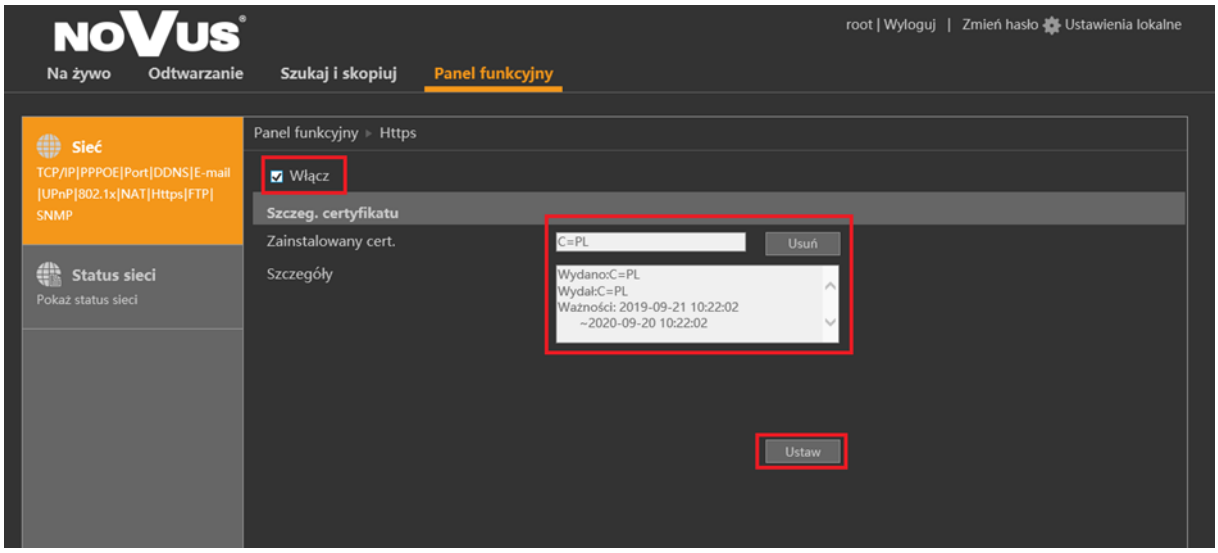
W następnym kroku tworzymy prywatny certyfikat, który będzie wykorzystywany do zabezpieczenia komunikacji HTTPS. Aby to zrobić wybieramy opcje *„Utwórz prywatny certyfikat”* i naciskając przycisk „Tworzenie”. Następnie należy wypełnić pola oznaczone gwiazdką np. tak jak podano poniżej i nacisnąć przycisk OK.

pl

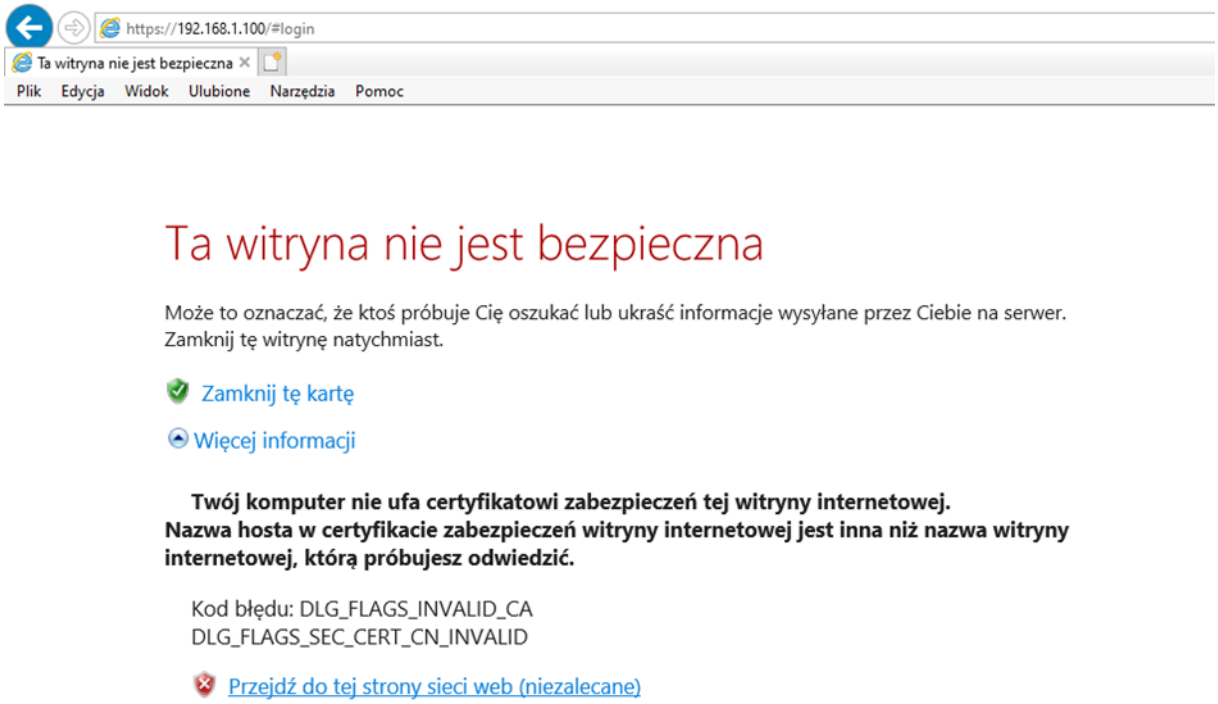
KONFIGURACJA HTTPS



Aby uruchomić finalnie opcje HTTPS należy zaznaczyć przycisk „*Włącz*” i kliknąć na przycisk *„Ustaw”*.



Po kliknięciu przycisku *„Ustaw”* przeglądarka spróbuje nawiązać połączenie używając protokołu HTTPS. W przeglądarce Internet Explorer należy rozwinąć przycisk *WIĘCEJ INFORMACJI* i kliknąć na *PRZEJDŹ DO TEJ STRONY SIECI WEB (NIEZALECANE).* Po kliknięciu powinna otworzyć się strona logowania do rejestratora.



pl

UWAGA: urządzenie umożliwia również wykorzystywanie własnych certyfikatów wydanych przez niezależne centra certyfikacji bądź własne PKI.

Opcje:

- Podpisany certyfikat dostępny. Zainstaluj teraz
- Utwórz żądanie certyfikatu

2.2.3. Ograniczenie dostępu do urządzeń

Zgodnie z powyższymi rekomendacjami, w celu zapewnienia odpowiedniej ochrony przed nieautoryzowanym dostępem zalecane jest przygotowanie oddzielnej podsieci LAN dedykowanej tylko i wyłącznie dla systemu monitoringu. Dodatkowo zdalny dostęp do urządzeń znajdujących się w dedykowanej podsieci (takich jak rejestrator, kamery) powinien być zabezpieczony przez zaporę sieciową filtrującą ruch na poziomie TCP/IP. Dodatkowym rozwiązaniem będzie ustawienie tzw. „ Czarnej i białej listy". Funkcjonalność ta jest dostępna bezpośrednio w urządzeniu. Umożliwia ona definiowanie urządzeń które będą mogły łączyć się zdalnie do urządzenia. Regułą może być ustawiona poprzez dodanie:

- Adresu IP zaufanego urządzenia (warstwa L3)
- Adresu MAC zaufanego urządzenia (warstwa L2).

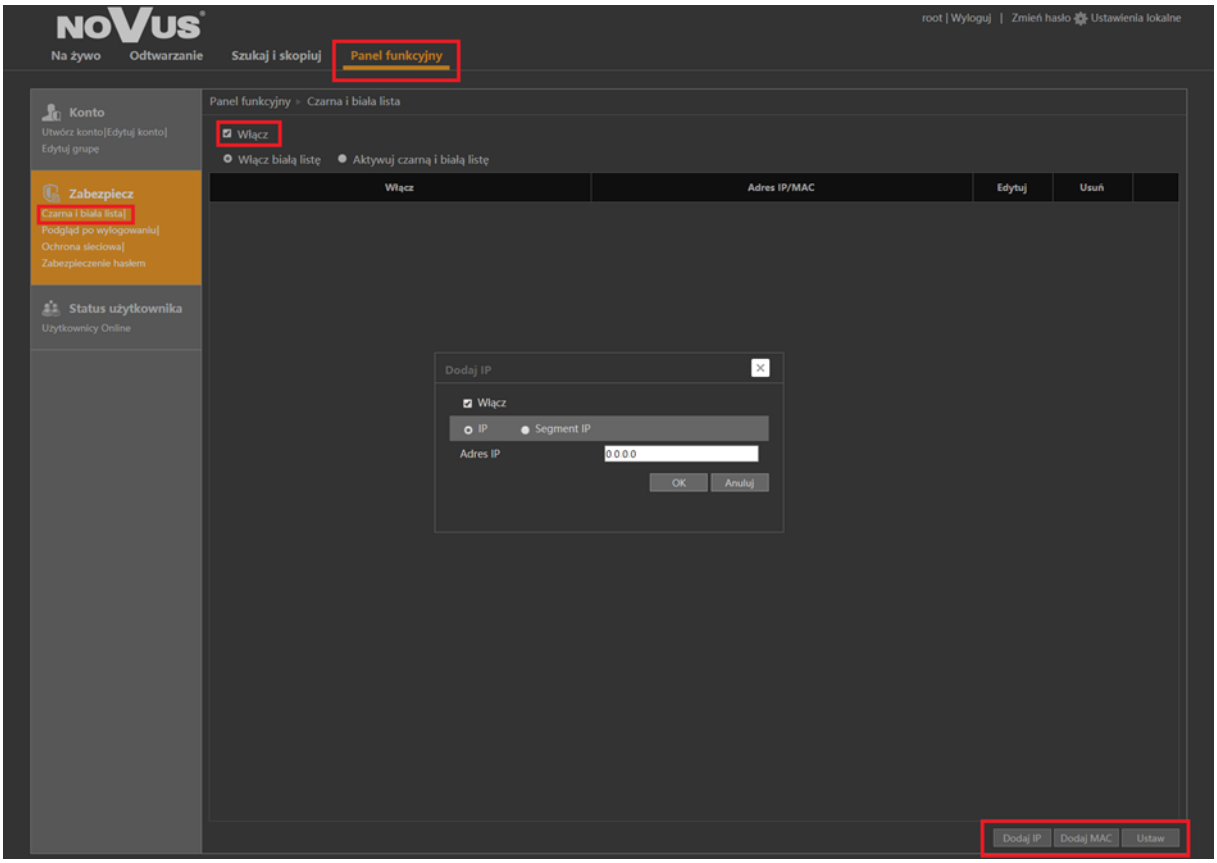
W celu skonfigurowania listy należy w *„Panelu funkcyjnym"* wybrać opcję „Konta i dostęp" *->„Zabezpiecz" -> „Czarna i biała lista".*

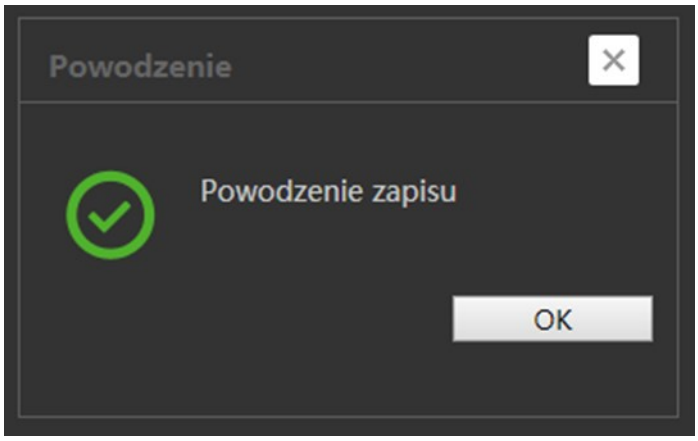
KONFIGURACJA HTTPS

Następnie wybrać opcje „*Włącz*” i w zależności o konfiguracji zdefiniować
Listę adresów IP bądź segmentów sieci z których będzie możliwość zdalnego nawiązywania połączenia do urządzenia. Opcja – *„Dodaj IP”*
Lisę adresów MAC z których będzie możliwość zdalnego nawiązywania połączenia do urządzenia. Opcja – *„Dodaj MAC”*
UWAGA: ze względu na charakterystykę protokołu TCP/IP preferowanym rozwiązaniem jest ustawienie filtracji na poziomie adresów IP

pl

Po zdefiniowaniu listy , całość zmian akceptujemy opcją „*Ustaw*”





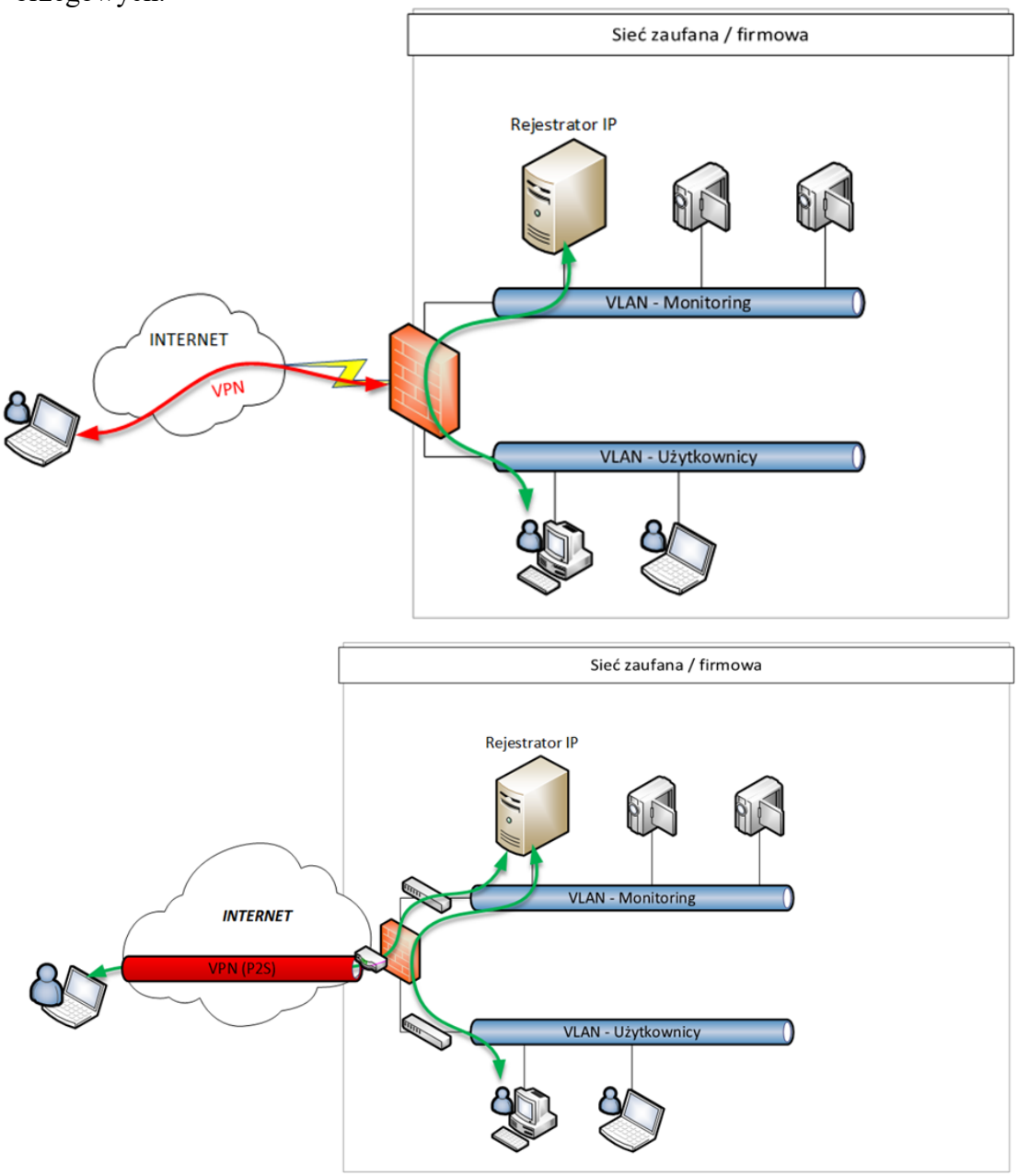
KONFIGURACJA VPN

2.2.4. Zdalny dostęp do urządzenia – VPN

Zgodnie z powyższymi rekomendacjami, preferowaną opcją zdalnego dostępu do urządzeń z / przez sieci niezaufane (np. Internet) jest zestawienie tunelu VPN który będzie chronił komunikację pomiędzy urządzeniami.

Architektura VPN:

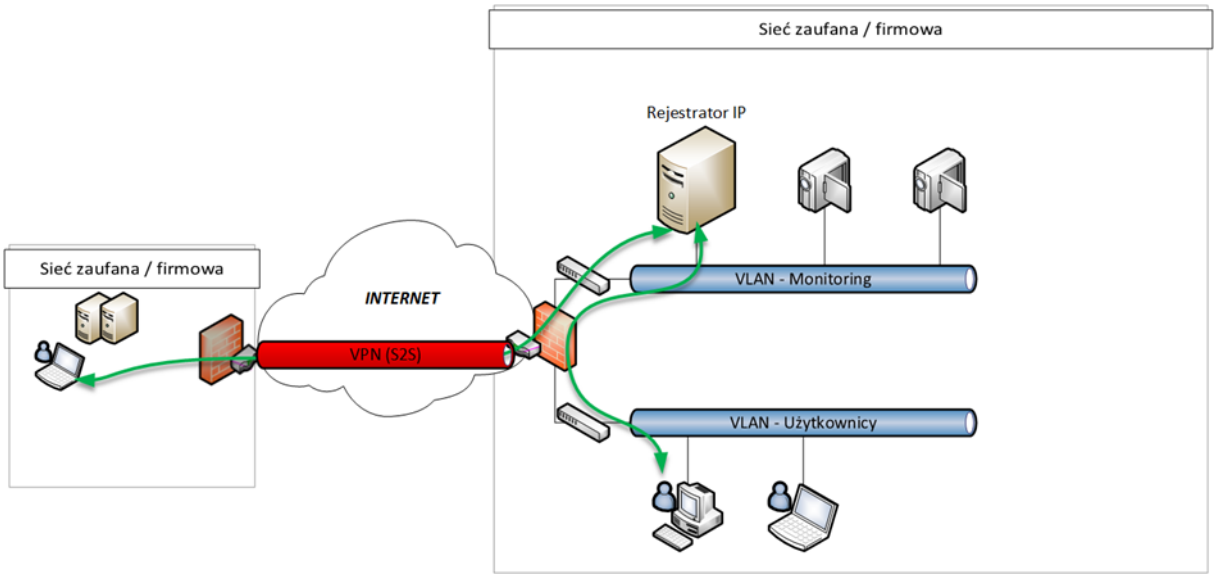
- *P2S VPN (Point to Site)* – w przypadku podłączenia się do urządzenia bezpośrednio ze stacji użytkownika znajdującego się w sieci niezaufanej. Stacja ta powinna mieć zainstalowaną aplikację umożliwiającą zestawienie sesji. Tunel najczęściej zestawiany jest na potrzeby jednorazowego zalogowania się do systemu.
- *S2S VPN (Site to Site)* – w przypadku podłączenia się do urządzenia z sieci zaufanej (np. drugiej lokalizacji firmy). Tunel zestawiany na stałe pomiędzy lokalizacjami na urządzeniach brzegowych.



Point to Site VPN

pl

KONFIGURACJA VPN



Site to Site VPN

Rekomendowane algorytmy szyfrowania

Algorytmy akceptowalne	
Symmetric Key Algorithms	AES-128, AES-192, AES-256
Cipher modes	GCM, CBC with integrity check (SHA),
Hashing Algorithms	SHA-256, SHA-512, SHA-3
Diffie-Hellman	Group 14 (2048) or higher
RSA	Factoring modulus ≥ 2048
Elliptic Curves (f)	f ≥ 256
Key Exchange	IKEv2
Transport layer protocols	TLS1.2

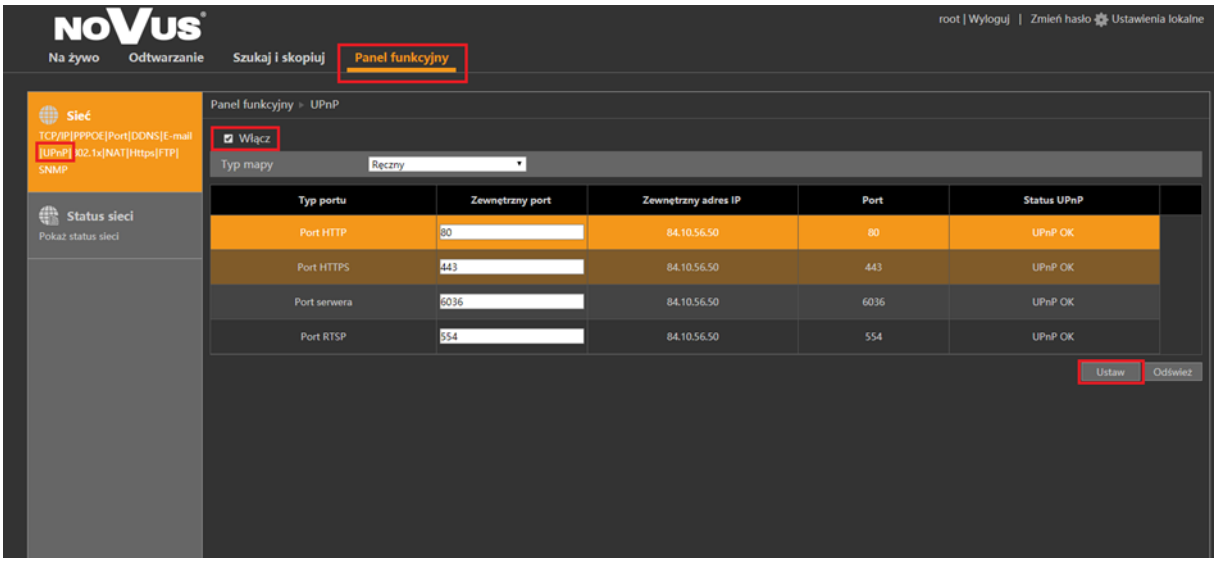
Urządzenie umożliwia również skorzystania z protokołu UPnP (Universal Plug-and-Play) w celu podłączenia się zdalnie do części usług sieciowych. Aby móc skorzystać z tej opcji należy:
uaktywnić opcję bezpośrednio na urządzeniu (patrz instrukcja poniżej)
w przypadku udostępniania usług do Internetu, uruchomić opcję UPnP na routerze brzegowym

UWAGA: ze względu na bezpieczeństwo nie rekomendowane jest korzystanie z protokołu UPnP w zdalnym dostępie do urządzeń (ze szczególnym uwzględnieniem dostępu z sieci niezaufanych takich jak Internet). Alternatywną opcją jest zestawienie tunelu VPN bądź ostatecznie udostępnienia usług sieciowych na zasadzie „Port Forwarding'u" z restrykcyjnymi regułami zapór sieciowych.

KONFIGURACJA UPNP

Uruchomienie opcji UPnP

W celu skonfigurowania UPnP należy w „Panelu funkcyjnym” wybrać opcję „Sieć” -> „UPnP”-> „Włącz”. Rozwiązanie umożliwia zmianę domyślnych portów TCP/IP po których będzie udostępniana dana usługa („Typ mapy – Ręczny”). Po ustawieniu wszystkich parametrów należy wcisnąć przycisk „Ustaw”



pl

2019-10-10 MB MK

AAT Holding S.A. , 431 Pulawska St., 02-801 Warsaw, Poland
tel.: +4822 546 07 00, fax: +4822 546 07 59
www.novuscctv.com