Moxa Technical Support Team <u>support@moxa.com</u>

Contents

1	Intro	oduction	2
2	Impo	ortant Benefits of a DMZ	2
3	Refe	rence Scenario 1: LAN Fully Isolated From the Internet	4
	3.1	Architecture	4
	3.2	Scenario 1 Configuration Guide	5
	3.3	Expected Result	9
4	Refe	rence Scenario 2: Isolated LAN With Limited Internet Access	12
	4.1	Architecture	12
	4.2	Scenario 2 Configuration Guide	13
	4.3	Expected Result	16
5	Refe	rence Scenario 3: LAN Fully Isolated From the Internet, With Modbus	
	Com	munications	19
	5.1	Architecture	19
	5.2	Scenario 3 Configuration Guide	20
	5.3	Expected Result	26

Copyright © 2024 Moxa Inc.

Released on May 14, 2024

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777 Fax: 1-714-528-6778



1 Introduction

A demilitarized zone, or DMZ for short, is a crucial concept in network security. It is a region located between an organization's internal trusted network and the external untrusted network. The primary purpose of a DMZ is to provide an additional layer of security while allowing certain network services and resources to be visible to the external world.

This guide provides information and instructions on how to set up a DMZ for different scenarios using Moxa's Secure Router Series devices.

2 Important Benefits of a DMZ

The Purdue Model of Industrial Control Systems (ICS) Security is a widely recognized framework for securing industrial networks. In this model, the Level 3.5 DMZ plays a crucial role in ensuring the security and reliability of critical industrial processes.



The Purdue Model

A DMZ provides several important security advantages, including:

Segregation and Protection: The DMZ acts as a buffer zone between the enterprise network (Level 4) and the process control network (Level 0-3). It provides a clear segregation of the different network levels, ensuring that critical industrial processes remain isolated from less secure enterprise networks.

Controlled Access: The DMZ allows for controlled access to and from the process control network. It enforces strict security policies to limit interactions with the industrial network, reducing the attack surface and preventing unauthorized access.

Security Inspection: Security devices, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and application-layer gateways (ALG), are usually deployed in the DMZ. These devices inspect network traffic, detect anomalies, and prevent malicious activities from reaching the critical process control network.

Network Monitoring: The DMZ provides a vantage point for monitoring network traffic between the enterprise network and the process control network. Security teams can analyze traffic patterns, detect potential threats, and respond promptly to any security incidents.

Data Exchange Gateway: In many industrial environments, data exchange between the enterprise network and the process control network may still be necessary for reporting, data analytics, and remote monitoring purposes. The DMZ serves as a secure gateway for facilitating this data exchange without compromising the integrity of industrial processes.

Resilience and Redundancy: Redundancy and failover mechanisms can be implemented within the DMZ to ensure the continuity of critical industrial processes. Proper redundancy tools help maintain the availability of essential services and minimize downtime from network disruptions.

Compliance and Auditing: Many industries have regulatory requirements for network security and data protection. The DMZ helps organizations comply with these regulations by enforcing security policies and providing a clear separation of networks.

Risk Mitigation: By placing security controls and monitoring functions within the DMZ, organizations can mitigate the risks associated with cyberthreats and vulnerabilities. This minimizes the potential impact of security incidents on industrial operations.

The following sections will introduce three different DMZ implementation scenarios. Each section will provide guidelines on how to set up the Moxa Secure Router for each scenario.

NOTE The instructions and images in this guide are for reference only and may appear different depending on which Moxa Secure Router is used.

3 Reference Scenario 1: LAN Fully Isolated From the Internet

3.1 Architecture

The user wants to access a field site from the Internet, while also protecting production equipment in the LAN from exposure to any external networks. To address this concern, the user aims to isolate direct communication from the WAN to LAN. To achieve this, the user will require an independent network zone allowing indirect data exchanges between the LAN and the Internet. To further enhance the network security of the field site, only user-specified IP addresses may access this network zone.





Key Actions:

- Configure 3 network interfaces: WAN, LAN, and DMZ. Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
- 2. Configure the Layer 3 firewall filter.
- 3. Create the allowlist policies.
- 4. Set up a DMZ to facilitate data exchange between the LAN and WAN interfaces.
- 5. Set up PAT for WAN to access the specific services in the DMZ.
- 6. Create NAT rules for the devices in the DMZ to access the Internet.

3.2 Scenario 1 Configuration Guide

As shown in the network topology below, the user intends to access the NPort web console in the LAN remotely to monitor the communication status. To enhance security and prevent unauthorized access from external networks, a DMZ is created to isolate the LAN and WAN segments.

To achieve remote access to the NPort web console, the user will connect to a remote access server (PC-2) located inside the DMZ. By allowing bidirectional communication between the DMZ and LAN, the user can access the NPort's web console through the remote server in the DMZ.

Refer to the network topology for this scenario below:



Network Topology

Communication Principles:

1. The DMZ is configured to allow bidirectional communication with the WAN.



2. The DMZ is configured to allow bidirectional communication with the LAN interface.



3. The LAN is not allowed to communicate with the WAN.



Setup Instructions:

- 1. In the Secure Router's web interface, navigate to Firewall > Layer 3-7 Policy.
- 2. In the **Global Policy Settings** section, set the Default Action to **Deny All**. This will block all communications except for user-specified IP addresses.

Global Policy	Settings		
Status		Default Action	
Enabled	-	Deny All	•
Global Policy	Event Set	tings	
Global Policy Log Enabled	Event Set	tings	

- 3. Click the **Add** (+) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
 - WAN-to-DMZ
 - DMZ-to-WAN
 - DMZ-to-LAN
 - LAN-to-DMZ

The firewall rules are subject to the network environment. Refer to the overview below as a reference for how to configure the firewall rule parameters.

Image:		Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action
2 Enabled DMZ-WAN Disabled/Warning DMZ WAN IP and Port Filtering Any Any Any Allow 2 2 Enabled DMZ-LAN Disabled/Warning DMZ LAN IP and Port Filtering Any Any Any Allow 2 4 Enabled LAN-DMZ Disabled/Warning DMZ LAN IP and Port Filtering Any Any Any Allow	/	1	Enabled	WAN-DMZ	Disabled/Warning	WAN	DMZ	IP and Port Filtering	Any	Any	Any	Any	Allow
3 Enabled DMZ-LAN Disabled/Warning DMZ LAN IP and Port Filtering Any Any Any Allow - // 4 Enabled LAN DIsabled/Warning LAN DMZ IP and Port Filtering Any Any Any Allow	/	2	Enabled	DMZ-WAN	Disabled/Warning	DMZ	WAN	IP and Port Filtering	Any	Any	Any	Any	Allow
LAN DMZ IP and Port Filtering Any Any Any Any Any Any Any	1	3	Enabled	DMZ-LAN	Disabled/Warning	DMZ	LAN	IP and Port Filtering	Any	Any	Any	Any	Allow
	1	4	Enabled	LAN-DMZ	Disabled/Warning	LAN	DMZ	IP and Port Filtering	Any	Any	Any	Any	Allow

NOTE The L3-7 firewall is a stateful firewall which allows bidirectional communication. When configuring a unidirectional communication rule (e.g. DMZ-to-LAN), a connection between the specified interfaces must be established first before the interfaces can communicate in the opposite direction.

NOTE If you want to monitor the Layer 3-7 firewall events, enable the **Global Policy Event Settings** option.

Status Enabled		▼ Defa	ult Action 19 All	*	
Global P Enabled	olicy Ever	nt Settings			
	Index	Status	Name		Event
	Index 1	Status Enabled	Name DMZ-WAN		Event Enabled/Warning

- 4. Navigate to **NAT Settings** and click the **Add** (+) icon to create a new NAT rule for the DMZ to access the Internet.
 - i. Set the **Mode** to **N-to-1** and enter the Source Start and End IP address in the **Original Packet** field. This range will determine the IP addresses in the DMZ that may connect to the Internet.

Status *		
Enabled	*	
Description		
	7/128	
Index *	1110	
2		
1 - 512		
Mode		
N-to-1	·	
Original Packet (Co	ondition)	
Source IP: Start *	Source IP: End *	
192.168.127.1	192.168.127.254	
Translated I	Packet (Action)	
Outoping Interfaces		
outgoing internace		
WAN	•	
WAN	•	

- ii. Set the **Outgoing Interface** to **WAN**.
- iii. Click **APPLY** to create the rule.

- 5. Click the **Add** (+) icon to create a new NAT rule for port forwarding the remote access server.
 - i. Set the **Mode** to **PAT** and select the appropriate protocol.
 - ii. Set the **Incoming Interface** to **WAN** and specify the port number of the remote service (in this case, 3389).
 - iii. Specify the **Destination IP** and **Destination Port** for the remote service.
 - iv. Click **APPLY** to create the rule.

One star la dans	1				
Create Index	I				
Status *					
Enabled	*				
Description	Server				
Access_	0011001		20 / 128		
Index *			207 120		
1					
1 - 512					
Mode					
PAT	•				
TCP			-		
MATLessheel		Double NAT			
NAT LOOPDACK					
Disabled Create Index 1	•	Disabled		 	
Create Index 1 Driginal Packet ncoming Interface WAN	(Conditi	Disabled		 	
Create Index 1 Driginal Packet ncoming Interface NAN Destination Port * 3389	(Conditi	Disabled		 	
Create Index 1 Disabled Create Index 1 Driginal Packet ncoming Interface NAN Destination Port * 3389 - 65535	(Conditi	Disabled		 	
Create Index 1 Create Index 1 Create Index 1 Driginal Packet ncoming Interface NAN Destination Port * 3389 1-65535 Translater	(Conditi	on)	ion)	 	
Create Index 1 Create Index 1 Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1- 65535 Translatec	(Conditi	on)	ion)		
Create Index 1 Create Index 1 Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1 - 65535 Translatec Destination IP *	(Conditi	on)	ion)		
Create Index 1 Disabled Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1-65535 Translatec Destination IP * 192.168.127.102	(Conditi	on)	ion)		
Create Index 1 Disabled Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1 - 65535 Translatec Destination IP * 192.168.127.102	(Conditi	on)	ion)		
Create Index 1 Disabled Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1 - 65535 Translatec Destination IP * 192.168.127.102 Destination Port * 3389	(Conditi	on)	ion)		
Create Index 1 Disabled Create Index 1 Driginal Packet ncoming Interface WAN Destination Port * 3389 1 - 65535 Translatec Destination IP * 192.168.127.102 Destination Port * 3389 1 - 65535	(Conditi	on)	ion)		

6. The created NAT rules will appear in the NAT rule table.

	R-G901	0-VPN-2MGS											Hi, admin	
Q Search for a function		Network	Addre	ess Translate										Í
Device Summary														
🜮: Setup Wizard		∎ I≣									Q Search			- 1
🔅 System	~		Status	Description	Index	Mada	Destand	Incoming	Src. IP:Port	Dst. IP:Port	Outgoing	Src. IP:Port	Dst. IP:Port	
Retwork Configuration	~		atatus	Description	muex	NIUGE	PIOLOCOI	Interface	(Original Packet)	(Original Packet)	Interface	(Translated Packet)	(Translated Packet)	
🖼 Redundancy	~	- <i>i</i>	Enabled	Remote_Access_Server	1	PAT	TCP	WAN	Any:Any	Dynamic:3389	Any	Any:Any	192.168.127.102:3389	
Network Service	~								192.168.127.1:Anv ~					
🛞 Routing	~	• •	Enabled	DMZ_WAN	2	N-to-1		Any	192.168.127.254:Any	Any:Any	WAN	Dynamic:Any	Any:Any	
→ NAT		Max. 512											1 - 2 of 2	
G Object Management		_												- 1
Firewall	~	APPLY												- 1
TE VIDA														

3.3 Expected Result

1. The image below shows users can remotely access the server in the DMZ from the Internet via the NAT PAT function. In this scenario, we accessed the NPort's web console in the LAN via the remote server in the DMZ.

No. 128.222.101 - Remote Deskto	p Connection			×
	NPort Web Console × +	-	- 0	×
← 〇 ▲ 不安全	192.168.10.253/home.htm?Submit=Submit&tok	en_text=&FakeChallenge=D446841EF959478026458AC81D 🖉 🗚 🏠 🕕 🏚 🧐	8	
MOXA	www.moxa.com	n		~
🔄 Main Menu	Welcome to NPort's web	console I		0
Overview				a
Basic Settings	Model Name	NPort 5110		-
Network Settings	MAC Address	00:90:E8:22:8A:A2		-18
🖲 🛄 Serial Settings	Serial No.	5961		
Operating Settings	Firmware Version	2.10 Build 21032913		G
Accessible IP Settings	System Uptime	0 days, 02h:30m:33s		_
Auto Warning Settings Monitor	NPort's web console provide the following fu	nction groups.		+
Change Password	Pacie Cottings			
Load Factory Default	Capies name, seal time cleak, time co	use ID address, and Web sensels. Telest sensels Eachis, Disable function		
G Save/Restart	berter name, rear and clock, and be	ter a deareas, and new console, remet console enable, plaque remetion.		
	Network Settings			
	IP address, netmask, default gateway,	static IP or dynamic IP, DNS, SNMP, IP location report.		
	Serial Settings			
	Baud rate, start bits, data bits, stop bi	ts, flow control, UART FIFO.		
	Operating Settings			
	Operation mode, TCP alive check, inac	tivity, delimiters, force transmit timeout.		
	Accessible IP Settings			
	"Accessible IP or Accessible IP group".	Disable to accept all IP's connection.		
	Auto Warning Settings			
	Auto warning E-Mail, SNMP Trap serve	r IP address.		-
	, in the server			α
	Monitor			~
	Line Arune Arune-Cetting			C

2. The firewall log shows devices in the DMZ can successfully connect to the Internet.

	DR-G901	0-VPN-2MGS	FP														Hi, adı	min 📔
		Event L	og															Å
Device Summary	Â	System	Log Firewall	Log	VPN I	.og	Settings ar	d Backup										-
System Network Configuration Redundancy	ž	c ı	7 🖸										Q, 338	:h 9				
Network Service	~	Index	Timestamp	Severity	Policy ID	Policy Name	Eth Tyj	e Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP ICMP Flags Type	ICMP Code	Action
Routing	×	3	2024/2/5 17:37:15+8:00	Warning	4	WAN_DMZ	204	8 TCP	WAN	00:30:88:80.de:fe	60.250.30.154	61137	DMZ	192.168.127.102	3389	PSH,ACK		Allow
A Object Management		28	2024/2/5 17:37:12+8:00	Warning	4	WAN_DMZ	204	8 TCP	WAN	00:30:88:80:de:fe	60.250.30.154	61137	DMZ	192.168.127.102	3389	PSH, -		Allow
Firewall	~	42	2024/2/5 17:37:9+8:00	Warning	4	WAN_DMZ	204	8 TCP	WAN	00:30:88:80:de:fe	60.250.30.154	61137	DMZ	192.168.127.102	3389	PSH, -		Allow
중 VPN	~	Max. 1000												erns per page: 50		r3 <	< :	> > I
Certificate Management	Ľ																	- 1
Disgnostics	,																	
System Status	~																	
Network Status	~																	
Event Logs and Notifications	^																	
Event Log	-1																	
Syslog																		
SNMP Trap/Inform																		
	DR.C001		:EP				-										Hi, adı	min :
	DR-G901	0-VPN-2MGS	FP														Hi, adı	min :
C Search for a function	DR-G901)	• •vpn-2MGs Event L	кр og														Hi, adı	min :
Control Contro Control Control Control Control Control Control Control Control Co	DR-G901)	• •-vpn-2MGS Event L System	FP Og Log Firewall	Log	VPNI	.0g	Settings ar	d Beckup									Hi, adı	min :
Search for a function Search for a function Device Summary Setup Wizard Source	DR-G901)	C-VPN-2MGS Event L System Laver 3-7	FP Og Log Firewall Policy -	Log	VPN	.09	Settings ar	d Beckup									Hi, adı	min :
Constant for a function Search for a function Oncose summary Oncose Summary Oncose Summary System Oncose Summary System Oncose Summary System Oncose Summary System Oncose Summary	DR-G9011	Event L System Layer 3-7	GG Log Firewall Policy -	Log	VPN	.09	Settings ar	d Backup					Sear	à			Hi, adı	min E
Constant for a function	DR-G901	Event L System Layer 3-7	FP Og Firewall Policy + F	Log	VPN I	.09	Settings ar	d Beckup					Seat Q. DMJ	:h Z_WAN			Hi, adı	nin E
C. Search for a function C. Search for a function C. Search for a function C. Search Witzard C. System C. Redundancy E. Network Configuration C. Redundancy E. Network Service	DR-G9011	Event L System Layer 3-7 C Index	FP OG Firewall Policy - F C Timestamp	Log	VPN I Policy ID	og	Settings ar Eth Tyj	d Backup zr IP e Protocol	Incoming	Source MAC	Source IP	Source Port	Seat Q. DMJ Outgoing Interface	h Z_WAN Destination IP	Destination Port	TCP ICMP Flags Type	Hi, add	Action
Second Control Contro	DR-G9011	CVPN-2MGS Event L System Layer 3-7 C Index 1	FP Og Log Firewall Policy - ¥ C Timestamp 2024/25 2024/25 1727:15+600	Log	VPN I Policy ID	og Policy Name DMZ,WAN	Settings ar Eth Tyj 204	d Backup zr IIP e Protocol 8 TCP	Incoming Interface DMZ	Source MAC 00:e0:00:60:96:6d	Source IP 192.168.127.102	Source Port : 32117	Q, DM2 Q, DM2 Outgoing Interface WAN	n Z_WAN Destination IP 10.168.1.23	Destination Port	TCP ICMP Flags Type SYN —	Hi, adı ICMP Code	nin :
MOXAL E	DR-G9011	CVPN-2MGS Event L System Layer 3-7 C Index 1 2		Log	VPN I Policy ID 3 3	-og Policy Name DMZ_WAN DMZ_WAN	Settings ar Eth Tyr 204 204	d Backup e Protocol 8 TCP 8 TCP	Incoming Interface DMZ DMZ	Source MAC 00:40100:60:96:6d 00:40100:60:96:6d	Source IP 192.168.127.102 192.168.127.102	Source Port : 32117 : 32116	Q DM: Q DM: Outgoing Interface WAN WAN	Destination IP 10.168.123	Destination Port 53 53	TCP ICMP Flags Type SYN – SYN –	Hi, add COMP Code 	Action Allow
Control Conference Control Conference Control Conference Confere	DR-G9011	C PPN-2MGS Event L System Layer 3-7 C I Index 1 2 4	FP Og Frewall Policy → F Timestamp 2024/2/5 2034/2/5 2	Log Severity Warning Warning Warning	VPN I Policy ID	Policy Name DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar Eth Tyr 204 204 204	d Backup e Protocol 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ	Source MAC 00 e0 00 50 96 6d 00 e0 00 50 96 6d 00 e0 00 50 96 6d	Source IP 192.168.127.102 192.168.127.102 192.168.127.102	Source Port 32117 32116 32099	Q DM3 Obtgoing Interface WAN WAN	n Z.WAN Destination IP 10.166.1.23 10.166.1.23 10.166.1.23	Destination Port 53 53 53	TCP ICMP Flags Type SYN – SYN – SYN –	Hi, add	nin ; Action Allow Allow
MOXAC E Asarch for a function Asarch for a function Overs Samme borks Samme borks Samme borks Samme borks Samme borks Samme borks b	DR-69011	CVPN-2MGS Event L System Layer 3-7 C index 1 2 4 5	FP Og Filewall Solution Filewall Filewa	Log Severity Warning Warning Warning	VPN U Policy ID 3 3 3 3	Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar Eth Tyr 204 204 204 204 204 204 204 204 204 204	d Backup rf IP Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ	Source MAC 00 x0 00 60 96 64 00 x0 00 60 96 64	Source (P 192, 168, 127, 102 192, 168, 127, 102 192, 168, 127, 102 192, 168, 127, 103	Source Port : 32117 : 32216 : 32209 : 32209	Controlling Outpoing Interface WAN WAN WAN WAN	Destination IP 10.168.123 10.168.123 10.168.123	Destination Port 53 53 53 53	TCP ICMP Flags Type SYN SYN SYN SYN	HL, add ICMP Code 	Action Allow Allow
Control of the section	DR-6901	CVPN-2MGS Event L System Layer 3-7 C Index 1 2 4 5 6	P P P Cog Premail Policy - P	Log Severity Warning W	VPN D Policy 3 3 3 3 3	Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar Eth Jy 20- 20- 20- 20- 20- 20- 20- 20- 20- 20-	d Beckup e Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ DMZ	Source MAC 00 x00 00 00 96 6d 00 x00 00 59 6d 00 x00 00 59 6d 00 x00 00 59 6d 00 x00 00 59 6d	Source IP 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102	Source Port 32117 32116 32099 32099	Cotgoing Interface WAN WAN WAN WAN	n 	Destination Port 53 53 53 53 53 53	TCP ICMP Flags Type SYN - SYN - SYN - SYN - SYN - SYN -	Hi, add ComP Code 	Action Allow Allow
Constraints of the second	DR-6901	CVPN-2MGS Event L System Layer 3-7 C Index I C G G G G G G G G G G G G G G G G G G	P P Cost	Log Severity Warning Warning Warning Warning	VPN I Policy 10 3 3 3 3 3 3	Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar Ethi 2044 204 204 204 204 204 204 204 204 20	d Backup T IP Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ DMZ DMZ	Source MAC 00/e000 600 96/d	Source IP 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102	Source Port : 32117 : 32116 : 32099 : 32098 : 32115	Control of the second s	Destination IP 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23	Destination Port 53 53 53 53 53 53	TCP ICMP Flags Type SYN SYN SYN SYN SYN	Hi, add Code 	nin E
MOXX E Generation of a function Generation of a function Generation G	DR-6901	CVPN-2MGS	P P Compared C	Log Severity Warning W	VPN L Policy 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	og Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Etitings ar Filings 204 204 204 204 204 204 204 204	r IP Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ DMZ DMZ DMZ DMZ	500mm MAC 00 e0 00 60 %6 dd 00 e0 00 60 %6 dd	Source IP 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102	Source Port 32117 32116 32099 32098 32115 32114	Search DMJ DMJ Outpoing WAN WAN WAN WAN WAN	Destination IP 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23	Destination Port 53 53 53 53 53 53	TCP ICMP Flags Type SYN – SYN – SYN – SYN – SYN – SYN – SYN –	HL, add ComP Code 	nin :
Constraints	DR. G901	CVPN-2MGS EVent L System Layer 3-7 C index 1 2 4 5 6 7 8	FP og Trendel log Freedel Policy - r T Trenstamp 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201 2024/201	Log Severity Varning Warning Warning Warning Warning Warning Warning Warning Warning Warning Harmon Kara Kara Kara Kara Kara Kara Kara Kar	VPN I Policy 3 3 3 3 3 3 3 3 3 3 3 3	og Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar 5 5 5 5 5 5 5 5 5 5 5 5 5	rr IP Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2	Bourse MAC 00 e00 05 00 46 44 00 e00 05 00 46 44	Source (P) 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102	Bource Port 32117 32219 32099 32099 32099 32115 32114 32113	Outgoing Outgoing WAN WAN WAN WAN WAN WAN WAN	Destination (P 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23 10.166.1.23	Destination 53 53 53 53 53 53 53 53 53 53 53 53 53	TCP ICMP Flags Type SYN – SYN – SYN – SYN – SYN – SYN – SYN – SYN –	HL, add SCMP Code 	nin :
Constraints Constrain	DR. G901	CVPN-2MGS Event L System Layer 3-7 C index 1 2 4 5 6 7 8 9	Trend Og Value Policy - Tenetary Value Valu	Log Severity Severity Warning	VPN L Policy 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Policy Name DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN DMZ_WAN	Settings ar FtH 20- 20- 20- 20- 20- 20- 20- 20- 20- 20-	er IP Constant Protocol 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ	Source MAC 00x000009640 00x00009640 00x00009640 00x00009644 00x000096944	Source (P) 192-168.127.102 192-168.127.102 192-168.127.102 192-168.127.102 192-168.127.102 192-168.127.102 192-168.127.102	Source Port 322117 32209 32209 32215 322114 322115 322114 322114 322115 322114 322114 322114 322114 322114	Outpoing Meteriace WAN WAN WAN WAN WAN WAN WAN	Destination IP Destination IP 10 168.1.23 10 168.1.23	Destination 53	TCP ICMP Flags Type SYN -	Hi, add Code 	nin i i i i i i i i i i i i i i i i i i
MOXCK EF Constantiation	DR-6901	CVPN-2MGS Event L System Layer 3-7 C Index 1 2 4 5 6 7 8 9 10	Trend Og Frend Value Frend Policy - Temestamy - Value	Severity Waming Waming Waming Waming Waming Waming Waming Waming Waming	VPN L Policy 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Policy Name DM2, WAH DM2, WAH	Ettings an Ettings an 204 204 204 204 204 204 204 204	27 Protocol 8 TCP 8 TCP	Incoming Interface DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ	Bource MAC OD 40 00 50 96 44 OD 40 00 50 96 44	Source IP 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102 192-168-127-102	Bource 32217 32216 32009 32098 32114 32113 32114 32112 32112	Control Contro	2.WAN Destination (P 10.168.1.23 10.168.1	Destination 53	TCP ICMP FRigit Type	HL, add ComP Code 	Action Action Allow
Control Configuration Control Configuration Configura	DR-6901	4 5 5 5 5 5 5 5 5 5 5 5 5 5	Trend 100 Frend Policy - 7 To 1123715400 - 2024278 - 1123715400 - 2024278 - 1123715400 - 2024278 - 1123715400 - 2024278 - 1123715400 - 2024278	Log Severity Warning W	Policy 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Policy Name Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA Du2_WAA	Settings ar Fifty 200- 204- 204- 204- 204- 204- 204- 204-	r IP Protocol 8 TCP 8 TCP	Incerning Interface DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ DMZ	Bource MAC 00 x0 00 00 96 96 60 00 x0 00 00 96 96 60	Source IP 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102 192.168.127.102	Boarce 32117 32116 32099 32116 32098 32114 32115 32114 32115 32115 32114 32115 32115 32114 32115 32115 32115	Control Contro	2	Destination 53 54 55 55 55 55 56 57 58 59 50 51 52 53 54 55 56 <tr< th=""><th>TCP ICMPP FR49 TSP STN - STN -</th><th>HL, add CodPe CodPe </th><th>Action Action Alare Alare Alare Alare Alare Alare Alare Alare Alare Alare</th></tr<>	TCP ICMPP FR49 TSP STN - STN -	HL, add CodPe CodPe 	Action Action Alare Alare Alare Alare Alare Alare Alare Alare Alare Alare
Banch for a function General for a function General for a function General for a function General for a function for the function	DR-G901	 Coverve 27M05 Coverve	Tenedation Via Frendation Policy - Tenestame - Tenestame - Via 2724-263	Log Severity Waning Waning Waning Waning Waning Waning Waning Waning	VPN II Policy 3	Раку Кален Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман Под. Уман	Settings ar Fift 200- 204 204 204 204 204 204 204 204 204 204	r IP (Protocol 8 TCP 8	Incenting DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2 DM2	Board MAC 00 re20 05 09 64 00 re20 05 09 64	Bource IP 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102 192-106-127.102	Boarce Perf 32117 32100 32000 32000 32000 32010 32010 32011 32012 32010 32011 32011 32011 320110 320100	Control of the second s	2 Destination IP 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23 10.168.1.23	Destination Port 53 54 55 53 54 55 56 57 58 59 53 54 55 56 57 58 59 <	TCP ICANP PR081 TYP SYN -	HL, add Cocke Coche Coche Coche Coche Coche Coche Coche Coch	Action Ac

3. Devices in the DMZ can establish a TCP connection with devices in the LAN.

	DR-G901	0-VPN-2MGS	FP														Hi, ad	min	
		Event Lo	og																Â
Device Summary	Î	System I	.og Firewa	II Log	VPN L	.og Setti	ngs and E	lackup											
Setup Wizard	~	Layer 3-7	Policy -																
Retwork Configuration	×	c 🛾											Q LAI	ch N					I
Tri Hedundancy	ž	Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP ICMP Flags Type	ICMP Code	Action	
Routing	~	18	2024/2/5 17:37:13+8:00	Warning	1	DMZ_LAN	2048	тср	DMZ	00:e0:00:60:96:6d	192.168.127.102	32105	LAN	192.168.10.253	80	SYN	-	Allow	1
Object Management		19	2024/2/5 17:37:13+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	32104	LAN	192.168.10.253	80	SYN	-	Allow	
Firewall	~	33	2024/2/5 17:37:11+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	32097	LAN	192.168.10.253	80	SYN	-	Allow	J
😵 VPN	ž	36	2024/2/5 17:37:11+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	32094	LAN	192.168.10.253	80	SYN	-	Allow	1
a Security	~	Max. 1000												terro per page: 50		r4 <	<	> >	I
System Status	Ŷ																		
Network Status	~																		
Event Logs and Notifications	^																		
Event Notifications																			
Syslog SNMP Trap/Inform		4																	

Copyright © 2024 Moxa Inc.

4. LAN devices cannot communicate with the WAN interface.

```
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Copyright © 2024 Moxa Inc.

4 Reference Scenario 2: Isolated LAN With Limited Internet Access

4.1 Architecture

The user wants to access a field site from the Internet, while also protecting production equipment in the LAN from exposure to external networks. However, the PCs in the LAN must still be able to access the Internet. Here, the user wants to isolate all direct communication from WAN to LAN, but allow the LAN to access the Internet. This requires an independent network zone allowing data exchanges between the LAN and the Internet alongside a user-defined security policy to only allow the LAN to send information to this zone. Additionally, only user-specified IP addresses may access this network zone.



Reference Diagram

Key Actions:

- Configure 3 network interfaces: WAN, LAN, and DMZ. Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
- 2. Configure the Layer 3 firewall filter.
- 3. Create the allowlist policies.
- 4. Set up a DMZ to exchange data between the LAN and WAN interfaces.
- 5. Set up PAT and NAT for DMZ communications.
- 6. Create NAT N-1 rules for devices in the LAN and DMZ to access the Internet.

4.2 Scenario 2 Configuration Guide

In this scenario, the user aims to access data sent by the NPort while ensuring the LAN remains protected from direct external connections coming from the WAN or DMZ. However, the NPort is configured to send email notifications to an external server on the Internet.

To fulfill these requirements, the user will establish a connection to a remote access server (PC-2) within the DMZ which is receiving data from the NPort. From PC-2, the user can monitor the data transmitted by the NPort while ensuring the security of the LAN environment. Additionally, the NPort will send email notifications to PC-1 over the Internet.

WAN NPort Series LAN ss: 192 168 10 253 IP Addre **Email Notifications** 220.128.222.101 Port 8 WAN TCP Connection Port 3 LAN A PC-1 (User) DMZ Port 2 Remote Access LAN B (Port 3389) PC-2 (Remote Access Server) IP Address: 192.168.127.102 Ethernet Data Flow

Refer to the network topology for this scenario below:



Communication Principles:

1. The DMZ is configured to allow bidirectional communication with the WAN.



2. The LAN is allowed to communicate with the DMZ but blocks all incoming connections from the DMZ.



3. The LAN can access the Internet, but the WAN cannot communicate with the LAN.



Setup Instructions:

- 1. In the Secure Router's web interface, navigate to **Firewall > Layer 3-7 Policy**.
- In the Global Policy Settings section, set the Default Action to Deny All. This will block all communications except for user-specified IP addresses to access the DMZ.

tatus		Default Action	
nabled	~	Deny All	*
Global Policy E	Event Set	tings	
Global Policy E	Event Set	tings	
Slobal Policy E	Event Set	tings	
Nobal Policy E	Event Set	tings	

- 3. Click the **Add** (+) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
 - WAN-to-DMZ
 - DMZ-to-WAN
 - LAN-to-DMZ
 - LAN-to-WAN

The firewall rules are subject to the network environment. Refer to the overview below as a reference for how to configure the firewall rule parameters.

Arid		Index	Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action
	1	1	Enabled	WAN-DMZ	Disabled/Warning	WAN	DMZ	IP and Port Filtering	Any	Any	Any	Any	Allow
	1	2	Enabled	DMZ-WAN	Disabled/Warning	DMZ	WAN	IP and Port Filtering	Any	Any	Any	Any	Allow
	1	3	Enabled	LAN-DMZ	Disabled/Warning	LAN	DMZ	IP and Port Filtering	Any	Any	Any	Any	Allow
	1	4	Enabled	LAN-WAN-only	Disabled/Warning	LAN	WAN	IP and Port Filtering	Any	Any	Any	Any	Allow

NOTE If you want to monitor the Layer 3-7 firewall events, enable the **Global Policy Event Settings** option.

Global Po Status Enabled	olicy Sett	ings - Defi	ault Action ny All	*	
Enabled		*]		
	Index	Status	Name	Eve	ent
	1	Enabled	DMZ-WAN	En	abled/Warning
• /	2	Enabled	LAN-DMZ	En	abled/Warning

- 4. Navigate to **NAT Settings** and click the **Add** (+) icon to create a new NAT rule for the LAN interface to access the Internet.
 - i. Set the **Mode** to **N-to-1**.
 - ii. Specify the **Source IP Start** and **End** to determine the LAN IP address range that can access the Internet.
 - iii. Set the **Outgoing Interface** to **WAN**.
 - iv. Click **APPLY** to create the rule.
- 5. Click the **Add** (+) icon to create another new NAT rule for the WAN to access the remote desktop service in the DMZ.
 - i. Set the **Mode** to **PAT** and select the appropriate protocol.
 - ii. Set the **Incoming Interface** to **WAN** and specify the port number of the remote service (in this case, 3389).
 - iii. Specify the **Destination IP** and **Destination Port** for the remote service.
 - iv. Click **APPLY** to create the rule.
- 6. Click the **Add** (+) icon to create another new NAT rule for the DMZ to access the Internet.
 - i. Set the **Mode** to **N-to-1**.
 - ii. Specify the **Source IP Start** and **End** to determine the DMZ IP address range that can access the Internet.
 - iii. Set the **Outgoing Interface** to **WAN**.
 - iv. Click **APPLY** to create the rule.

7. The created NAT rules will appear in the NAT rule table.

)R-G90	10-VF	PN-2M	IGSFI											Hi, admin 📔 🗄
Q Search for a function		Ne	two	ork /	Addre	ss Translate									*
😰 Device Summary			Ð	13									Q Search		
🔅 System	* *				Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Redundancy	~			1	Enabled	Remote_Access_Server	1	PAT	TCP	WAN	Any:Any	Dynamic:3389	Ary	Any:Any	192.168.127.102:3389
E Network Service	× ×			/	Enabled	DMZ_WAN	2	N-to-1		Any	192.168.127.1:Any ~ 192.168.127.254:Any	Any:Any	WAN	Dynamic:Any	Any:Any
→ NAT Æ Object Management				/	Enabled	LAN_WAN	3	N-10-1		Any	192.168.10.1:Any ~ 192.168.10.254:Any	Any:Any	WAN	Dynamic:Any	Any:Any
Firewall	~		Max. 51	2											1 - 3 of 3
다 VPN 같 Certificate Management	* *		APPLY												

4.3 Expected Result

1. The image below shows users can remotely access the server in the DMZ from the Internet via the NAT PAT function. In this scenario, we accessed the remote server in the DMZ and received data from the NPort in the LAN.

The rest of the rest of connection		
Comm Terminal Emulator - IPv4 TCP Server (192.168.10.253:5010)(10	cal:4001) Dumb Terminal	
Profile Edit Port Manager Window Help		
🕞 IPv4 TCP Server (192.168.10.253:5010)(local:4001) Dumb Terminal		
Time: 15:16:43, Temperature: 28.75 C	^	
Time: 15:16:53, Temperature: 26.0 C		
Time: 15:17:03, Temperature: 15:07 C		
Time: 15:17:22 Temperature: 15:21 C		
Time: 15:17:33 Temperature: 23 34 C		
Time: 15:17:43. Temperature: 18.1 C		
Time: 15:17:53, Temperature: 22.24 C		
Time: 15:18:03, Temperature: 24.94 C		
Time: 15:18:13, Temperature: 19.17 C		
Time: 15:18:23, Temperature: 20.83 C		
Time: 15:18:33, Temperature: 18.92 C		
Time: 15:18:43, Temperature: 20.68 C		
Time: 15:18:53, Temperature: 29.98 C		
Time: 15:19:03, Temperature: 18.81 C		
Time: 15:19:13, Temperature: 18.33 C		
Time: 15:19:23, Temperature: 27.06 C		
Time: 15:19:33, Temperature: 23.96 C		
Time: 15:19:43, Temperature: 28.27 C		
Time: 15:19:53, Temperature: 28.54 C		
lime: 18:20:03, lemperature: 18:2 C		
	~	
<	>	
Status: Connect Ready	TX:0 RX:19245	
		J

2. The firewall log shows devices in the LAN and DMZ can successfully connect to the Internet. Additionally, devices in the LAN can communicate with devices in the DMZ.

WAN-to-DMZ

	DR-G9010	-VPN-2MGSFI	P														Hi, admir	:	
Q Search for a function	_	Event L	og																^
Device Summary	^	System	Log Firewall	Log	VPN L	og Set	ings and E	ackup											
🔅 Setup Wizard																		_	
🔅 System	~	Layer 3-7	Policy +																
Retwork Configuration	č	c ı	i 🖸										Q WAN	h I_DMZ					
E Network Service	~	Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP ICMP Flags Type	ICMP Code	Action	
Routing	ř	2	2024/2/6 15:37:6+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	95.214.55.253	58154	DMZ	192.168.127.102	3389	SYN, ECE, CWR	-	Allow	
Object Management		3	2024/2/6 15:37:5+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	34144	DMZ	192.168.127.102	3389	rst, - ack	-	Allow	
Firewall	~	4	2024/2/6 15:37:5+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	41487	DMZ	192.168.127.102	3389	SYN, ECE, CWR	-	Allow	
다. Contificante Management	ž	5	2024/2/6 15:37:4+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	95.214.55.253	57096	DMZ	192.168.127.102	3389	ACK		Allow	
Security		7	2024/2/6 15:37:2+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	26980	DMZ	192.168.127.102	3389	RST,		Allow	
Diagnostics	^	8	2024/2/6 15:37:2+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	34144	DMZ	192.168.127.102	3389	ECE, CWR	-	Allow	
System Status	~	9	2024/2/6 15:37:2+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	95.214.55.253	57096	DMZ	192.168.127.102	3389	ECE, CWR	-	Allow	
Network Status Event Logs and Notifications	×	12	2024/2/6 15:37:0+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	95.214.55.253	60613	DMZ	192.168.127.102	3389	RST,	-	Allow	
Event Log	- 1	13	2024/2/6 15:36:59+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	26980	DMZ	192.168.127.102	3389	ECE, CWR	-	Allow	
Event Notifications		14	2024/2/6 15:36:59+8:00	Warning	3	WAN_DMZ	2048	TCP	WAN	00:30:88:80:de:fe	185.16.38.15	19339	DMZ	192.168.127.102	3389	RST, ACK		Allow	
Syslog SNMP Trap/Inform	Ţ	17	2024/2/6 15:36:57+8:00	Warning	3	WAN_DMZ	2048	ТСР	WAN	00:30:88:80:de:fe	95.214.55.253	60613	DMZ	192.168.127.102	3389	ECE, CWR evin	-	Allow	÷

LAN-to-WAN

	G9010	-VPN-2MGSFF															Hi, admi	n I
Q Search for a function		Event Lo	og															Â
Device Summary	^	System I	.og Firewall	Log	VPN L	.og s	ettings and	Backup										
🕬 Setup Wizard																		
🔅 System	·	Layer 3-7	Policy -															- 1
Network Configuration	·	c i											Q I AN	th WAN				- 1
Redundancy	۲		-															
Network Service	۲ II	Index	Timestamp	Severity	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming	Source MAC	Source IP	Port	Outgoing	Destination IP	Port	TCP ICMP Flags Type	Code	Action
Routing •	۲ I	202	2024/2/6 15:35:11+8:00	Warning	4	LAN_WAN	2048	TCP	LAN	00:90:e8:65:c3:4f	192.168.10.253	1038	WAN	74.125.203.109	25	ACK		Allow
€ NAT		209	2024/2/6 15:35:8+8:00	Warning	4	LAN_WAN	2048	TCP	LAN	00:90:e8:65:c3:4f	192.168.10.253	1038	WAN	74.125.203.109	25	SYN		Allow
Coject Management		250	2024/2/6	Warning	4	I AN WAN	2048	TOP	LAN	00.90 e8:65 c3:4f	192 168 10 253	1037	WAN	74 125 203 109	25	4CK		Allow
Firewall Y	Ĭ	237	15:34:41+8:00	warning	*	CONCININ	2040	TOP	Lon	00.90.00.037.0.41	192.100.10.200	1007	100	74.123.203.109	2.5	Avn		2000
B Certificate Mananement		264	15:34:38+8:00	Warning	4	LAN_WAN	2048	TCP	LAN	00:90:e8:65:c3:4f	192.168.10.253	1037	WAN	74.125.203.109	25	SYN		Allow
🖧 Security		265	2024/2/6 15:34:38+8:00	Warning	4	LAN_WAN	2048	TCP	LAN	00:90:e8:65:c3:4f	192.168.10.253	1036	WAN	74.125.203.109	25	ACK		Allow
Diagnostics	~	268	2024/2/6 15:34:34+8:00	Warning	4	LAN_WAN	2048	TCP	LAN	00:90:e8:65:c3:4f	192.168.10.253	1036	WAN	74.125.203.109	25	SYN	-	Allow
System Status	-													terrar per pager 50	- 1-67	00 LZ	,	
Network Status	-	Max. 1000																·
Event Logs and Notifications	`																	-
Event Log																		
Event Notifications																		
Syslog																		
SNMP Trap/Inform	-	4																• •

3. The firewall policy is blocking devices in the DMZ to ping and communicate with devices in the LAN.



4. The device in the LAN is sending mail notifications to the user via the Internet.

□ ☆ ▷ 我	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 12:04:29	下午12:04
□ ☆ ▷ 我	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:59:16	上午11:59
	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:58:5	上午11:59
□ ☆ ▷ 我	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:50:0	上午11:50
	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:49:4	上午11:49
□ ☆ ▷ 我	NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:42:4	上午11:42

NP6150 alert (S/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06, 03:58:58) admin: Authentication failed 192.168.127.102:39482 \times

 NP6150 alert (\$/N:7838, 192.168.10.253, 00:90:E8:65:C3:4F): (2024-02-06,
 ▷
 ▷

 12:04:29) Port 1 DSR changed (0 -> 1)
 ▷
 IM#E ×

Moxa Tech Note How to Build an Industrial DMZ to Protect Internal LAN Networks

With Moxa Secure Routers

5 Reference Scenario 3: LAN Fully Isolated From the Internet, With Modbus Communications

5.1 Architecture

In this scenario, the user is running a factory network that uses the Modbus protocol to communicate with Modbus field devices. The user wants to access the field site from the Internet, but they have some security concerns. The user wants to protect the Modbus devices in the LAN which includes much of the sensitive production line equipment.

To achieve this, direct communication from WAN to LAN is blocked. As a result, an independent network zone is required to allow the Modbus master in the zone to call specific Modbus read functions to poll data from Modbus Slave devices in the LAN. Additionally, the isolated zone will only share this data with specific IPs.





Key Actions:

- Configure 3 network interfaces: WAN, LAN, and DMZ. Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
- 2. Configure the Layer 3 Firewall filter.
- 3. Create the allowlist policies.
- 4. Set up a DMZ to exchange Modbus data between the LAN and WAN interfaces.
- 5. Set up NAT and PAT policies for the DMZ.
- 6. Configure the Modbus policy in the advanced firewall protection settings.

5.2 Scenario 3 Configuration Guide

In the provided network topology, the user aims to retrieve I/O data from the ioLogik device within the LAN using the Modbus TCP protocol. To enhance security and prevent unauthorized access from external networks, a DMZ has been created to isolate the LAN and WAN segments.

To interact with Modbus devices in the LAN, the user will connect to a remote access server (PC1) situated within the DMZ. Through remote access capabilities, the user can securely monitor the I/O data from an external network while safeguarding the integrity of the LAN environment.

Refer to the network topology for this scenario below:



Network Topology

Communication Principles:

1. The DMZ is configured to allow bidirectional communication with the WAN.



2. Only allow Modbus TCP read-only communications between the DMZ and the LAN.



3. The LAN is not allowed to communicate with the WAN.



Copyright $\ensuremath{\mathbb{C}}$ 2024 Moxa Inc.

Setup Instructions:

- 1. In the Secure Router's web interface, navigate to **Object Management**.
- 2. Click the **Add** (+) icon to create a new Modbus object. This object is necessary for restricting traffic between the DMZ and LAN to Modbus traffic only.
 - i. Select Industrial Application Service as the type.
 - ii. Check Modbus (TCP 502, UDP 502).

Nami	5 M	
Mod	lbus	- 1
	6 / 32	
Objec	t Type *	
Indu	Istrial Application Service +	
Selec	t Industrial Application Service(s)	
~	Modbus (TCP 502; UDP 502)	
	DNP3 (TCP 20000)	
	IEC-60870-5-104 (TCP 2404)	
	IEC-61850-MMS (TCP 102)	
	OPC-DA (TCP 135)	
	OPC-UA (TCP 4840; UDP 4840)	
	CID Feb asNet/ID (TOD 44010-UDD 2022)	

- iii. Click **CREATE**.
- 3. Navigate to **Firewall > Layer 3-7 Policy**.
- 4. In the **Global Policy Settings** section, set the Default Action to **Deny All**. This will block all communications except for user-specified IP addresses to access the DMZ.

tatus		Default Action	
abled	*	Deny All	*
lobal Policy	Event Set	tinas	
Global Policy	Event Set	tings	
og	Event Set	tings	

- 5. Click the **Add** (+) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
 - WAN-to-DMZ
 - DMZ-to-WAN
 - DMZ-to-LAN: Uses the Modbus object created in step 2 as the Destination Port.
 - LAN-to-DMZ: Uses the Modbus object created in step 2 as the Source Port.

The firewall rules are subject to the network environment. Refer to the overview below as a reference for how to configure the firewall rule parameters.

Status	Name	Event	Incoming Interface	Outgoing Interface	Filter Mode	Source Address	Source Port	Destination Address	Destination Port or Protocol	Action
Enabled	WAN-DMZ	Enabled/Warning	WAN	DMZ	IP and Port Filtering	Any	Any	Алу	Any	Allow
Enabled	DMZ-WAN	Enabled/Warning	DMZ	WAN	IP and Port Filtering	Any	Any	Any	Any	Allow
Enabled	DMZ-LAN	Enabled/Warning	DMZ	LAN	IP and Port Filtering	Any	Any	Any	Modbus	Allow
Enabled	LAN-DMZ	Enabled/Warning	LAN	DMZ	IP and Port Filtering	Any	Modbus	Any	Any	Allow

NOTE If you want to monitor the Layer 3-7 firewall events, enable the **Global Policy Event Settings** options.

Global Pe Status Enabled	olicy Sett	ings Tefa	ult Action ny All	<u> </u>
Global Pe Log Enabled	olicy Ever	•		
	Index	Status	Name	Event
•	1	Enabled	DMZ-WAN	Enabled/Warning
• •	2	Enabled	LAN-DMZ	Enabled/Warning

- 6. Navigate to **Firewall > Advanced Protection > Configuration > Global Settings**.
- 7. In the Enforcement section, set **Enforcement** to **Enable** to enable advanced protection.

8. Enable **Modbus/TCP Firewall** and specify the Modbus TCP service's port number. The default port is 502.

IPS * Disabled	*	IPS Operation Mode * Prevention Mode	*	
Enforcement				
Enforcement * Enabled	Ŧ	Action * Reset	*	
Modbus/TCP Firewall *		Modbus/TCP ADP *	(Modbus/TCP Service Port *
Enabled	*	Enabled	_	502
				1 - 65535, allow comma(,)
DNP3 Firewall *		DNP3 ADP *		DNP3 Service Port *
Enabled	*	Enabled	*	20000
IEC 104 Eironall 8		IEC 104 ADD 1		1 - 65535, allow comma(,)
Enabled	*	Enabled	*	2404
				1 - 65535 allow comma()
MMS Firewall *				MMS Service Port *
Enabled	*			102
				1 - 65535, allow comma(,)
-				
I roubleshooting				
Disabled	-			

- 9. Navigate to Firewall > Advanced Protection > Configuration > Protocol Filter Object.
- 10. Click the **Add** (+) icon to create a new Modbus TCP protocol filter object.
 - i. Select **Modbus/TCP** as the Category and set the Protocol Filter Profile to **Read Only**.

Name *			
Read_Only			
	9/64		
Category *			
Modbus/TCP	-		
Slave ID			
1			
0 - 255 or 0x00 - 0xFF			
Protocol Filter Profile *			
Read Only	-		
Function Code *			
1, 2, 3, 4, 7, 20, 24	-		
		CANCEL	CREATE

- ii. Click **CREATE** to create the object.
- 11. Navigate to Firewall > Advanced Protection > Protocol Filter Policy.

- 12. Click the **Add** (+) icon to create a new protocol filter policy for the Modbus Master in the DMZ to interact with Modbus Slave devices in the LAN.
 - i. Select **DMZ** as the **From Interface** and **LAN** as the **To Interface** and specify the corresponding IP addresses.
 - ii. Set the **Command Type** to **Master Query**. Since the Modbus Master is within the DMZ, the Master Query should be allowed to pass through the firewall between the DMZ and the LAN.
 - iii. Select the Modbus object created in step 10 as the Application Protocol.
 - iv. Select Accept as the Action.
 - v. Click **APPLY** to create the rule.

Index * 1 1-200 Policy Name * Read_Query 10 / 64 Status * Enabled • From Interface * DMZ • Source IP * Single • Single • 192.168.1 Protocol * Application Protocol *	27.102	•		
Index * 1 1 1 1 1 1 1 1 1 1 1 1 2 Policy Name * Read_Query 10 / 64 Status * Enabled • From Interface * DMZ • Io Interface * DMZ • Single • Single • 192.168.1 Protocol * TCP • Command Type * Master Query • Application Protocol *	27.102	*		
1 1-200 Policy Name * Read_Query 10 / 64 Status * Enabled * From Interface * DMZ * Source IP * Single * 192.168.1 Protocol * TCP * Command Type * Master Query * Application Protocol *	27.102	•		
1 - 200 Policy Name * Read_Query 10 / 64 Status * Enabled • From Interface * DMZ • LAN Source IP * Single • I92.168.1 Destination IP * Single • Protocol * TCP • Command Type * Master Query • Application Protocol *	27.102	•		
Policy Name * Read_Query 10 / 64 Status * Enabled • From Interface * DMZ • LAN Source IP * Single • 192.168.1 Protocol * TCP • Command Type * Master Query • Application Protocol *	27.102	*		
Read_Query 10 / 64 Status * Enabled • From Interface * LAN DMZ • Source IP * From * Single • Protocol * From * TCP • Command Type * Master Query Application Protocol * •	27.102	*		
10 / 64 Status * Enabled From Interface * DMZ Source IP * Single Destination IP * Single Protocol * TCP Command Type * Application Protocol *	27.102	*		
Status * Enabled From Interface * DMZ From * Single Prom * Single Protocol * TCP Command Type * Master Query Application Protocol *	27.102	•		
Enabled - From Interface * DMZ - Source IP * Single - Prom * 192.168.1 Prom * 192.168.1 Prom * 192.168.1 Prom * 192.168.1 Prom * Command Type * Master Query - Application Protocol *	27.102	•		
From Interface * To Interface DMZ - LAN Source IP * From * 192.168.1 Destination IP * From * Single - 192.168.1 Protocol * TCP - Command Type * Master Query - Application Protocol *	27.102	*		
Profit interface DMZ - LAN Source IP * From * Single - 192.168.1 Destination IP * From * Single - 192.168.1 Protocol * TCP - Command Type * Master Query - Application Protocol *	27.102 0.250	•		
Source IP * From * Source IP * From * Single • 192.168.1 Protocol * TCP Command Type * Master Query Application Protocol *	27.102 0.250			
Source IP * From * 192.168.1 Destination IP * From * 192.168.1 Protocol * TCP Command Type * Master Query Application Protocol *	27.102 0.250			
Single - 192.168.1 Destination IP * From * 192.168.1 Single - 192.168.1 Protocol * - - Command Type * - - Application Protocol * - -	27.102 0.250			
Destination IP * From * 192.168.1 Protocol * TCP Command Type * Master Query Application Protocol *	0.250			
Destination (P * From * 192.168.1 Protocol * TCP Command Type * Master Query Application Protocol *	0.250			
Protocol * TCP ~ Command Type * Master Query ~ Application Protocol *	0.250			
Protocol * TCP - Command Type * Master Query - Application Protocol *				
Command Type * Master Query - Application Protocol *				
Command Type * Master Query ~ Application Protocol *				
Application Protocol *				
Application Protocol *				
Read_Only +				
Action *				
Accept -				

- 13. Click the **Add** (+) icon to create a new protocol filter policy for the Modbus Slave devices in the LAN to interact with the Modbus Master in the DMZ.
 - i. Select **LAN** as the **From Interface** and **DMZ** as the **To Interface** and specify the corresponding IP addresses.
 - ii. Set the **Command Type** to **Slave Response**.
 - iii. Select the Modbus object created in step 10 as the Application Protocol.
 - iv. Select **Accept** as the Action.

With Moxa Secure Routers

- Add Policy Index * 2 1 - 200 Policy Name Read_Slave 10/64 Enabled om Interface To Interface * LAN DMZ Single -192.168.10.250 192.168.127.102 Single ТСР nd Type * Slave Response Read_Only Accept CANCEL APPLY
- v. Click **APPLY** to create the rule.

Both rules will appear in the protocol filter policy table.

	Index	Policy Name	Status	Protocol Filter Object	col Filter Object From Interface		To Interface Source IP		Protocol	Command Type	Application Protocol	Action
. 🗉 🖊	5	Master	Enabled	Modbus	DMZ	LAN	Any	Any	TCP	Master Query	Modbus/TCP	Accept
	6	Slave	Enabled	Modbus	LAN	DMZ	Any	Any	TCP	Slave Response	Modbus/TCP	Accept

- 14. Navigate to **NAT Settings** and click the **Add** (+) icon to create a new NAT rule for the DMZ to access the Internet.
 - i. Set the **Mode** to **N-to-1**.
 - ii. Specify the **Source IP Start** and **End** to determine the DMZ IP address range that can access the Internet.
 - iii. Set the **Outgoing Interface** to **WAN**.
 - iv. Click **APPLY** to create the rule.
- 15. Click the **Add** (+) icon to create another new NAT rule for the WAN to access specific services in the DMZ.
 - i. Set the **Mode** to **PAT** and select the appropriate protocol.
 - ii. Set the **Incoming Interface** to **WAN** and enter the port number of the remote service (in this case, 3389).
 - iii. Specify the **Destination IP** and **Destination Port** for the remote service.
 - iv. Click **APPLY** to create the rule.

Moxa Tech Note How to Build an Industrial DMZ to Protect Internal LAN Networks

With Moxa Secure Routers

16. The created NAT rules will appear in the NAT rule table.

	G901	0-VPN-2	MGSFI											Hi, admir	ו ו
Q Search for a function		Netw	ork /	Addre	ss Translate										Î
Device Summary Setup Wizard	Ľ	٥	1Ξ									Q Search			
System System				Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)	
Redundancy	-		1	Enabled	Remote_Access_Server	1	PAT	TCP	WAN	Any:Any	Dynamic:3389	Any	Any:Any	192.168.127.102:3389	
E Network Service			/	Enabled	DMZ_WAN	2	N-to-1		Any	192.168.127.1:Any ~ 192.168.127.254:Any	Any:Any	WAN	Dynamic:Any	Any:Any	
∲+ NAT		Max. 5	512											1 - 2 of 2	
Colject Management															- 1
Firewall	*	APPL	<u> </u>												_

5.3 Expected Result

 The image below shows users can remotely access the server in the DMZ from the Internet via the NAT PAT function. In this scenario, we accessed the ioLogik in the LAN via the remote server in the DMZ. However, the remote server can only communicate with the ioLogik through the Modbus protocol. As a result, pinging the ioLogik via the remote server failed.

Able to access but unable to ping the ioLogik devi
--

National Science (1997) - Remote Desktop Connection	
Select Command Prompt - powershell	
Request timed out. Request timed out.	
Ping statistics for 192.168.10.250: Packets: Sent = 2, Received = 0, Lost = 2 (100% loss Control-C PS C:\Users\KaiKY_Lo> PS C:\Users\KaiKY_Lo>	s),
PS C:\Users\KaiKY_Lo> Test-NetConnection 192.168.10.250	-p 502
ComputerName : 192.168.10.250 RemoteAddress : 192.168.10.250 RemotePort : 502 InterfaceAlias : 乙太網路 4 SourceAddress : 192.168.127.102 TcpTestSucceeded : True	
PS C:\Users\KaiKY_Lo> Test-NetConnection 192.168.10.250 WARNING: Ping to 192.168.10.250 failed with status: Time	edOut
ComputerName : 192.168.10.250 RemoteAddress : 192.168.10.250 InterfaceAlias : 乙太網路 4 SourceAddress : 192.168.127.102 PingSucceeded : False PingReplyDetails (RTT) : 0 ms	

2. Monitoring Modbus TCP communications between PC and ioLogik

📲 220.128.222.101 - Remote Desktop Connection
쉽 Modbus Poll - Mbpoll1
File Edit Connection Setup Functions Display View Window Help
🗋 🚔 🔚 🎒 🗙 🛅 🖳 🛄 几 05 06 15 16 17 22 23 TC 🖗 🌌 🦓 💦
Tx = 4859: Err = 1: ID = 1: F = 01: SR = 1000ms
Name 00000
2
4 5
6
7
8
9

3. The firewall log shows the Modbus Master in the DMZ can establish a connection to the Modbus Slave in the LAN.

	DR-G901	0-VPN-2MGS	FP														Hi, adr	min
Q Search for a function		Event L	og															
Device Summary	^	System	Log Firewall	Log	VPN L	og	Settings and	Backup										
Setup Wizard																		
System	~	Layer 3-7	Policy -															
Network Configuration	~												Sear	h				
Redundancy	~	G											Q DM.	LAN				
Network Service	~	Index	Timestamp	Severity	Policy ID	Policy Name	Ethe Type	IP Protocol	Incoming Interface	Source MAC	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	TCP ICMP Flags Type	ICMP Code	Action
Bouting	~	4	2024/2/6 17:45:0+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH,		Allow
NAT			2024/2/6													DCH DCH		
Object Management		11	17:44:57+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	ACK		Allow
Firewall	~	17	2024/2/6 17:44:54+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH, ACK		Allow
VPN	~	21	2024/2/6 17:44:50+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH, ACK		Allow
Certificate Management	×	29	2024/2/6	Warning	1	DM7 LAN	2046	TCP	DM7	00:e0:00:60:96:6d	192 168 127 102	23008	LAN	192 168 10 250	502	PSH,		Allow
Security	~	27	17:44:47+8:00	manning		Diffic of the	2040		DINE		172.100.127.102	20000	2.01	172.100.10.200	001	ACK		
🔁 Diagnostics	^	35	2024/2/6 17:44:44+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	ACK		Allow
System Status	~	39	2024/2/6 17:44:41+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH, ACK		Allow
Network Status	~	45	2024/2/6	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH,		Allow
Event Logs and Notifications	^	50	2024/2/6 17:44:35+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	ACK	-	Allow
Event Notifications	.	56	2024/2/6 17:44:32+8:00	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	ACK		Allow
Syslog		60	2024/2/6	Warning	1	DMZ_LAN	2048	TCP	DMZ	00:e0:00:60:96:6d	192.168.127.102	23008	LAN	192.168.10.250	502	PSH,		Allow
SNMP Trap/Inform																		

4. Since the Advanced Protection settings are configured for read-only traffic to pass through, the Write Coil function will cause the firewall to reset the connection.

	9010-'	VPN-2MG	SFP												Hi, adr	nin :	l
Q Search for a function	E	Event I	Log														i
Device Summary	4	System	m Log Fire	wall Log	VPN Log	Settings	and Backup										
🜮 Setup Wizard																	
🔅 System 🗸 🗸		Protoco	Filter Policy 🔹														
🛞 Network Configuration 🛛 🗸		a	≐ - ⊡									0.5000	-de				
🖼 Redundancy 🗸 🗸												~ 3001					
军 Network Service v		Index	Timestamp	Severity	Application Protocol	Policy ID	Policy Name	Ether Type	IP Protocol	Incoming Interface	Source IP	Source Port	Outgoing Interface	Destination IP	Destination Port	Action	
🕀 Routing 🗸 🗸		1	2024/2/6	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	23007	LAN	192.168.10.250	502	Reset	
∲+ NAT		2	2024/2/6	Ememency	Morbue/TCP	00000	Enforcement	2048	TCP	DM7	102 168 127 102	23006	LAN	102 168 10 250	502	Decet	
G Object Management		-	17:43:34+8:00	Energency	incoded by Tel		Enoreement	2040	101	DML	172.100.121.102	20000	Din	192.100.10.200	001	Treaser	
Firewall Y		3	2024/2/6 17:43:32+8:00	Emergency	Modbus/TCP	999999	Enforcement	2048	TCP	DMZ	192.168.127.102	23005	LAN	192.168.10.250	502	Reset	l
얍 VPN V		4	2024/2/6 17:43:30+8:00	Emergency	Modbus/TCP	999999	Enforcement	2048	TCP	DMZ	192.168.127.102	23004	LAN	192.168.10.250	502	Reset	
Certificate Management V		5	2024/2/6	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	23003	LAN	192.168.10.250	502	Reset	
Ga Security V		6	2024/2/6	Emorrange	Modbus (TCD	00000	Enforcement	2049	TCD	0147	102 169 127 102	19002	LAN	102 168 10 250	500	Deset	
Diagnostics ^		,	17:43:26+8:00	childrendy	10000000101		Chloreement	2040	101	DINE	172.100.121.102	20002	Dat	172.100.10.200	001	THEFT	
System Status 🗸 🗸 🗸		7	2024/2/6 17:43:24+8:00	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	23001	LAN	192.168.10.250	502	Reset	
Network Status 🗸 🗸		8	2024/2/6 17:43:22+8:00	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	23000	LAN	192.168.10.250	502	Reset	
Event Logs and Notifications		9	2024/2/6 17:43:20+8:00	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	22999	LAN	192.168.10.250	502	Reset	
Event Notifications		10	2024/2/6 17:43:18+8:00	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	22998	LAN	192.168.10.250	502	Reset	
Syslog		11	2024/2/6	Emergency	Modbus/TCP	99999	Enforcement	2048	TCP	DMZ	192.168.127.102	22997	LAN	192.168.10.250	502	Reset	
SNMP Trap/Inform		-	17.40.1010.00														1

5. The remote server can monitor Modbus communication between the server and the ioLogik. Any write data will be blocked by the firewall as it violates the read-only policy.

-													
4	-59	220.128.222.101 -	Remote Desktop	Connection									
ť] N	Aodbus Poll - Mbp	oll1										
F	ile	Edit Connection	Setup Function	ıs Display V	liew	Win	dow	Help)				
	2	i 🖻 🖬 🎒 🏅	K 🗉 🗒 é	05	06	15	16	17	22	23	тс 🥻	1	 4
	00:1	Mbpoll1								×			
	Тх	= 16: Err = 16:	ID = 1: F = 05	5: SR = 100	0ms	\$				_			
	WI	rite error											
		Name	00000										
	0												
	1		0										
	2												
	3												
	4												
	5			_									
	6			_									
	7												
	8												
	9												
Ľ	1												