Bezpieczny dostęp do danych w sieci przemysłowej – konfiguracja.

Spis treści

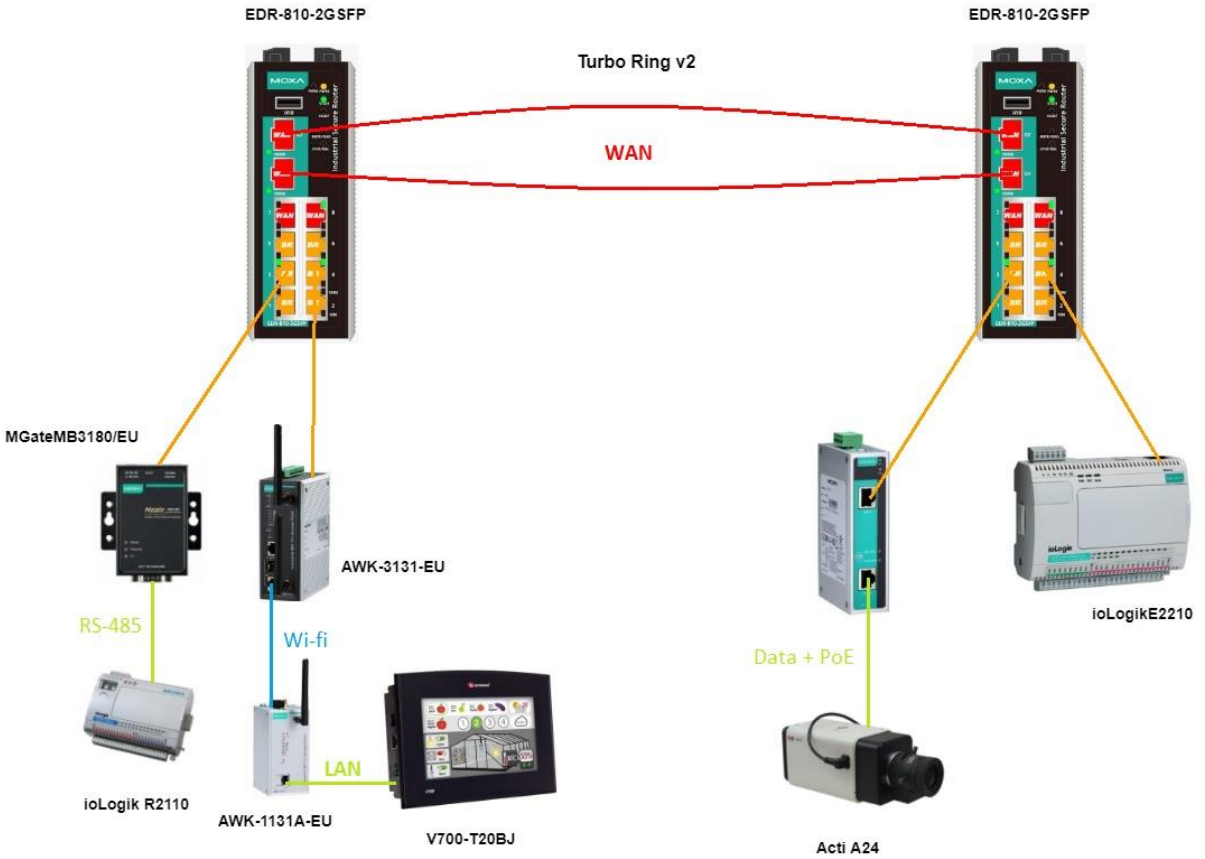
1. Wstęp

Opis konfiguracyjny jest integralną częścią wpisu opublikowanego na blogu Moxa. Konfiguracje konkretnych urządzeń były już omawiane na naszym blogu. Aby w łatwy i szybki sposób móc znaleźć więcej informacji umieszczone zostały odnośniki do konkretnych wpisów z konfiguracją.

Powyższa tabelka natomiast zawiera szczegółową listę wykorzystanego sprzętu, wraz z adresacją urządzeń.

Lp	Symbol	Opis	Adresacja IP/Maska
1	**EDR-810-2GSFP**	router, firewall, switch, 8xEth, 2xSFP	WAN: 192.168.128.254/24 BRG-LAN: 192.168.127.254/24
2	**EDR-810-2GSFP**	router, firewall, switch, 8xEth, 2xSFP	WAN: 192.168.128.253/24 BRG-LAN: 192.168.127.254/24
3	**ioLogik E2210**	Moduł 12DI/8DO	192.168.127.100/24
4	**AWK-3131-EU**	konwerter Ethernet-Wi-Fi 802.11 a/b/g/n	192.168.127.200/24
5	**AWK-1131A-EU**	konwerter Ethernet-Wi-Fi 802.11 a/b/g/n	192.168.127.210/24
6	**V700-T20BJ**	Sterownik z panelem dot. Kolor. 7"	192.168.127.220/24
7	**INJ-24A**	Injector PoE	-
8	**Acti A24**	Kamera IP	192.168.127.30/24
9	**MGate MB3180/EU**	1x RS-232/422/485 Gateway	192.168.127.15/24
10	**ioLogik R2110**	Moduł 12DI/8DO	RS-485
11	**SFP-1GLXLC-T (4 sztuki)**	moduł SFP: 1x 1000LX LC 10km	-
12	**SDR-120-12**	zasilacz na szynę DIN 120W 12V 10A	-
13	**GS18E48-P1J**	zasilacz wtyczkowy EU 18W 48V 0.375A	-

Poniższy opis w znacznym stopniu dotyczy możliwości konfiguracji firewalla na routerach EDR-810. Na potrzeby tego wpisu został zbudowany zestaw demo, którego topologia zaprezentowana została na poniższym rysunku.



Model demo składa się z dwóch routerów EDR-810-2GSFP. Urządzenia te zostały zaprojektowane z myślą o sieciach dostępowych. Jedną z ważniejszych ich funkcji jest umożliwienie bezpiecznego zdalnego dostępu do urządzeń w sieci lokalnej. Głównymi funkcjonalnościami routerów EDR-810 są: możliwość konfigurowania zapory ogniowej (Firewall), filtrowanie ruchu między konkretnymi portami, a także inspekcja pakietów Modbus.

Dwa routery są ze sobą połączone w topologii pierścienia z zaimplementowany również został protokół Turbo Ring v2, który umożliwia redundancję połączeń, zwiększając przy tym niezawodność sieci. Zamiast skrętki, do połączenia routerów wykorzystano odporny na zakłócenia światłowód jednomodowy, a sam router wyposażony jest we wkładki gigabitowe SFP-1GLXLC-T (złącza LC, transmisja do 10 km). Wykorzystanie NAT umożliwia zastosowanie takiej samej adresacji sieci LAN na obu routerach (szerzej ten problem został opisany na naszym blogu – Adresacja urządzeń w sieci przemysłowej z wykorzystaniem NAT).

W sieci LAN mogą znajdować się różnego rodzaju urządzenia. Topologia przedstawiona wcześniej zakłada, iż dwa routery EDR-810 służą do odseparowania dwóch segmentów sieci. W pierwszym segmencie sieci znajduje się linia produkcyjna, ale urządzenia, które są w niej zastosowane umożliwiają komunikację tylko z wykorzystaniem RS-485. Urządzenia starszego typu można podłączyć do sieci Ethernet z wykorzystaniem bramek. W tym przypadku została wykorzystana bramka Modbus MGate MB3180. Czasami konieczne jest umożliwienie komunikacji z urządzeniami znajdującymi się w trudno dostępnych miejscach, albo z urządzeniami, które znajdują się w ciągłym ruchu. Problem ten można rozwiązać wykorzystując urządzenia umożliwiające transmisję bezprzewodową, np. AWK-3131 lub AWK-1131A, które mogą pracować w trybach access point i client.

Drugi segment sieci zawiera urządzenia pracujące w linii produkcyjnej i konieczna jest ich integracja z systemami SCADA. Moduły iologik E2210 można podłączyć do sieci Ethernet. Obecnie, prawie każdy zakład produkcyjny wyposażony jest w kamery monitoringu wizyjnego. Minimalizując koszty, kamery można zasilać z wykorzystaniem PoE (Power over Ethernet). PoE umożliwia jednoczesną transmisję

danych i zasilania wykorzystując tylko jeden przewód. Do podłączenia większej liczby kamer można wykorzystać dedykowane switche z portami PoE. Do podłączenia jednej kamery (tak jak w tym przypadku) korzystniejszym rozwiązaniem jest zastosowanie injectora PoE – INJ-24A, który może dostarczyć do 60W mocy przy własnym napięciu zasilania 24/48VDC.

Powyższe przykłady, to niewielki procent różnych problemów, które mogą pojawić się podczas tworzenia infrastruktury sieciowej w przemyśle. Głównym celem tego wpisu jest pokazanie możliwości integracji ze sobą urządzeń spełniających różne funkcjonalności. Wachlarz możliwości jest o wiele większy.

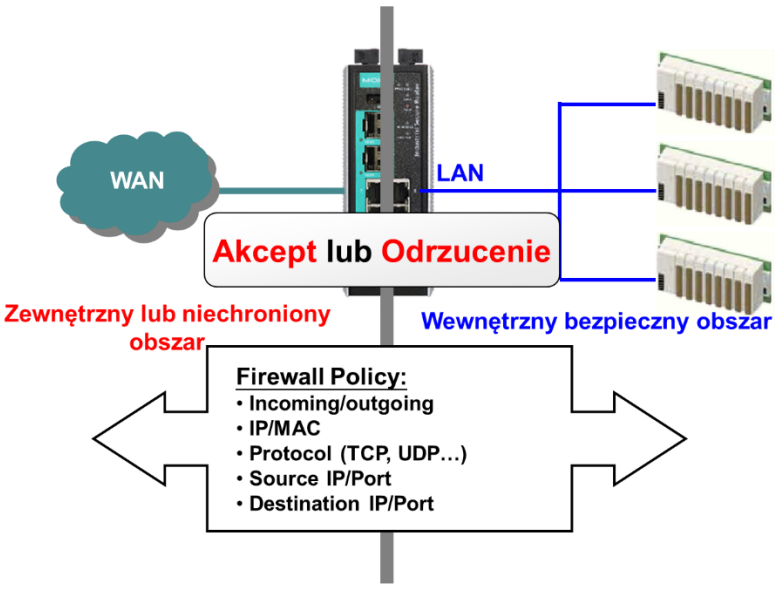
2. Przeląd funkcjonalności firewall na EDR-810

Routery przemysłowe Moxa EDR-810 posiadają wiele funkcjonalności, które umożliwiają poprawę bezpieczeństwa. W tym wpisie będę skupiał się głównie na jednej z nich – firewall, ale w ramach porządku wymienię pozostałe mechanizmy bezpieczeństwa, a są to:

- Segmentacja sieci VLAN
- SNMP wersja 3
- Autentykacja logować do urządzeń poprzez RADIUS/TACACS+
- SSH
- Wyłączenie nieużywanych portów
- Definiowanie adresów mających dostęp do konfiguracji
- Kontrola otwartych sesji
- Zablokowanie dostępu do konfiguracji w przypadku niepowodzeń w logowaniu
- Szyfrowanie plików konfiguracji
- Ograniczenie ruchu – traffic rate limiting

Firewall

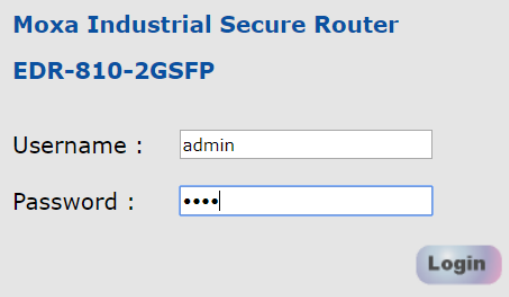
Mechanizm firewall jest używany głownie, aby zapewnić bezpieczny przepływ danych w sieci Ethernet. Urządzenia z obsługą firewall implementowane są najczęściej w krytycznych punktach, pomiędzy zewnętrzną (niezabezpieczoną) siecią, a wewnętrzną (w domyśle zabezpieczoną siecią). Schematycznie zostało to przedstawione na poniższym rysunku. Ponadto firewall na routerze EDR-810 może filtrować protokoły przemysłowe i zapewniać alarmowanie w czasie rzeczywistym.



Przejdźmy zatem opisu sposobów konfiguracji fiewalli na routerze EDR-810.

Najwygodniej konfigurację można przeprowadzić z wykorzystaniem przeglądarki internetowej.

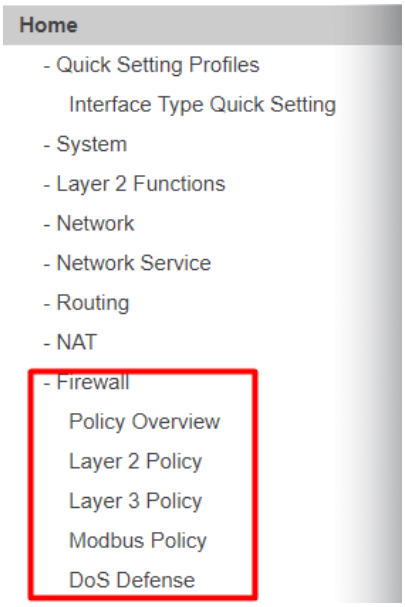
Domyślny adres IP – 192.168.127.254
Username: admin
Password: moxa (lub brak hasła – w zależności od wersji oprogramowania zainstalowanego na routerze). Ze względów bezpieczeństwa zaleca się zmianę domyślnego hasła.



Po wpisaniu domyślnego adresu IP w przeglądarce pojawi się następujące okno.

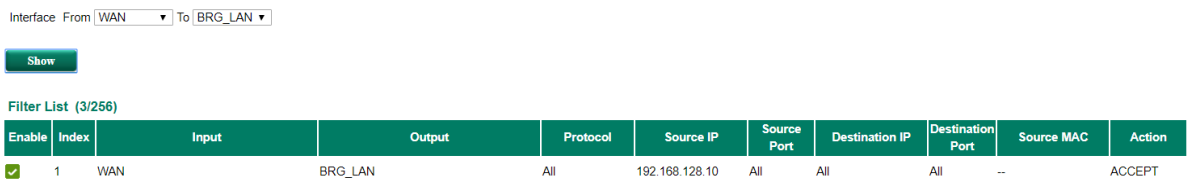
Po lewej stronie znajduje się spis kategorii. Najbardziej interesuje nas oczywiście kategoria Firewall. Zakładka składa się z pól

- Policy Overview
- Layer 2 Policy
- Layer 3 Policy
- Modbus Policy
- DoS Defense



Policy Overview

Zakładka umożliwia podgląd ustawionych reguł firewall. Można filtrować utworzone reguły po kierunku przepływu danych. Np. można wyświetlić reguły z WAN do LAN itp.

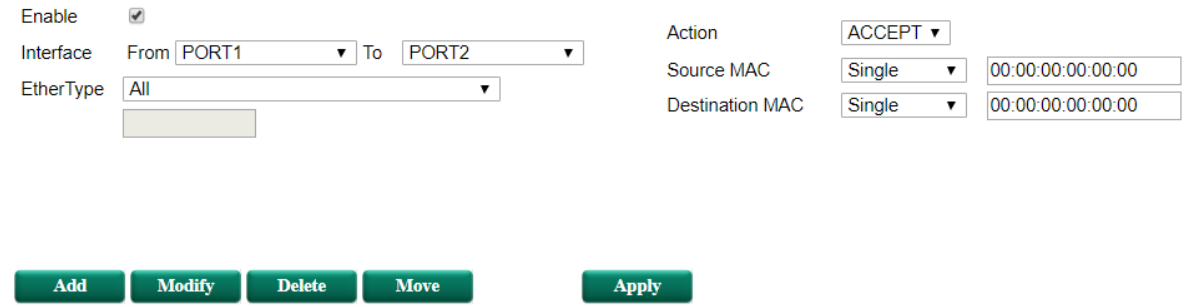


Layer 2 policy

EDR-810 umożliwia zaawansowane możliwości kontroli przepływu na poziomie warstwy drugiej, która może zależeć od konkretnych parametrów. Layer 2 policy umożliwia filtrowanie pakietów dla portów skonfigurowanych w trybie Bridge. Layer 2 Policy ma wyższy priorytet niż L3 Policy.

Istnieje możliwość wybrania konkretnych portów, z których ruch będzie przepuszczany lub odrzucany, jeżeli będzie spełniał założenia reguły firewall. A także bardziej szczegółowe ustawienia

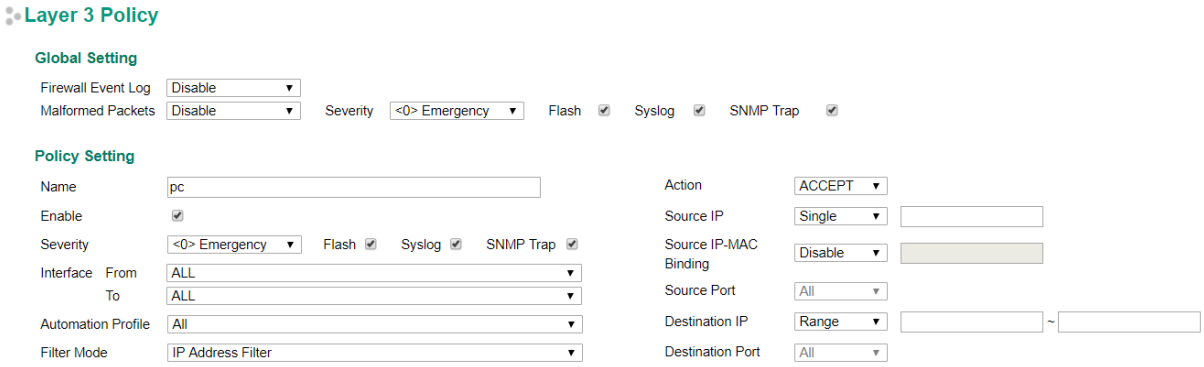
jak adres MAC urządzenia, które nadaje ramkę, adres MAC urządzenia, które odbiera ramkę danych, a także tym protokołów warstwy drugiej zgodnych z modelem



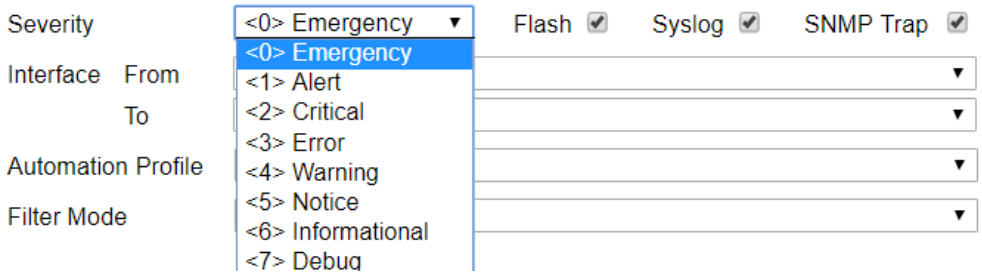
Layer 3 Policy

EDR-810 umożliwia także utworzenie reguł kontrolujących przepływ danych na poziomie warstwy trzeciej.

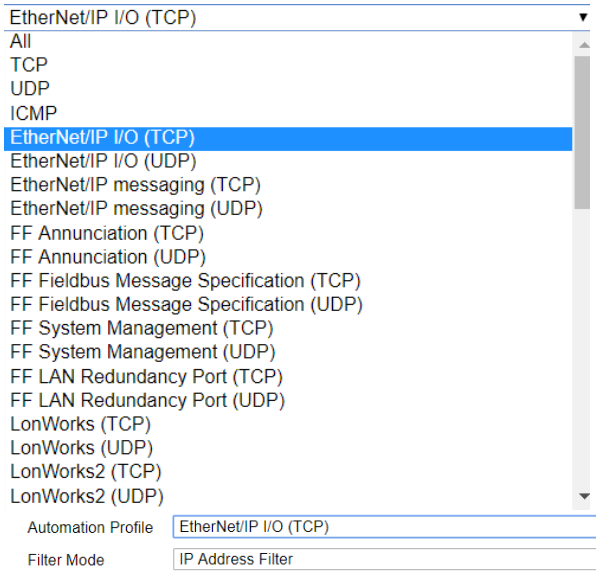
EDR-810 wspiera wysyłanie powiadomień w czasie rzeczywistym (**Firewall Event Log**), które mogą być automatycznie zapisywane na nośniku zewnętrznym wysyłane do serwera Syslog lub mogą być wysyłane powiadomienia SNMP Trap.



Opcja **Severity** umożliwia zdefiniowane w jaki sposób konkretna reguła firewalla, która zostanie spełniona, będzie wyświetlana oraz raportowana do serwera syslog , tzn. jako zagrożenie, błąd, powiadomienie itp. oraz w jaki sposób to raportowanie będzie się odbywać – tzn. pamięć flash, syslog, SNMP trap.



Podobnie, jak w przypadku Layer 2 Policy można zdefiniować ruch pomiędzy konkretnymi interfejsami. Można również odfiltrować konkretny zakres IP.



Wybór konkretnych protokołów przemysłowych i predefiniowanych numerów portów również jest możliwy. Po wybraniu konkretnego protokołu zostanie przypisany zdefiniowany programowo numer portu docelowego.

Są dwie główne polityki implementacji reguł firewall – polityka Whitelisting i polityka Blacklisting.

Polityka **Whitelisting** polega na akceptacji tylko pożądanych pakietów i na odrzucaniu wszystkich innych. Poniżej przedstawiony jest przykład takiej polityki.

Filter List (3/256)

Enable	Index	Input	Output	Protocol	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Action	Event Log / Severity
☑	1	WAN	BRG_LAN	All	192.168.128.10	--	All	All	All	ACCEPT	Enable / <0> Emergency
☑	2	BRG_LAN	WAN	All	All	--	All	192.168.128.1 ~192.168.128.20	All	ACCEPT	Enable / <0> Emergency
☑	3	ALL	ALL	All	All	--	All	All	All	DROP	Enable / <0> Emergency

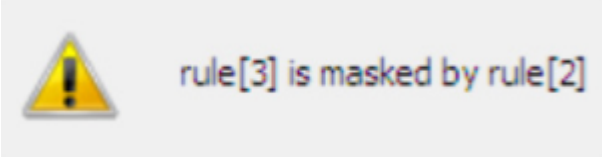
Polityka Blacklisting działa odwrotnie tzn. polega na odrzucaniu konkretnych pakietów i na zezwalaniu na przepływ wszystkich innych. Poniżej przedstawiono przykład takiej polityki:

Filter List (3/256)

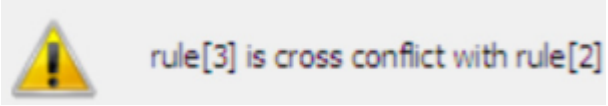
Enable	Index	Input	Output	Protocol	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Action	Event Log / Severity
☑	1	WAN	BRG_LAN	EtherNet/IP I/O (TCP)	192.168.128.10	--	All	All	2222	DROP	Enable / <0> Emergency
☑	2	BRG_LAN	WAN	All	All	--	All	192.168.128.1 ~192.168.128.20	All	DROP	Enable / <0> Emergency
☑	3	ALL	ALL	All	All	--	All	All	All	ACCEPT	Enable / <0> Emergency

Ciekawym narzędziem jest funkcja **PolicyCheck,** która informuje użytkownika, czy nie występują błędy i konflikty w konfiguracji.

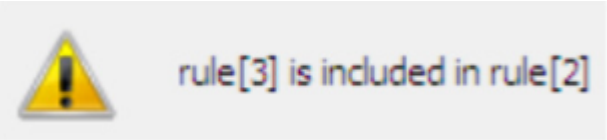
- Mask – wykrywanie konfliktu dla pojedynczego parametru (np. dwie reguły pokrywają ten sam adres)



- Cross Conflict – wykrywanie „poprzecznych" konfliktów w dwóch parametrach (np. IP i Port)

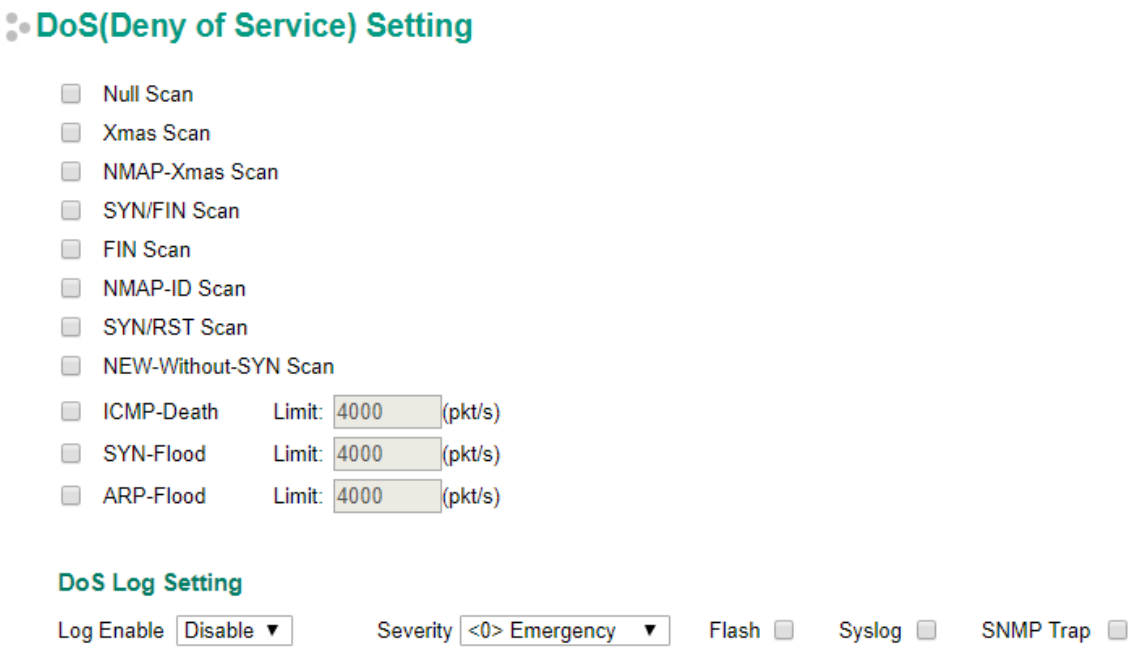


- Include – wykrywanie zdublowanych reguł (dodatkowe obciążenie routera)



DoS (Deny of Service)

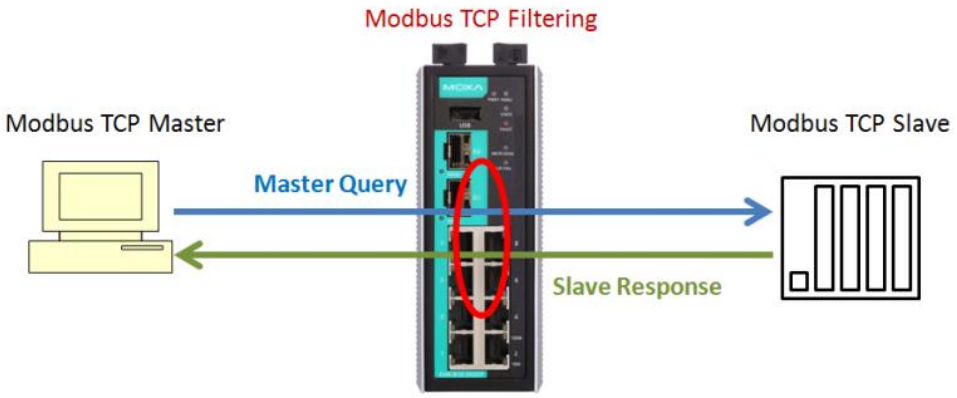
EDR-810 umożliwia zdefiniowanie 9 różnych DoS funkcji dla detekcji lub zdefiniowania nietypowych pakietów danych. Router wykryje nietypową ramkę danych, odrzuci ją i może wysłać odpowiednie powiadomienie.

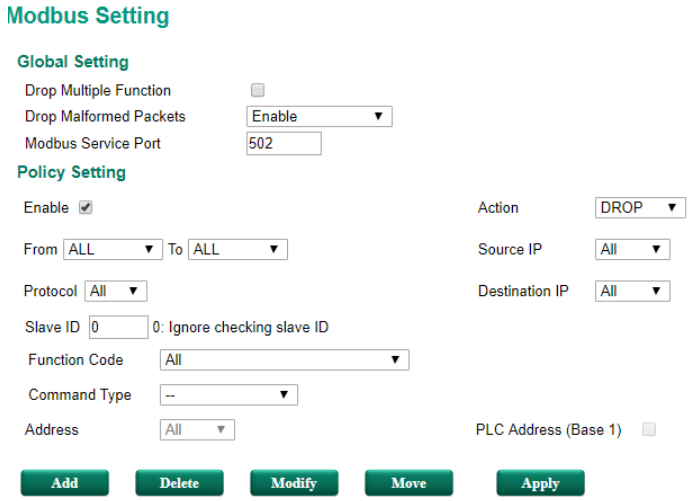


Modbus Deep Packet Inspection

EDR-810 posiada funkcję inspekcji pakietów Modbus – **Modbus TCP Filtering.**

O protokole Modbus można przeczytać na naszym blogu: Konwersja protokołu Modbus i konwertery firmy Moxa. Router EDR-810 umożliwia inspekcję pakietów Modbus TCP, która pozwala użytkownikowi kontrolować ramki Modbus według parametrów: Slave ID, Function Code, Command Type (zapytanie od mastera – Master Querty, odpowiedź slave'a – Slave Response, adress IP źródła i urządzenia docelowego.

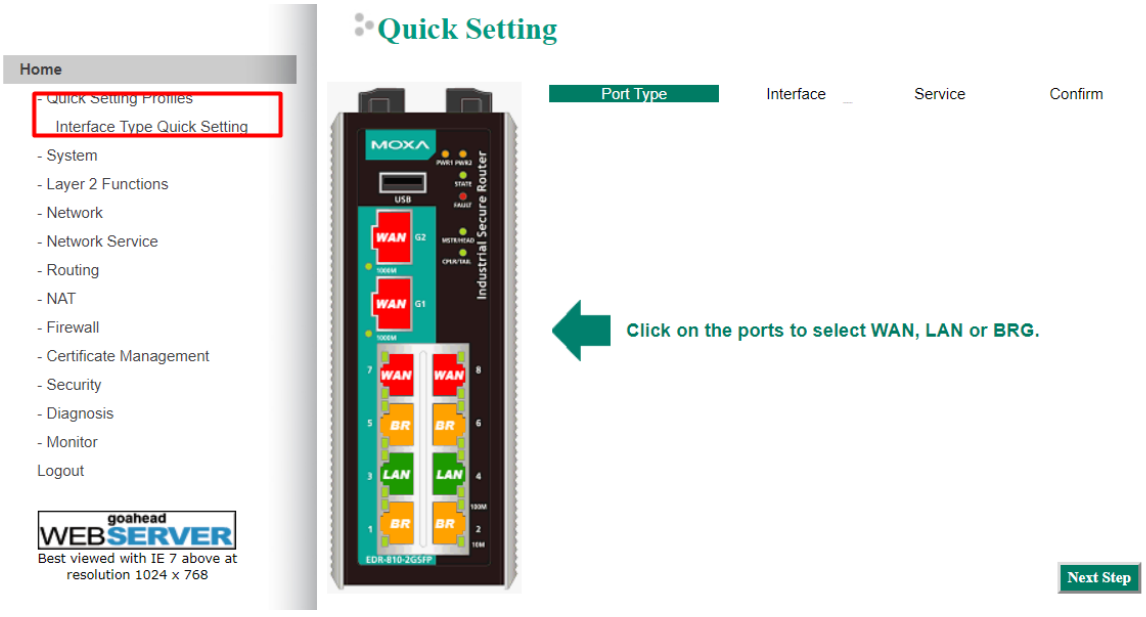




3. Konfiguracja EDR-810

Interfejsy

Router 1 (192.168.128.254)

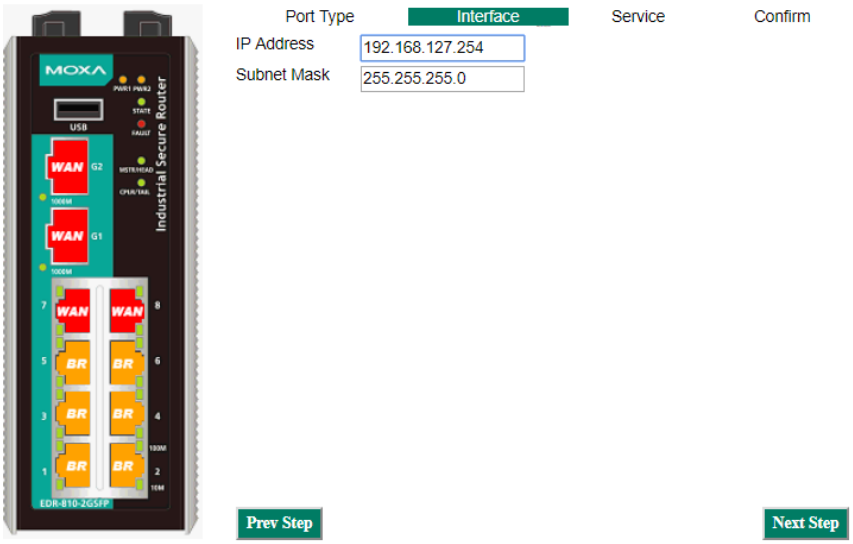


Po lewej stronie ekranu znajduje się spis kategorii. Szybka konfiguracja portów umożliwiona jest dzięki opcji **Quick Setting Profiles.**

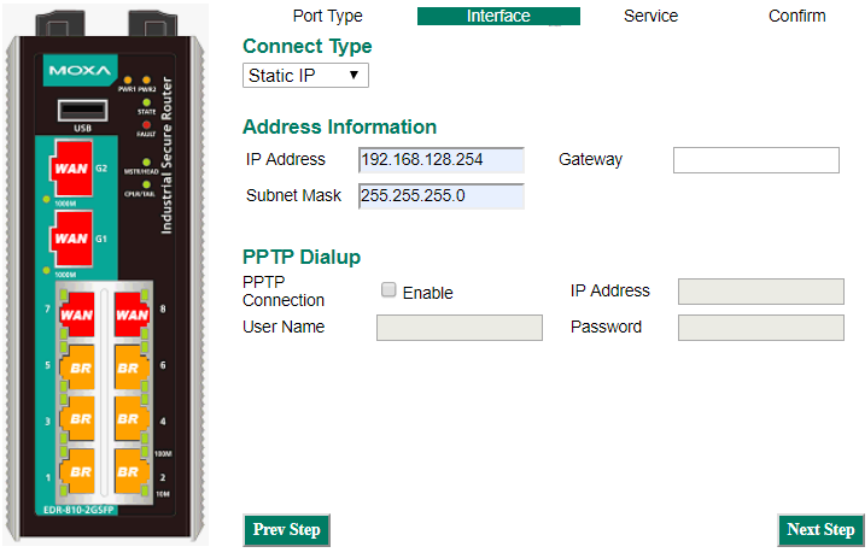
Klikając myszką na odpowiednie porty można zmienić ich status: tzn. WAN, LAN lub Bridge.

W następnym kroku określany jest adres interfejsu BRG-LAN

IP Address – 192.168.127.254, Subnet Mask – 255.255.255.0

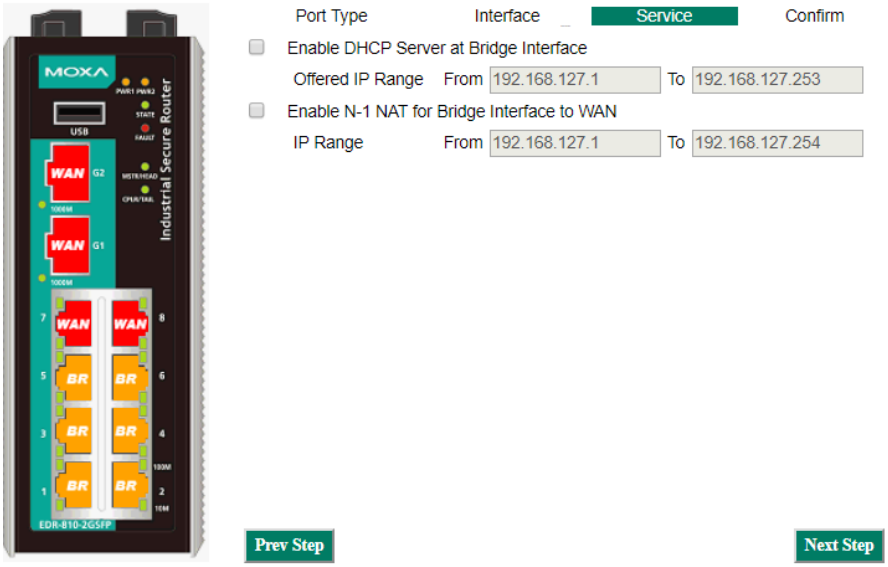


W następnym kroku określany jest adres portów w sieci WAN.

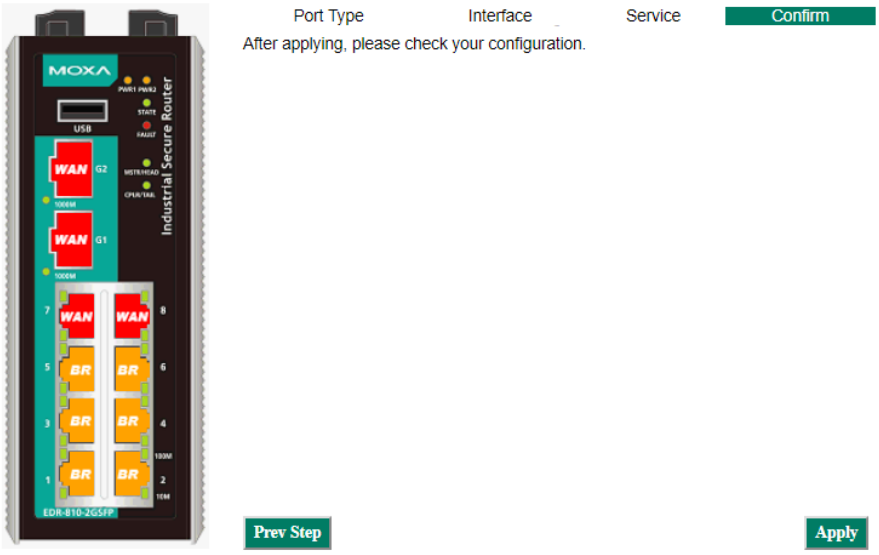


Static IP, IP address: 192.168.128.254, Subnet Mask 255.255.255.0

W następnym kroku odznaczamy ustawienia serwera DHCP i NAT. W tej konfiguracji DHCP nie jest nam potrzebny, a ustawienia NAT będą skonfigurowane w kolejnym punkcie.

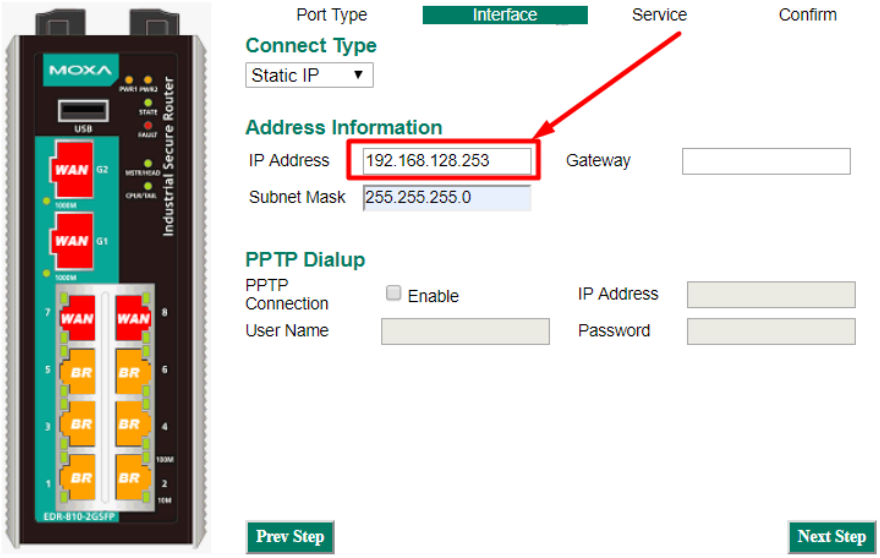


Wystarczy tylko potwierdzić ustawienia klikając przycisk „Apply”. Router uruchomi się w tym czasie ponownie wraz z nowymi ustawieniami.



Router 2 (192.168.128.253)

Ustawienia interfejsów na drugim routerze EDR-810 konfigurowane są w podobny sposób, ale adres portów w sieci WAN musi być inny (ale w tej samej podsieci). Np. IP address 192.168.128.253, Subnet mask 255.255.255.0



NAT

NAT- Network Address Translation, umożliwia translację prywatny adresów urządzeń, na inne adresy w sieci WAN. Jest to kolejny mechanizm bezpieczeństwa. Szczegółowy opis NAT, wraz z przykładową konfiguracją znajduje się już na naszym blogu - [Adresacja urządzeń w sieci przemysłowej z wykorzystaniem NAT](). W związku z tym umieszczone zostały tylko zrzuty koniecznych ustawień

Z sieci WAN do urządzeń będzie próbował się połączyć komputer o adresie w sieci WAN 192.168.128.10, który został zmieniony z wykorzystaniem NAT na adres w sieci lokalnej 192.168.127.10

Router 1

NAT List (5/128)

Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	Name
☑	1	BRG_LAN	--	192.168.128.10	--	192.168.127.10	--	--	PC
☑	2	WAN	--	192.168.127.15	--	192.168.128.15	--	--	MB3180
☑	3	WAN	--	192.168.127.200	--	192.168.128.200	--	--	awk3131
☑	4	WAN	--	192.168.127.210	--	192.168.128.210	--	--	awk1131a
☑	5	WAN	--	192.168.127.220	--	192.168.128.220	--	--	plc

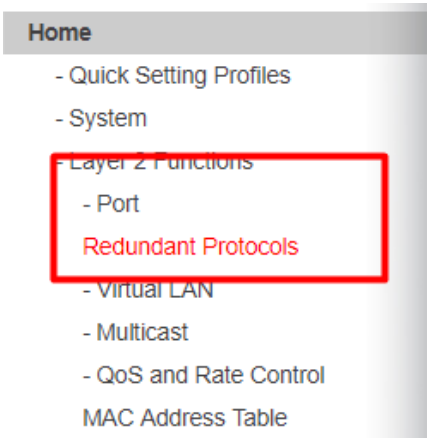
Router 2

NAT List (3/128)

Enable	Index	Outside Interface	Protocol	Local IP (Host IP)	Local Port	Global IP (Interface IP)	Global Port	VRRP Binding	Name
☑	1	WAN	--	192.168.127.100	--	192.168.128.100	--	--	iologikE2210
☑	2	WAN	--	192.168.127.30	--	192.168.128.30	--	--	ActiA24
☑	3	BRG_LAN	--	192.168.128.10	--	192.168.127.10	--	--	PC

Turbo Ring v2

Turbo Ring jest redundantnym protokołem, który z przypadku sieci 1G, gdy nastąpi awaria głównej ścieżki, zapewnia przełączenie na zapasowe połączenie w czasie krótszym niż 50 ms.



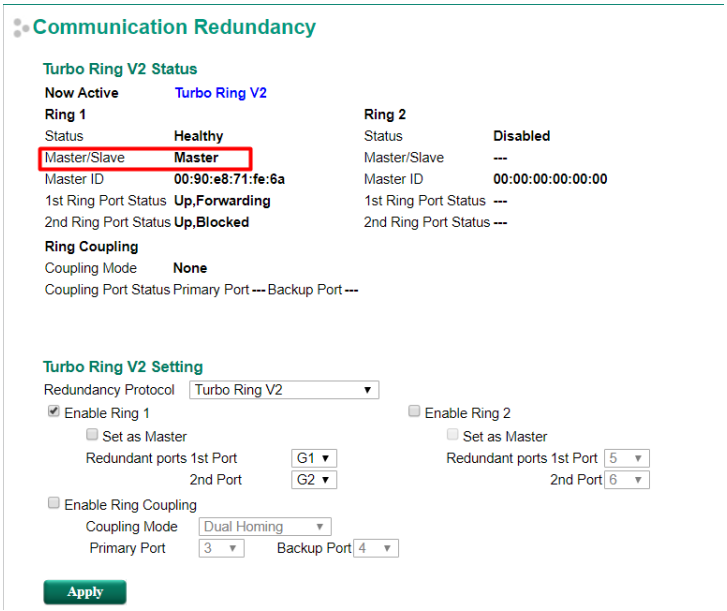
Ustawienia Turbo Ring można znaleźć w zakładce Layer 2 Protocols → Port→ Redundant Protocols.

Tak jak w przypadku NAT, konfiguracja Turbo Ring została opisana na naszym blogu - Konfiguracja protokołu redundantnego Turbo Ring na switchach Moxa.

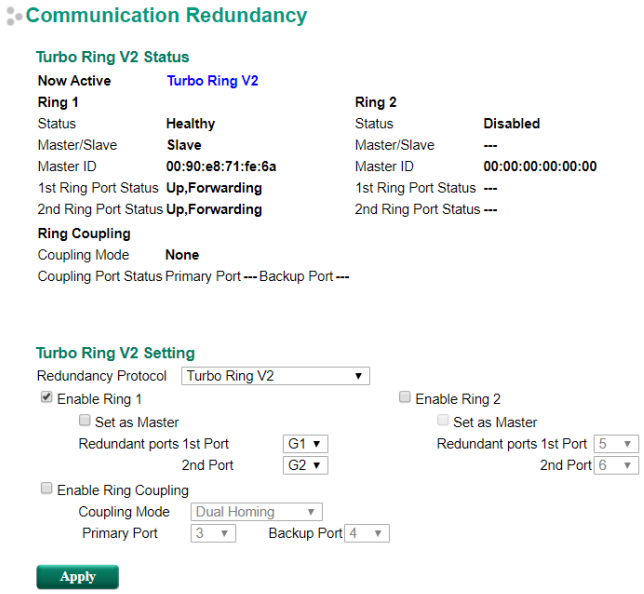
Turbo Ring na obu routerach skonfigurowany jest na sieci WAN z wykorzystaniem portów G1 i G2, do których włożone są gigabitowe wkładki jednomodowe **SFP-1GLXLC-T.**

Po poprawnym skonfigurowaniu powinny pojawić się poniższe ustawiania. Router 1 został automatycznie ustawiony jako Master, co oczywiście można zmienić ręcznie.

Router 1



Router 2



Firewall

Jakie rodzaj ruchu umożliwia firewall wg tych ustawień? Dostęp do każdego urządzenia z osobna możliwy jest tylko z komputera o adresie 192.168.128.10. Urządzenia natomiast mogą wysyłać dane do sieci WAN, ale tylko do urządzeń o adresie IP z zakresu: 192.168.128.1-192.168.128.20. Komunikacja bezpośrednia między urządzeniami jest ograniczona poprzez reguły Layer 2 Policy. Użytkownik ma możliwość odczytu statusu cewek na iologik R2110. Natomiast na iologik E2210 może zarówno odczytywać jak i zmieniać status cewek. Te ustawienia zostały ograniczone przez Modbus Policy.

Opis Firewall znajduje się w rozdziale drugim, poniżej zrzuty ustawień.

Router 1

Layer 2 Policy

Filter List (3/256)

Enable	Index	Input	Output	Protocol	Source MAC	Destination MAC	Action
☑	1	PORT3	PORT4	All	All	All	DROP
☑	2	PORT4	PORT3	All	All	All	DROP
☑	3	All BRG Members	All BRG Members	All	All	All	ACCEPT

Layer 3 Policy

Filter List (3/256)

Enable	Index	Input	Output	Protocol	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Action	Event Log / Severity
☑	1	WAN	BRG_LAN	All	192.168.128.10	--	All	All	All	ACCEPT	Enable / <0> Emergency
☑	2	BRG_LAN	WAN	All	All	--	All	192.168.128.1 ~192.168.128.20	All	ACCEPT	Enable / <0> Emergency
☑	3	ALL	ALL	All	All	--	All	All	All	DROP	Enable / <0> Emergency

Modbus Policy

1. Master querty
2. Slave Response

Modbus List (3/64)

Index	Enable	Input	Output	Protocol	Source IP	Destination IP	Slave ID	Function Code	Address	Action
1	✓	WAN	BRG_LAN	All	--	--	0	1: Read Coils	--	ACCEPT
2	✓	BRG_LAN	WAN	All	--	--	0	1: Read Coils	--	ACCEPT
3	✓	ALL	ALL	All	--	--	0	All	--	DROP

Router 2

Layer 2 Policy

Filter List (3/256)

Enable	Index	Input	Output	Protocol	Source MAC	Destination MAC	Action
✓	1	PORT3	PORT4	All	All	All	DROP
✓	2	PORT4	PORT3	All	All	All	DROP
✓	3	All BRG Members	All BRG Members	All	All	All	ACCEPT

Layer 3 Policy

Enable	Index	Input	Output	Protocol	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Action	Event Log / Severity
✓	1	WAN	BRG_LAN	All	192.168.128.10	--	All	All	All	ACCEPT	Enable / <0> Emergency
✓	2	BRG_LAN	WAN	All	All	--	All	192.168.128.1 ~192.168.128.20	All	ACCEPT	Enable / <0> Emergency
✓	3	ALL	ALL	All	All	--	All	All	All	DROP	Enable / <0> Emergency

Modbus Policy

1. Master querty
2. Master querty
3. Slave Response

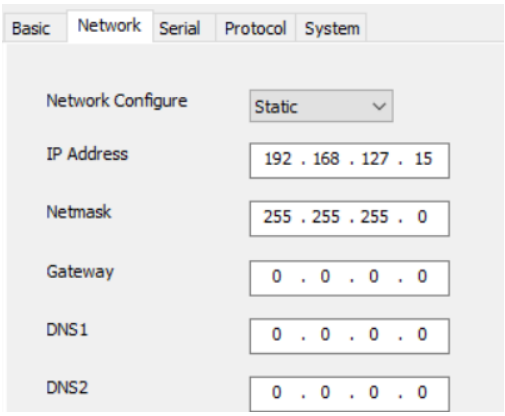
Modbus List (4/64)

Index	Enable	Input	Output	Protocol	Source IP	Destination IP	Slave ID	Function Code	Address	Action
1	✓	WAN	BRG_LAN	All	--	--	1	1: Read Coils	--	ACCEPT
2	✓	WAN	BRG_LAN	All	--	--	1	5: Write Single Coil	--	ACCEPT
3	✓	BRG_LAN	WAN	All	--	--	0	All	--	ACCEPT
4	✓	ALL	ALL	All	--	--	0	All	--	DROP

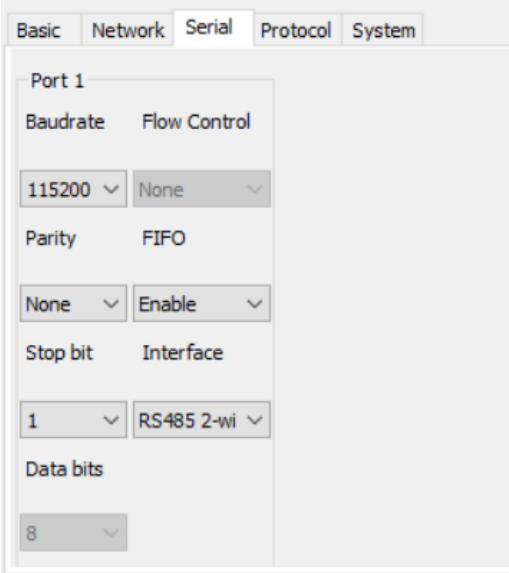
4. Konfiguracja MGate MB3180

Dedykowanym programem do wyszukiwania i konfiguracji konwerterów protokołów przemysłowych jest MGate Manager. Jest do darmowe oprogramowanie do pobrania z oficjalnej strony producenta urządzeń Moxa.

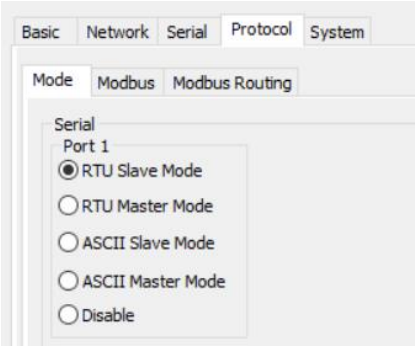
Po wyszukaniu urządzenia konieczna jest zmiana jego adresu IP na 192.168.127.15



Następnie należy zmienić ustawienia komunikacji szeregowej, m.in. prędkość transmisji, bit stopu itp. tak aby te same ustawienia komunikacji szeregowej ustawione były na iologik R2110. Konieczne jest wybranie interfejsu RS-485 2-wire.



Wystarczy dodatkowo wybrać tryb pracy jako RTU Slave.



Po zapisaniu ustawień, urządzenie jest już gotowe to konwersji protokołu RS-485 na sieć Ethernet.

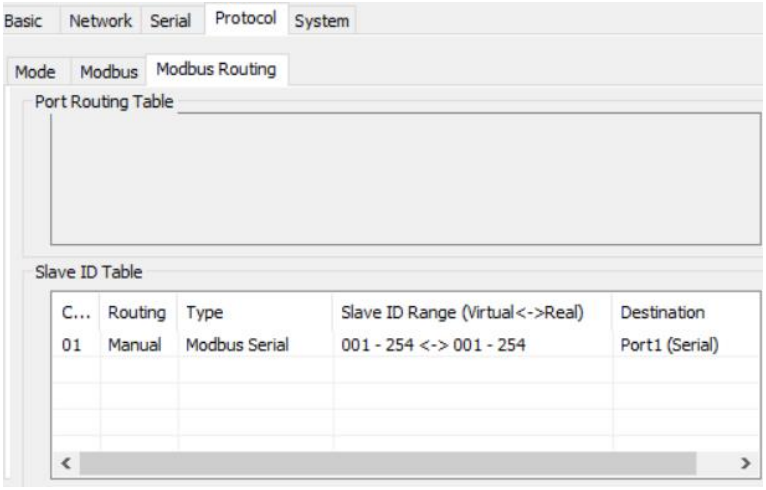
5. Konfiguracja iologik R2110

Ustawienie Baudrate dla RS-485 2-przewodowego

Konieczne jest przełączenie na pozycję domyślną „0”, która zapewni takie same ustawienia komunikacji szeregowej, jakie są ustawione na Iologik R2110

	Baudrate for RS-485 (parameters are N, 8, 1)	Dial setting and corresponding baudrate: 0:115200 1:57600 2:38400 3:19200 4:9600 5:4800 6:2400 7:1200

Można jeszcze zmienić ID slave’a przełącznikami na panelu czołowym iologika np. na wartość 10, ale tak aby wartość Slave ID mieściła się w zakresie Modbus Routingu skonfigurowanym na Mgate MB3180.



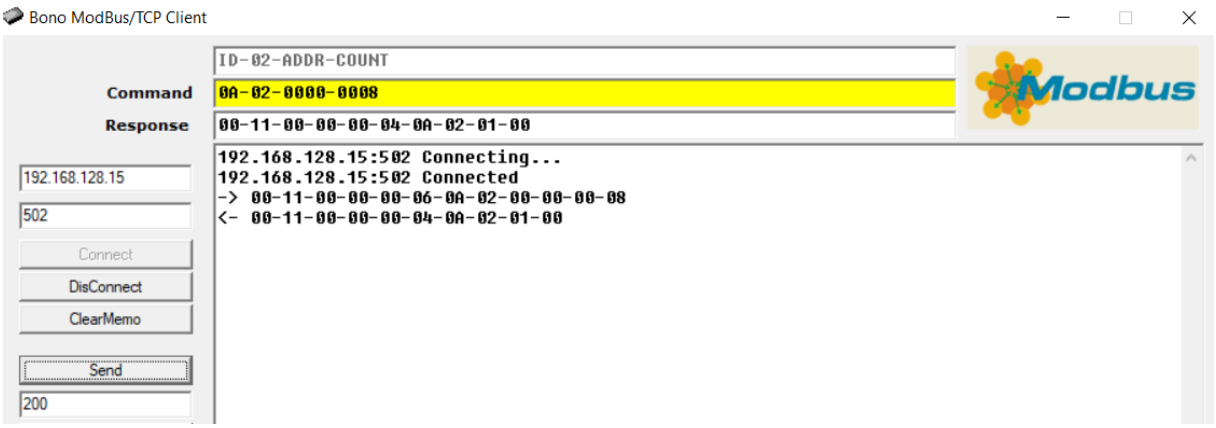
Minimalne ustawienia do zapewnienia komunikacji zostały spełnione.

Jeżeli wszystko zostało poprawnie skonfigurowane, można przejść do etapu testowania komunikacji.

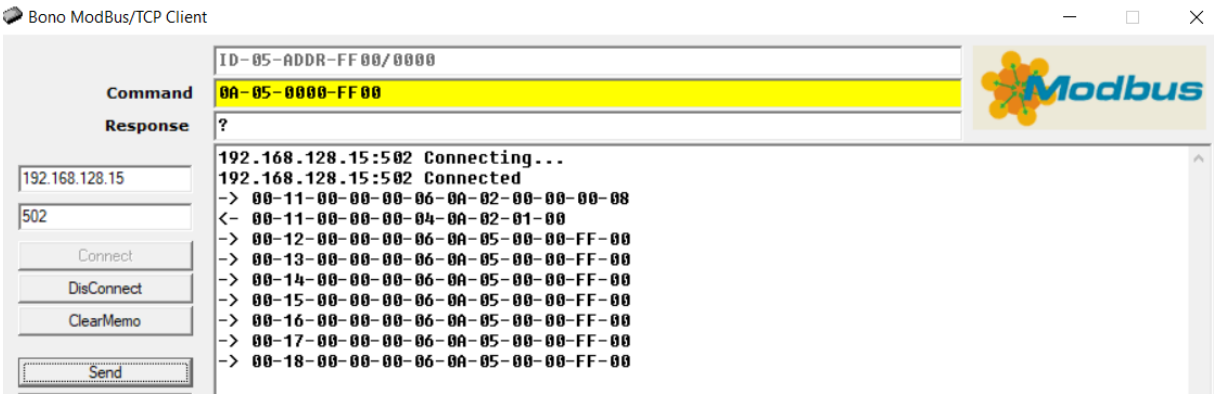
Został wykorzystany prosty program do wysyłania zapytań Modbus TCP.

Komunikacja z urządzeniem została osiągnięta poprzez połączenie się z bramką MGate MB3180, która z sieci WAN dostępna jest pod adresem 192.168.128.15.

Zgodnie z regułami Firewall, możliwy jest tylko odczyt wartości cewek. Co zostało zobrazowane na poniższym rysunku.



Nie jest możliwe wpisywanie nowych wartości.

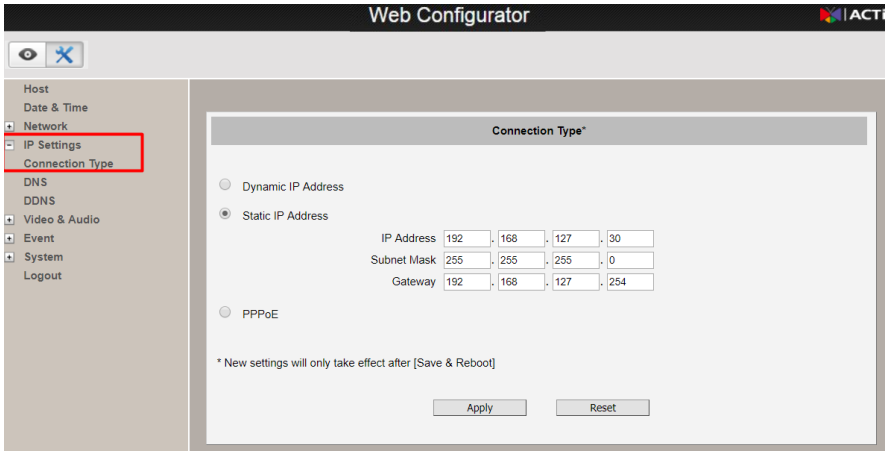


6. Konfiguracja kamery Acti A24

Konieczna jest zmiana adresacji kamery. Aby wyszukać urządzenie w sieci można skorzystać z dedykowanego oprogramowanie producenta – IP Utility.

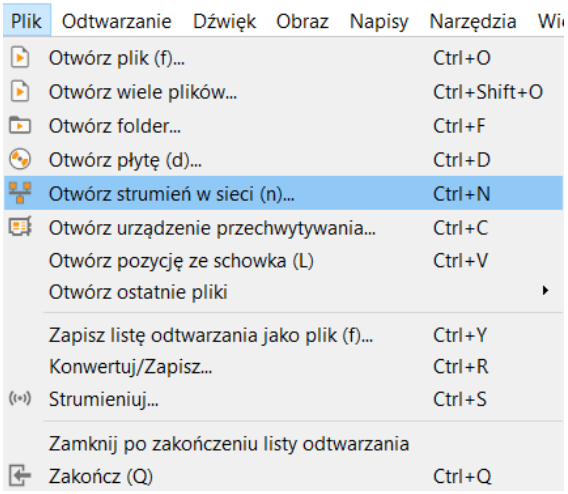
Po wpisaniu adresu IP w przeglądarce powinien ukazać się panel konfiguracyjny (domyślny login: admin, hasło:123456).

Należy zmienić adres IP na 192.168.127.30.



Podgląd obrazu można uzyskać wykorzystując protokół RTSP i program VLC media player.

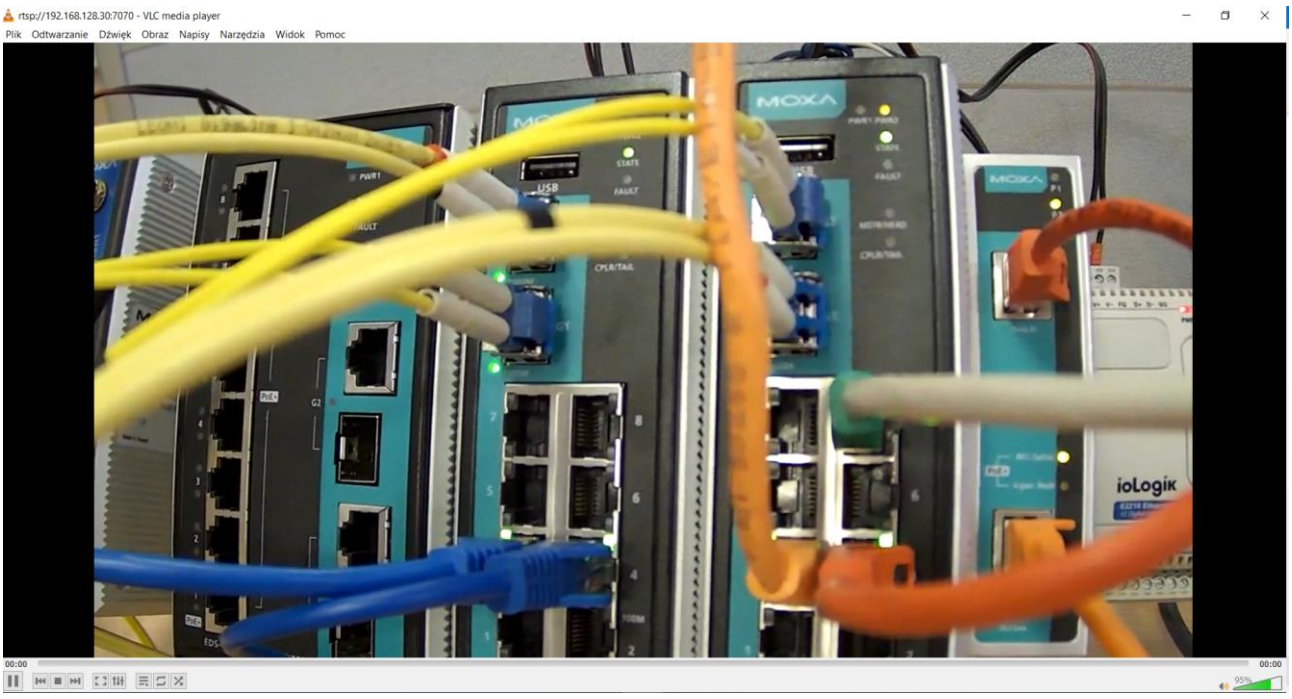
W programie VLC media player:



Wpisując komendę:

rtsp://[admin]:[123456]@192.168.128.30:7070

uzyskamy dostęp do obrazu video w czasie rzeczywistym:



7. Konfiguracja AWK-3131 – tryb Access Point

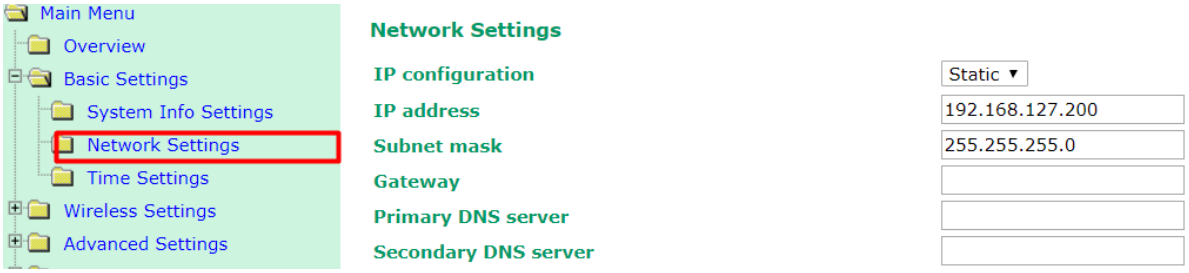
Szczegółowe informacje na temat konfiguracji urządzeń bezprzewodowych Wi-Fi można znaleźć na naszym blogu.

[Konfiguracja urządzeń bezprzewodowych Wi-Fi]

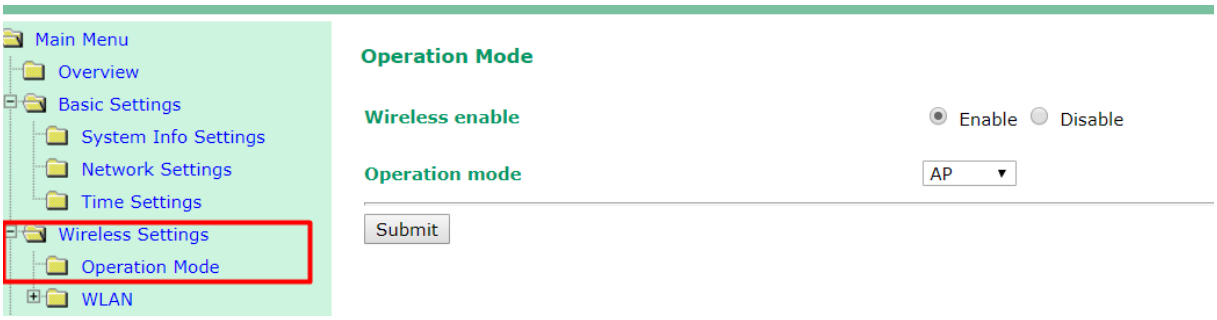
Domyślny adres IP – 192.168.127.253, login: moxa, hasło: root

Po wpisaniu powyższych danych w przeglądarce uzyskamy dostęp do panelu konfiguracyjnego.

W zakładce Basic settings→Network settings konieczna jest zmiana adresu IP na 192.168.127.200



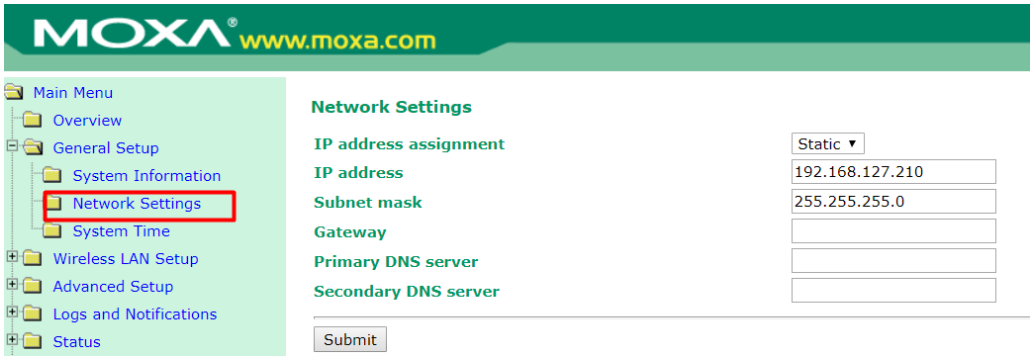
A w zakładce Wireless settings → Operation Mode konieczna jest zmiana trybu pracy na AP – czyli Access Point.



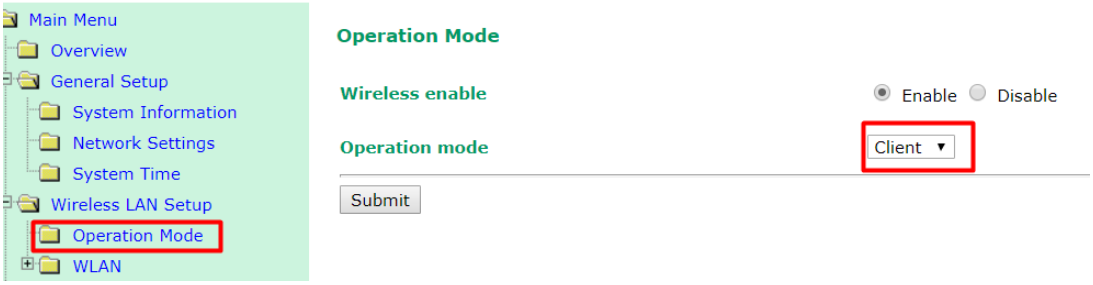
Po wpisaniu ustawień należy zapisać zmiany i zrestartować urządzenie.

8. Konfiguracja AWK-1131A – tryb Client

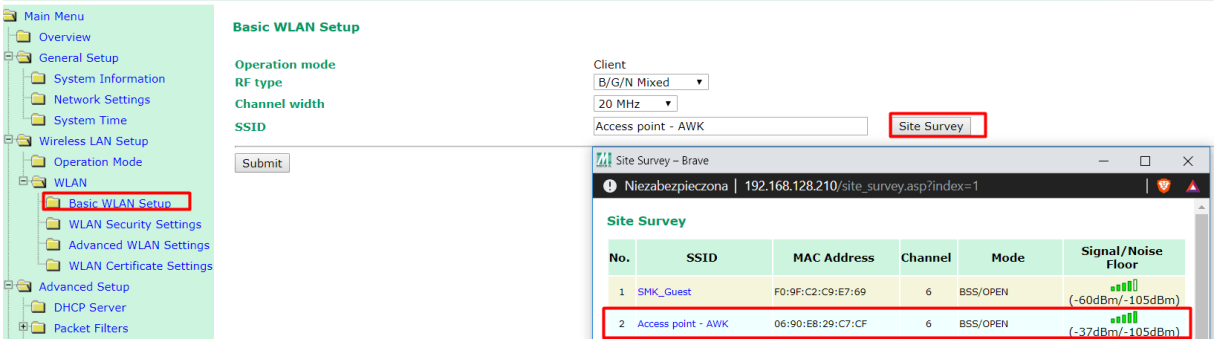
Podobnie jak w punkcie 7, AWK-1131A ma te same domyślne ustawienia. Należy zmienić adres IP na 192.168.127.210



Tym razem tryb pracy, który trzeba ustawić to – Client



W zakładce Basic WLAN Setup należy wybrać wcześniej skonfigurowany identyfikator sieci, który jest dodawany do nagłówków pakietów wysyłanych przez urządzenie – SSID, tak jak na screenie poniżej.

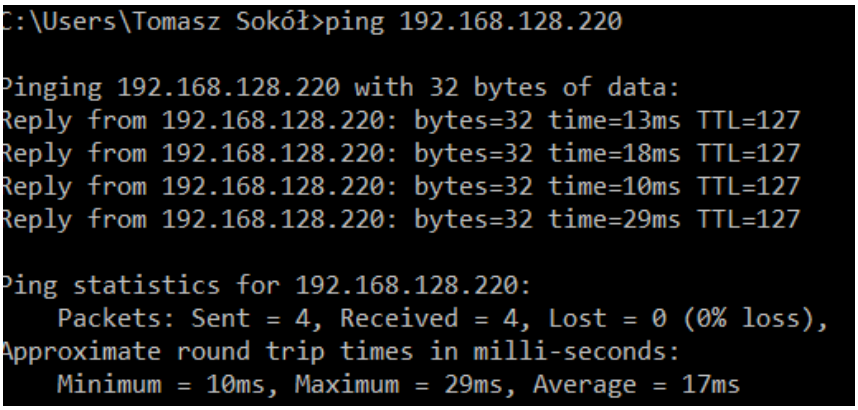


Po zapisaniu ustawień, należy zrestartować urządzenie.

9. Konfiguracja PLC

Aby uzyskać komunikację ze sterownikiem PLC, należy zmienić jego adres IP na 192.168.127.220 i maskę podsieci 255.255.255.0

Urządzenie w sieci WAN jest dostępne pod adresem 192.168.128.220. Po poprawnej konfiguracji, komunikacja ze sterownikiem powinna być możliwa.



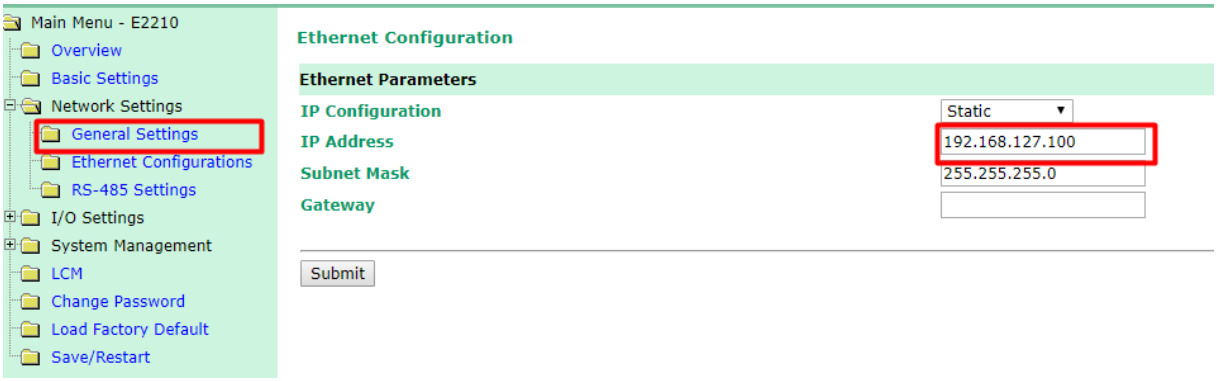
10. Konfiguracja iologik E2210

Do konfiguracji produktów serii ioLogik E2210 służy dedykowane oprogramowanie producenta – ioAdmin, które można pobrać ze strony – link. Konfiguracja może się również odbywać przy użyciu konsoli webowej. Domyślny adres IP to 192.168.127.253.

W zakładce Network Settings → Ethernet Configuration należy zmienić adres IP na 192.168.127.100.

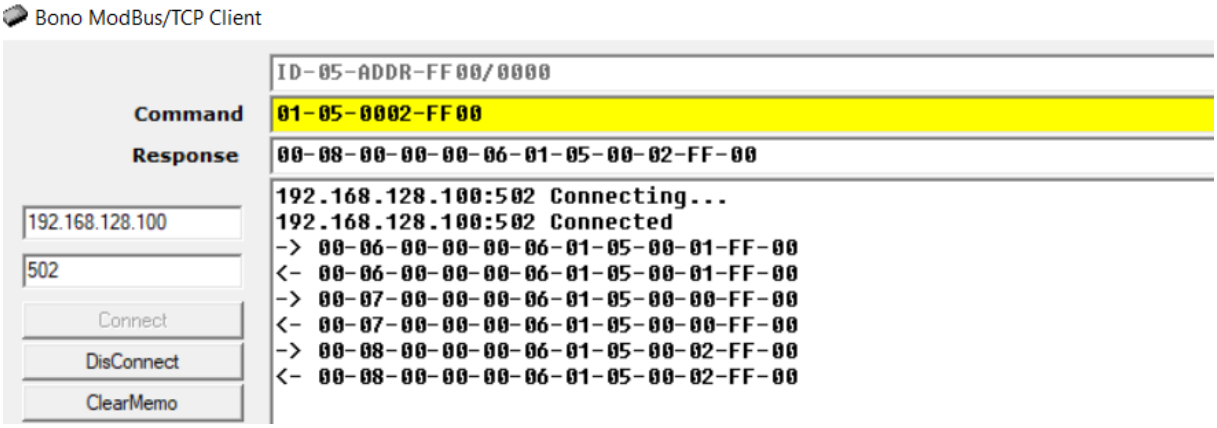
Urządzenie jest dostępne w sieci WAN pod adresem 192.168.128.100.

```
C:\Users\Tomasz Sokół>ping 192.168.128.100

Pinging 192.168.128.100 with 32 bytes of data:
Reply from 192.168.128.100: bytes=32 time=2ms TTL=254
Reply from 192.168.128.100: bytes=32 time=1ms TTL=254
Reply from 192.168.128.100: bytes=32 time=1ms TTL=254
Reply from 192.168.128.100: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.128.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```



Zgodnie z regułami firewall, użytkownik, który łaczy się do iologik E2210 ma możliwość zmiany wyjść cyfrowych i odczytywania stanu cewek.

Aby sprawdzić, czy reguły inspekcji pakietów Modbus działają, włączono pierwsze trzy wyjścia cyfrowe:

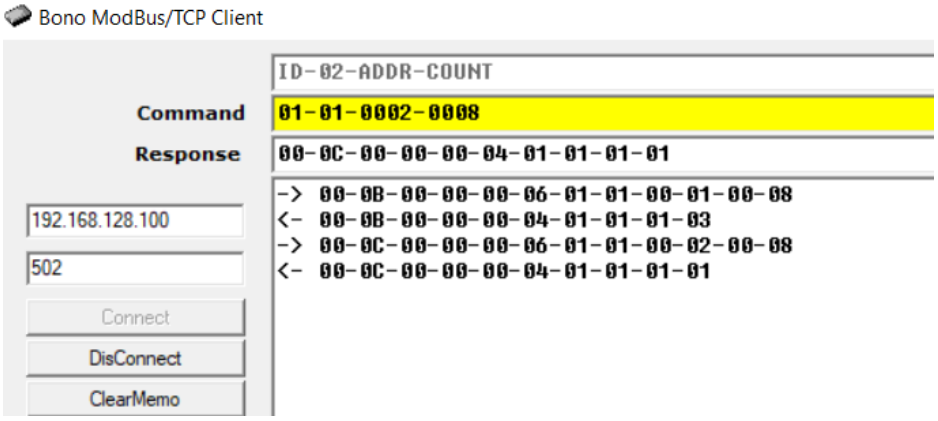


Które zmieniły status na ON

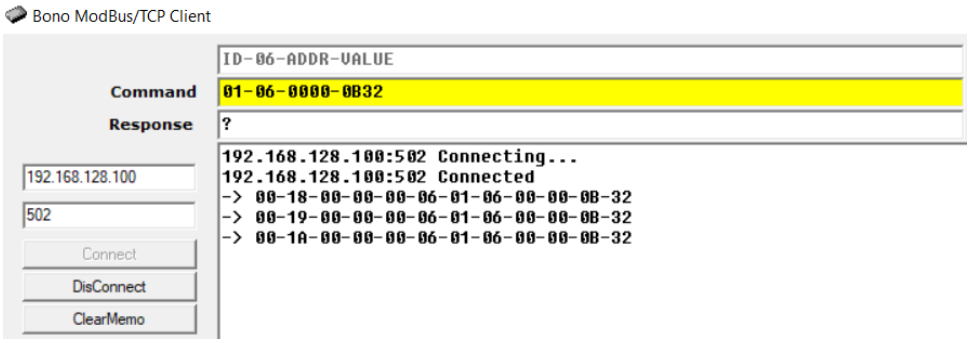
DO Channel Settings

DO Channel #	Mode	Status
DO-00	DO	ON
DO-01	DO	ON
DO-02	DO	ON
DO-03	DO	OFF
DO-04	DO	OFF
DO-05	DO	OFF
DO-06	DO	OFF
DO-07	DO	OFF

Odczytywanie stanu cewek również jest możliwe (kod funkcji 01):

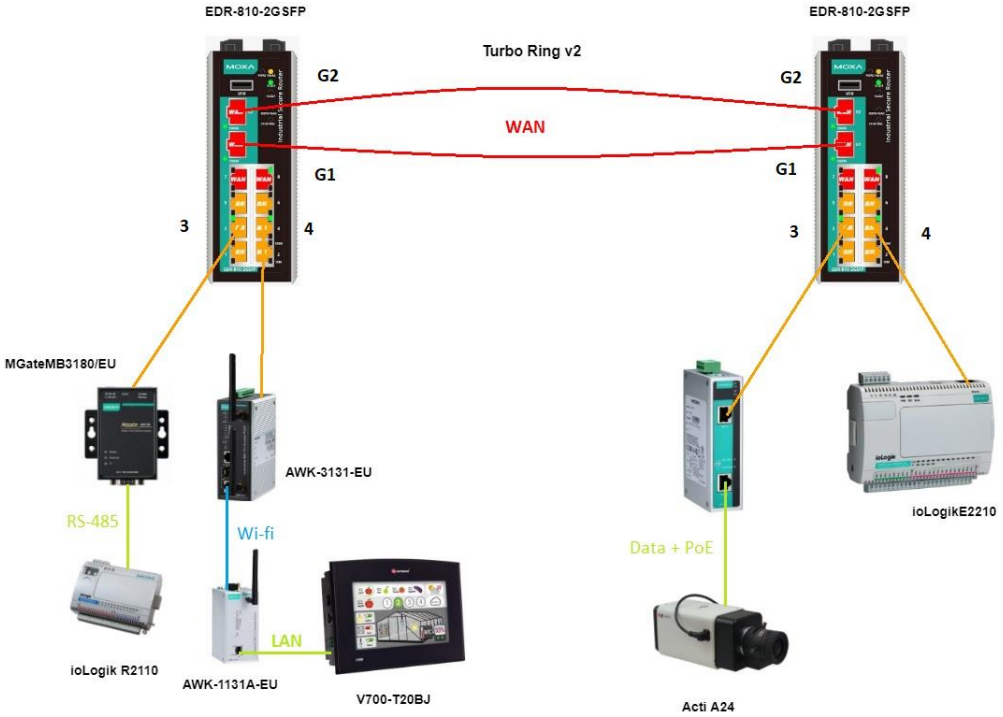


Pozostałe zapytania Modbus są odrzucane:

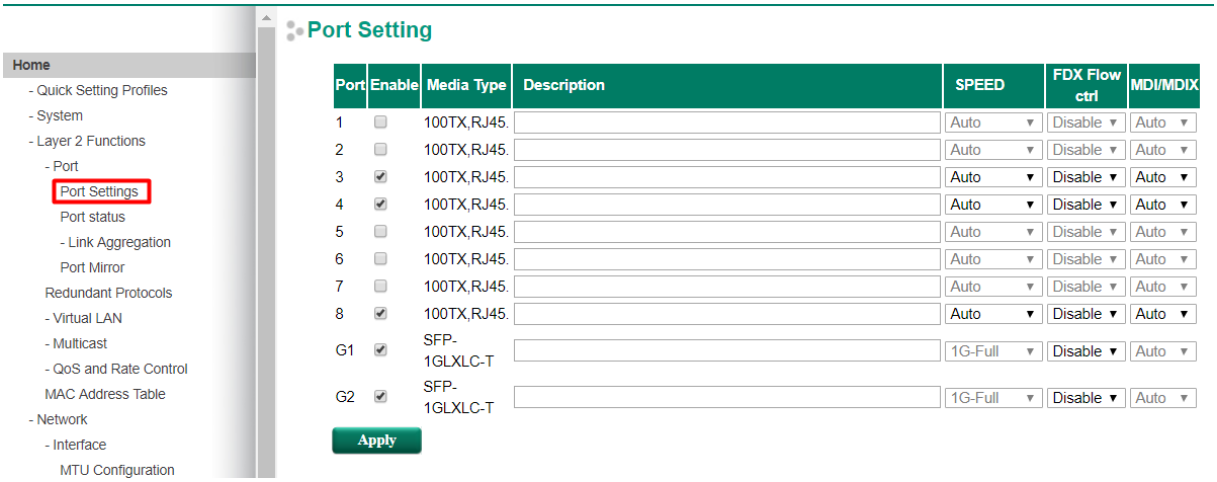


11. Podłączenie urządzeń

Urządzania zostały podłączone zgodnie z poniższym schematem.



Nieużywane porty, w ramach bezpieczeństwa można wyłączyć w ustawieniach routera – w zakładce: Layer 2 Function → Port → Port Settings.



Urządzenia są zasilacze zasilaczem SDR-120-12. Natomiast kamera jest zasilana z wykorzystaniem technologii PoE. Napięci 10V jest niewystarczające do zasilania kamer, dlatego zastosowano injector PoE (INJ-24A), który zasilany jest napięciem 48V.

12. Podsumowanie

Główną ideą tego wpisu było pokazanie funkcjonalności i możliwości konfiguracji firewalla na routerach przemysłowych Moxa EDR-810. Topologia, która została zbudowana i opisana porusza rzeczywiste problemy, które mogą pojawić się podczas tworzenia infrastruktury przemysłowej. Konfigurowanie firewall w dużym stopniu można dostosować do danej aplikacji, możliwości jest bardzo dużo. Możliwe jest również nadzorowanie infrastruktury sieciowej, uzyskiwanie powiadomień o próbach nieautoryzowanego dostępu do sieci, z wykorzystaniem pakietu MXStudio.

Więcej informacji na ten temat na naszym blogu:

Problematyka konfiguracji i zarządzania sieciami Ethernet na przykładzie pakietu MXstudio

Zachęcam do czytania naszego bloga: http://moxa.elmark.com.pl

W przypadku pytań można się z nami skontaktować mailowo: moxa@elmark.com.pl