



Bezpieczny dostęp do danych w sieci przemysłowej – konfiguracja.

Spis treści

1.	Wstęp	1
2.	Przeląd funkcjonalności firewall na EDR-810	3
F	irewall	3
Ν	Nodbus Deep Packet Inspection	7
3.	Konfiguracja EDR-810	8
Ir	nterfejsy	8
N	IAT	11
Т	urbo Ring v2	12
F	irewall	13
4.	Konfiguracja MGate MB3180	15
5.	Konfiguracja iologik R2110	16
6.	Konfiguracja kamery Acti A24	17
7.	Konfiguracja AWK-3131 – tryb Access Point	18
8.	Konfiguracja AWK-1131A – tryb Client	19
9.	Konfiguracja PLC	20
10.	Konfiguracja iologik E2210	20
11.	Podłączenie urządzeń	22
12.	Podsumowanie	23

1. Wstęp

Opis konfiguracyjny jest integralną częścią wpisu opublikowanego na <u>blogu Moxa</u>. 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.

Elmark Automatyka Sp. z o.o.







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 – <u>Adresacja urządzeń w sieci przemysłowej z wykorzystanie NAT</u>).

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

Elmark Automatyka Sp. z o.o.





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.

Moxa Industrial Secure Router									
EDR-810-2GSFP									
Username :	admin								
Password :	••••								
	(Login							

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

Home

- Quick Setting Profiles
- Interface Type Quick Setting
- System
- Layer 2 Functions
- Network
- Network Service
- Routing

- NAT

Firewall 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.

Interfac	e From	WAN TO BRG_LAN V								
Show	v									
Filter L	.ist (3/:	256)								
Enable	Index	Input	Output	Protocol	Source IP	Source Port	Destination IP	Destination Port	Source MAC	Action
~	1	WAN	BRG_LAN	All	192.168.128.10	All	All	All		ACCEPT

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

Enable	×	Action	ACCEPT V	
Interface EtherType	From PORT1 V To PORT2 V All V	Source MAC Destination MAC	Single Single	00:00:00:00:00:00 00:00:00:00:00:00
Add	Modify Delete Move	Apply		

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.

Layer 3 Policy						
Global Setting						
Firewall Event Log	Disable •					
Malformed Packets	Disable •	Severity <0> Emerger	ncy 🔻 Flash 🗹	Syslog 🗹 SNMP Ti	ap 🕑	
Policy Setting						
Name	рс			Action	ACCEPT V	
Enable				Source IP	Single •]
Severity	<0> Emergency •	Flash 🗹 Syslog 🗹	SNMP Trap 🕑	Source IP-MAC	Disable v	1
Interface From	ALL		•	Binding		1
То	ALL		T	Source Port	All v	
Automation Profile	All		٣	Destination IP	Range •	~
Filter Mode	IP Address Filter		▼	Destination Port	All v	

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.

Severity	<0> Emergency •	🛛 🖌 Flash 🗹	Syslog 🗹	SNMP Trap 🕑
	<0> Emergency			
Interface From	<1> Alert]		•
То	<2> Critical			•
	<3> Error			
Automation Profile	<4> Warning			•
Filter Mede	<5> Notice			-
Filler Wode	<6> Informational			•
	<7> Debug			

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





 TCP UDP ICMP EtherNet/IP I/O (TCP) EtherNet/IP I/O (UDP) EtherNet/IP messaging (TCP) EtherNet/IP messaging (UDP) FF Annunciation (TCP) FF Annunciation (UDP) 	I
UDP ICMP EtherNet/IP I/O (TCP) EtherNet/IP I/O (UDP) EtherNet/IP messaging (TCP) EtherNet/IP messaging (UDP) FF Annunciation (TCP) FF Annunciation (UDP)	est
ICMP Instant, if if of the parameter is go proceeded EtherNet/IP I/O (TCP) zostanie przypisany zdefiniowany programowo EtherNet/IP messaging (TCP) numer portu docelowego. FF Annunciation (TCP) FF Annunciation (UDP)	
EtherNet/IP I/O (TCP) Zostanie przypisany zdefiniowany programowo EtherNet/IP I/O (UDP) numer portu docelowego. EtherNet/IP messaging (UDP) FF Annunciation (TCP) FF Annunciation (UDP) FF Annunciation (UDP)	
EtherNet/IP I/O (UDP) EtherNet/IP messaging (TCP) EtherNet/IP messaging (UDP) FF Annunciation (TCP) EF Annunciation (UDP)	
EtherNet/IP messaging (TCP) EtherNet/IP messaging (UDP) FF Annunciation (TCP) EF Annunciation (UDP)	
EtherNet/IP messaging (UDP) FF Annunciation (TCP) FF Annunciation (UDP)	
FF Annunciation (TCP) FF Annunciation (UDP)	
FE Annunciation (UDP)	
FF Fieldbus Message Specification (TCP)	
FF Fieldbus Message Specification (UDP)	
FF System Management (TCP)	
FF System Management (UDP)	
FF LAN Redundancy Port (TCP)	
FF LAN Regulatory Port (UDP)	
LonWorks (UDP)	
Automation Profile EtherNet/IP I/O (TCP)	
Filter Mode IP Address Filter Destination Port Single 2222	

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
	2	1	WAN	BRG_LAN	All	192.168.128.10		All	All	All	ACCEPT	Enable / <0> Emergency
l	-	2	BRG_LAN	WAN	All	All		All	192.168.128.1 ~192.168.128.20	All	ACCEPT	Enable / <0> Emergency
ł	2	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	I
	 Image: A second s	2	BRG_LAN	WAN	All	All	-	All	192.168.128.1 ~192.168.128.20	All	DROP	Enable / <0> Emergency	I
	-	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)



Elmark Automatyka Sp. z o.o. ul. Niemcewicza 76, 05-075 Warszawa-Wesoła, tel. (+48) 22 773 79 37; elmark@elmark.com.pl; www.elmark.com.pl NIP: 525-20-72-585; KRS: 0000157170, Sąd Rejonowy dla M-St. Warszawy, XIII Wydział Gosp. KRS; Kapitał Zakładowy 500.000 zł





• 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.

• DoS	(Deny of Service) Setting
	Null Scan
	Xmas Scan
	NMAP-Xmas Scan
	SYN/FIN Scan
	FIN Scan
	NMAP-ID Scan
	SYN/RST Scan
	NEW-Without-SYN Scan
	ICMP-Death Limit: 4000 (pkt/s)
	SYN-Flood Limit: 4000 (pkt/s)
	ARP-Flood Limit: 4000 (pkt/s)
Do	S Log Setting
Log	Enable Disable Severity <0> Emergency Flash Syslog SNMP Trap

Modbus Deep Packet Inspection

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

O protokole Modbus można przeczytać na naszym blogu: <u>Konwersja protokołu Modbus i konwertery</u> <u>firmy Moxa</u>. 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.





Modbus TCP Filteri	ng
Modbus TCP Master Master Query	Modbus TCP Slave
Modbus Setting Global Setting Drop Multiple Function Drop Malformed Packets Modbus Service Port 502	
Policy Setting	
Enable 🕑	Action DROP V
From ALL TO ALL T	Source IP All V
Protocol All 🔻	Destination IP All
Slave ID 0: Ignore checking slave ID	
Function Code All	
Command Type 🔻	
Address All T	PLC Address (Base 1)
Add Delete Modify Move	Apply

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.

	Port Typ Connect Typ Static IP	e Interface	Servio	ce Confirm
	IP Address	192.168.128.254	Gateway	
	Subnet Mask	255.255.255.0		
WAN GI Ducu 2 WAN WAN 5 BR BR 6 3 BR BR 4	PPTP Dialup PPTP Connection User Name	p Enable	IP Address Password	
1 BR BR 2 EDR 810-2GSFP	Prev Step			Next Step

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.





		Port Type	Interface	Service	Confirm
		Enable DHCP Serve	er at Bridge Interface		
MOXA		Offered IP Range	From 192.168.127.1	To 1	92.168.127.253
Kout		Enable N-1 NAT for	Bridge Interface to W/	AN	
USB suur g		IP Range	From 192.168.127.1	To 1	92.168.127.254
CHATMA LL					
,					
1354					
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1					
DR-810-2GSFP	Pre	v Step			Next Step
y					- Contraction of the second seco

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

	Port Type	Interface	Service	Confirm
	After applying, please check	your configuration.	Service	
5 BR BR 6 3 BR BR 4 1 BR BR 2 1 USW 2	Prev Step			Apply





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

	Port Ty	pe Interface	Servic	ce Confirm
	Static IP	/pe ▼		•
dustra en esta	Address In IP Address Subnet Mask	formation 192.168.128.253 255.255.255.0	Gateway	
VIAN GI VIAN VIAN VIAN VIAN VIAN VIAN C URAN C UR	PPTP Dialu PPTP Connection User Name	IP	IP Address Password	
	Prev Step			Next Step

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 - <u>Adresacja urządzeń w sieci przemysłowej z</u> <u>wykorzystaniem NAT</u>. 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)											
l	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		
ł	/	5	WAN		192.168.127.220		192.168.128.220			plc		

Router 2

NAT Lis	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 \rightarrow Port \rightarrow Redundant Protocols.

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

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

iurbo Ring V2 St	atus		
Now Active	Turbo Ring V2		
Ring 1		Ring 2	
Status	Healthy	Status	Disabled
Master/Slave	Master	Master/Slave	
Master ID	00:90:e8:71:fe:6a	Master ID	00:00:00:00:00:00
1st Ring Port Status	Up,Forwarding	1st Ring Port Sta	tus
2nd Ring Port Status	Up,Blocked	2nd Ring Port Sta	atus
Ring Coupling			
O	Mana		
Coupling Mode	None		
Coupling Mode Coupling Port Status	None Primary Port Backup Po	ort	
Coupling Mode Coupling Port Status	Primary Port Backup Po	ort	
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protoco	None Primary Port Backup Po tting I Turbo Ring V2	• • • • •	
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protoco Enable Ring 1	tting	ort	Ring 2
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protoco Enable Ring 1 Set as Mas	Primary Port Backup Po tting I Turbo Ring V2 ter	• Enable	Ring 2 Set as Master
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protocc I Enable Ring 1 I Set as Mas Redundant pr	None Primary Port Backup Po tting I Turbo Ring V2 ter tris 1st Port G1 ▼	rt Enable Ret	Ring 2 Set as Master Jundant ports 1st Port 5
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protocc I Enable Ring 1 ■ Set as Mas Redundant pc	tting I Turbo Ring V2 ter vrts 1st Port G1 • 2nd Port G2 •	v Enable	Ring 2 Set as Master Jundant ports 1st Port 5 2nd Port 6
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protocc	tting I Turbo Ring V2 ter	• Enable	Ring 2 Set as Master Jundant ports 1st Port 5 2nd Port 6
Coupling Mode Coupling Port Status Turbo Ring V2 Se Redundancy Protocc I Enable Ring 1 ■ Set as Mas Redundant pc Enable Ring Cou Coupling Moc	None Primary Port Backup Port tting ol Turbo Ring V2 ter Cold V2 tris 1st Port C1 V 2nd Port C2 V pling E Dual Homing V	v Enable	Ring 2 Set as Master Jundant ports 1st Port 5 2nd Port 6





Router 2

Sommunication Redundancy Turbo Ring V2 Status Turbo Ring V2 Now Active Ring 1 Ring 2 Status Healthy Status Disabled Master/Slave Slave Master/Slave Master ID 00:90:e8:71:fe:6a Master ID 00:00:00:00:00:00 1st Ring Port Status Up,Forwarding 1st Ring Port Status ---2nd Ring Port Status Up,Forwarding 2nd Ring Port Status ---**Ring Coupling** Coupling Mode None Coupling Port Status Primary Port --- Backup Port ---Turbo Ring V2 Setting Redundancy Protocol Turbo Ring V2 Enable Ring 1 Enable Ring 2 Set as Master Set as Master Redundant ports 1st Port G1 🔻 Redundant ports 1st Port 5 🔹 2nd Port G2 🔻 2nd Port 6 🔻 Enable Ring Coupling Coupling Mode Dual Homing

Primary Port 3

Backup Port 4 Apply

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 L	ilter 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 L	.ist (3/2	256)									
Enable	Index	Input	Output	Protocol	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Action	Event Log / Severity
2	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)

Mo	dbus Lis	t	(3/64)							
Inde	ex 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	Image: A start of the start	ALL	ALL	All			0	All		DROP

Router 2

Layer 2 Policy

Filter	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 <u>z oficjalnej strony producenta</u> <u>urządzeń Moxa</u>.

Po wyszukaniu urządzenia konieczna jest zmiana jego adresu IP na 192.168.127.15

Basic	Network	Serial	Pro	tocol	S	yste	em				
Ne	twork Confi	igure		Statio	:			\sim	1		
TP	Address			102			_	107		15	1
1	A001 C33			192	•	108	•	12/	•	15]
Ne	tmask			255		255		255		0]
6.											1
Ga	iteway			0	•	0	•	0	•	0]
DN	IS1			0		0		0		0]
											1
DN	IS2			0	•	0		0		0	

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.

Basic Network	c Serial	Protocol	System	
Port 1				
Baudrate Fl	ow Control			
115200 V No	ne	1		
115200	// N_			
Parity FI	FO			
		_		
None 🗸 En	able 🕚	~		
Stop bit In	terface			
$1 \lor RS$	3485 2-wi 🕚	-		
Data bits				
8 ~				

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 "O", która zapewni takie same ustawienia komunikacji szeregowej, jakie są ustawione na lologik R2110

150	Baudrate for RS-485	Dial setting	g and corres	ponding bar	udrate:
	(parameters are N, 8, 1)	0:115200	1:57600	2:38400	3:19200
200		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.

de	Modbus	Mod	Ibus Routing		
Port R	louting T	able _			
Slave C.	ID Table	ing	Туре	Slave ID Range (Virtual<->Real) Destin	ation
Slave C. 01	ID Table Rout I. Manu	ing Jal	Type Modbus Serial	Slave ID Range (Virtual <->Real) Destin 001 - 254 <-> 001 - 254 Port1	ation (Serial)

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.





Х

Bono ModBus/TCP Client

	ID-82-ADDR-COUNT	- 1 -0
Command	0A-02-0000-0008	Modbus
Response	00-11-00-00-00-04-0A-02-01-00	
192.168.128.15 502	192.168.128.15:502 Connecting 192.168.128.15:502 Connected -> 00-11-00-00-00-06-0A-02-00-00-00-08 <- 00-11-00-00-00-04-0A-02-01-00	^
Connect DisConnect ClearMemo		
Send		

Nie jest możliwe wpisywanie nowych wartości.

Bono ModBus/TCP Client		- 🗆 ×
	ID-05-ADDR-FF 00/0000	- Sec
Command	0A-05-0000-FF00	Modbus
Response	?	~
192.168.128.15 502 Connect DisConnect ClearMemo	192.168.128.15:502 Connecting 192.168.128.15:502 Connected > 00-11-00-00-00-00-00-00-00-00-00 <- 00-11-00-00-00-00-00-00-00-00-00 > 00-12-00-00-00-00-00-00-00-FF-00 -> 00-13-00-00-00-00-00-00-00-FF-00 -> 00-14-00-00-00-00-00-00-00-FF-00 -> 00-16-00-00-00-00-00-00-FF-00 -> 00-17-00-00-00-00-00-00-FF-00 -> 00-17-00-00-00-00-00-00-FF-00 -> 00-18-00-00-00-00-00-00-FF-00	A

6. Konfiguracja kamery Acti A24

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

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.

	Web Configurator	ACTi
• 🗙		
Host Date & Time Network IP Settings Connection Type DNS DDNS DDNS Video & Audio Event System Logout	Connection Type* Dynamic IP Address Static IP Address IP Address IP Address Subnet Mask 255 255 0 Gateway 192 168 127 30 Gateway 192 168 127 254	
	PPPoE New settings will only take effect after [Save & Reboot] Apply Reset	

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





W programie VLC media player:

Plik	Odtwarzanie	Dźwięk	Obraz	Napisy	Narzędzia	Wie
Þ	Otwórz plik (f)				Ctrl+O	
Þ	Otwórz wiele pl	ików			Ctrl+Shift+	0
►	Otwórz folder				Ctrl+F	
	Otwórz płytę (d)			Ctrl+D	
<u>.</u>	Otwórz strumier	ń w sieci (n)		Ctrl+N	
5	Otwórz urządze	nie przecl	hwytywa	nia	Ctrl+C	
	Otwórz pozycję	ze schow	ka (L)		Ctrl+V	
	Otwórz ostatnie	pliki				•
	Zapisz listę odt	warzania j	iako plik	(f)	Ctrl+Y	
	Konwertuj/Zapi	SZ			Ctrl+R	
((*))	Strumieniuj				Ctrl+S	
	Zamknij po zako	ończeniu l	listy odtv	varzania		
C	Zakończ (Q)				Ctrl+Q	

Wpisując komendę:

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

uzyskamy dostęp do obrazu video w czasie rzeczywistym:



49 95%

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

Main Menu Overview	Network Settings	
Basic Settings	IP configuration	Static 🔻
- System Info Settings	IP address	192.168.127.200
- Network Settings	Subnet mask	255.255.255.0
Time Settings	Gateway	
🖲 🔲 Wireless Settings	Primary DNS server	
🖻 🦲 Advanced Settings	Secondary DNS server	

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

Main Menu	Operation Mode	
Basic Settings	Wireless enable	Enable Disable
Network SettingsTime Settings	Operation mode	AP T
Use Wireless Settings	Submit	
🖻 🚞 WLAN		

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

ΜΟΧΛ°₩₩	w.moxa.com	
Main Menu	Network Settings	
🖣 🔄 General Setup	IP address assignment	Static 🔻
System Information	IP address	192.168.127.210
Network Settings	Subnet mask	255.255.255.0
System Time	Gateway	
🗉 🧰 Wireless LAN Setup	Primary DNS server	
🖶 🧰 Advanced Setup	Secondary DNS server	
🖻 🧰 Logs and Notifications		
🗉 🧰 Status	Submit	

Tym razem tryb pracy, który trzeba ustawić to - Client

Main Menu	Operation Mode	
🗀 Overview	operation noue	
📲 General Setup	Wireless enable	Enable Disable
💼 System Information		
💼 Network Settings	Operation mode	Client 🔻
🛄 System Time		
 🕤 🔄 Wireless LAN Setup	Submit	
间 Operation Mode		
🗄 🧰 WLAN		

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.





Main Menu	Basic WLAN Setup						
Image: Second	Operation mode RF type Channel width SSID	Client B/G/N 20 MH Access	I Mixed • Iz • s point - AWK	(Site Surve	·y	
Operation Mode	Submit	Site	e Survey – Brave				- 🗆 X
Basic WLAN Setup	Viezabezpieczona 192.168.128.210/site_survey.asp?index=1 Site Survey						
Advanced WLAN Settings WLAN Certificate Settings		No.	SSID	MAC Address	Channel	Mode	Signal/Noise Floor
Advanced Setup		1	SMK_Guest	F0:9F:C2:C9:E7:69	6	BSS/OPEN	(-60dBm/-105dBm)
Packet Filters		2	Access point - AWK	06:90:E8:29:C7:CF	6	BSS/OPEN	(-37dBm/-105dBm)

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.

C:\Users\Tomasz Sokół>ping 192.168.128.220
Pinging 192.168.128.220 with 32 bytes of data:
Reply from 192.168.128.220: bytes=32 time=13ms TTL=127
Reply from 192.168.128.220: bytes=32 time=18ms TTL=127
Reply from 192.168.128.220: bytes=32 time=10ms TTL=127
Reply from 192.168.128.220: bytes=32 time=29ms TTL=127
Ping statistics for 192.168.128.220:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 29ms, Average = 17ms

10.Konfiguracja iologik E2210

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

W zakładce Network Settings \rightarrow 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>p	ing 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 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 Main Menu - E2210 Main Menu - E2210 Main Menu - E2210 Main Menu - E2210 Rehernet Configuration Ethernet Configuration IP Address Subnet Mask Gateway System Management LCM Change Password Log Eactory Defuit		
Ping statistics for 192 Packets: Sent = 4, Approximate round trip Minimum = 1ms, Maxi	.168.128.100: Received = 4, Lost = 0 (0% loss), times in milli-seconds: mum = 2ms, Average = 1ms	
Main Menu - E2210 Overview	Ethernet Configuration	
- Basic Settings	Ethernet Parameters	
🖻 🔄 Network Settings	IP Configuration	Static 🔻
📋 General Settings	IP Address	192.168.127.100
Ethernet Configurations	Subnet Mask	255.255.255.0
RS-485 Settings	Gateway	
System Management		
	Submit	
Change Password		
Load Factory Default		
ave/Restart		

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:

Bono ModBus/TCP Client

	1D-05-HDDK-FF 00/0000
Command	01-05-0002-FF00
Response	00-08-00-00-06-01-05-00-02-FF-00
192.168.128.100 502 Connect DisConnect	192.168.128.100:502 Connecting 192.168.128.100:502 Connected -> 00-06-00-00-00-06-01-05-00-01-FF-00 <- 00-06-00-00-06-01-05-00-01-FF-00 -> 00-07-00-00-06-01-05-00-00-FF-00 <- 00-07-00-00-06-01-05-00-00-FF-00 -> 00-08-00-00-06-01-05-00-02-FF-00 <- 00-08-00-00-06-01-05-00-02-FF-00
ClearMemo	

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

Elmark Automatyka Sp. z o.o.

ul. Niemcewicza 76, 05-075 Warszawa-Wesoła, tel. (+48) 22 773 79 37; elmark@elmark.com.pl; www.elmark.com.pl NIP: 525-20-72-585; KRS: 0000157170, Sąd Rejonowy dla M-St. Warszawy, XIII Wydział Gosp. KRS; Kapitał Zakładowy 500.000 zł





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

Bono M	odBus/TCP Client
--------	------------------

	ID-02-ADDR-COUNT
Command	01-01-0002-0008
Response	89-90-99-99-99-94-91-91-91-91
192.168.128.100 502	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$
Connect	
DisConnect	
ClearMemo	

Pozostałe zapytania Modbus są odrzucane:

Bono ModBus/TCP Client	
	ID-06-ADDR-VALUE
Command	01-06-0000-0B32
Response	?
192.168.128.100 502 Connect DisConnect	192.168.128.100:502 Connecting 192.168.128.100:502 Connected -> 00-18-00-00-06-06-01-06-00-08-08-32 -> 00-19-00-00-06-01-06-00-00-08-32 -> 00-1A-00-00-06-01-06-00-00-08-32

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 \rightarrow Port \rightarrow Port Settings.

	^	Por	t Set	ting	g						
Home									FDX Flow		
- Quick Setting Profiles		P	ortEna	able	Media Type	Description	SPEED		ctrl	MDI/N	IDIX
- System		1			100TX,RJ45.		Auto	v	Disable v	Auto	Ŧ
- Layer 2 Functions		2			100TX.RJ45.		Auto		Disable v	Auto	Ŧ
- Port		3					Auto	-	Disable •	Auto	-
Port Settings			•		10017,1045.				Disable +	Auto	•
Port status		4			1001X,RJ45.		Auto	•	Disable •	Auto	•
- Link Aggregation		5			100TX,RJ45.		Auto	Ŧ	Disable v	Auto	Ψ.
Port Mirror		6			100TX,RJ45.		Auto	W	Disable v	Auto	۳
Redundant Protocols		7			100TX,RJ45.		Auto	V	Disable •	Auto	Ŧ
- Virtual LAN		8	•		100TX,RJ45.		Auto	v	Disable •	Auto	T
- Multicast		6	1 🖃		SFP-				Dischle =	Auto	
- QoS and Rate Control		6			1GLXLC-T		IG-Full	*	Disable •	Auto	Ŧ
MAC Address Table		G	62 🕑	1	SFP-		1G-Full		Disable •	Auto	
- Network					1GLXLC-T						
- Interface			Apply	7							
MTU Configuration											

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