How to Build an Industrial DMZ to Protect Internal LAN Networks With Moxa Secure Routers

Moxa Technical Support Team

support@moxa.com

Contents

 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

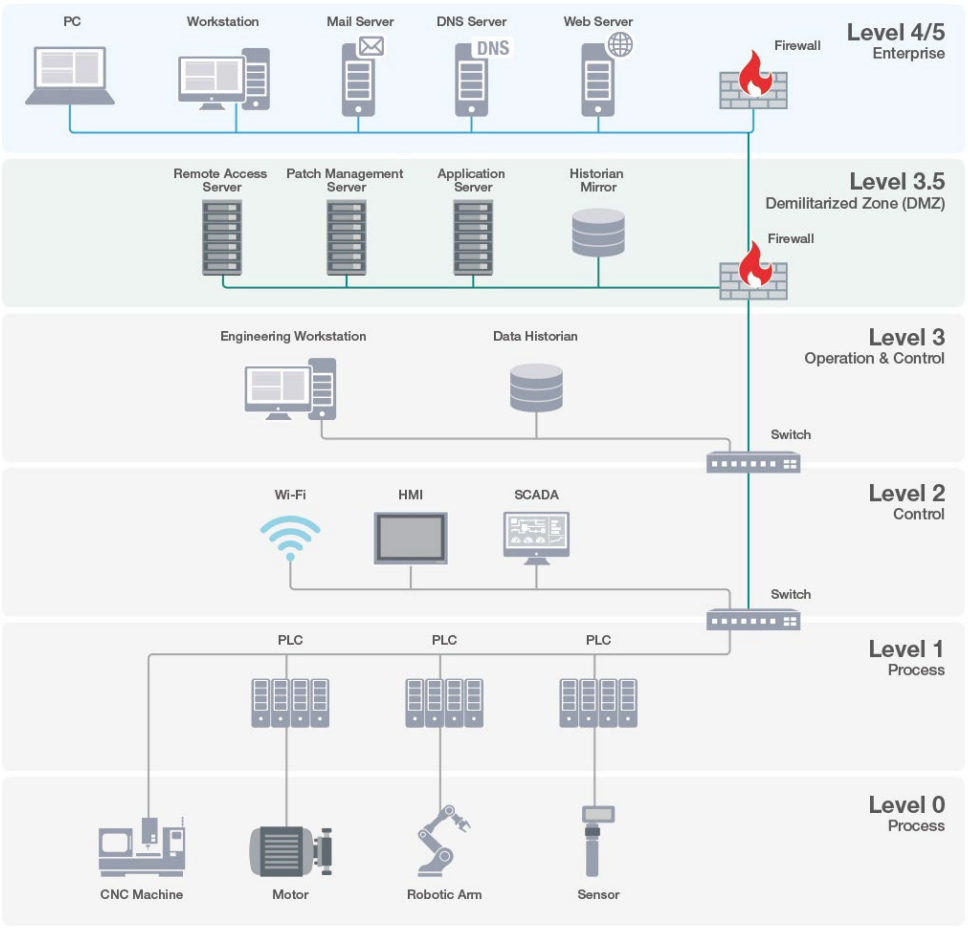
1 Introduction

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.

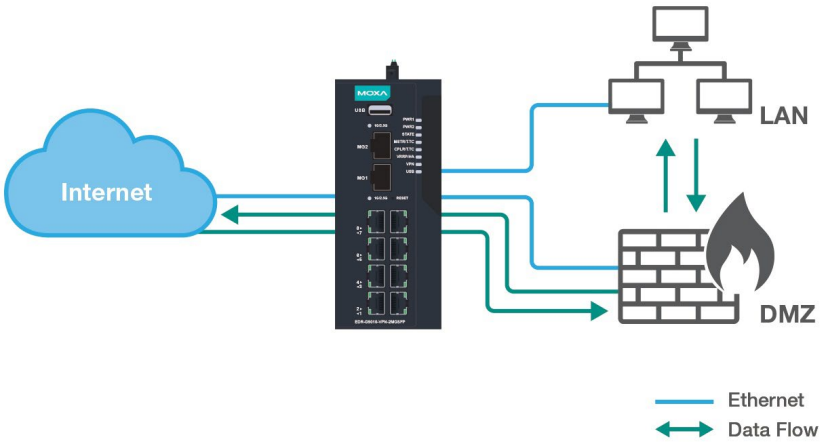
The following sections will introduce three different DMZ implementation scenarios. Each section will provide guidelines on how to set up the Moxa Secure Router for each scenario.

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.



Reference Diagram

Key Actions:

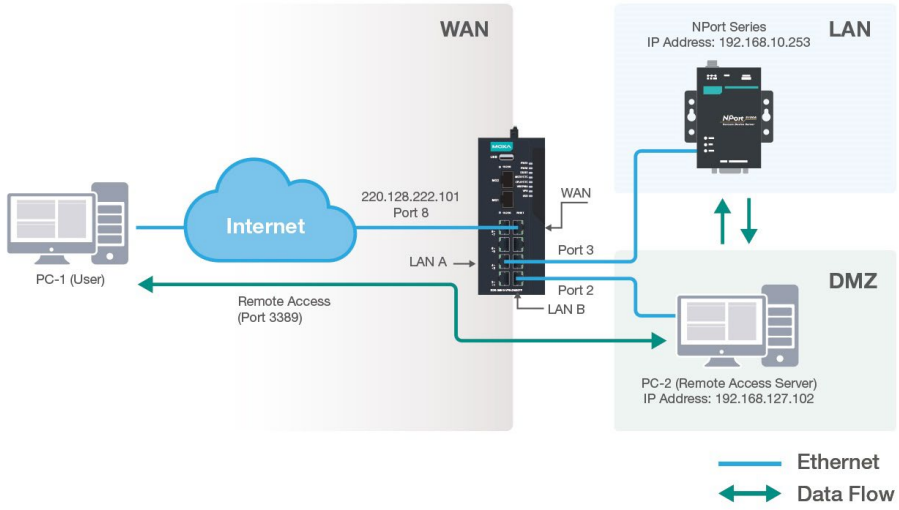
1. Configure 3 network interfaces: WAN, LAN, and DMZ.
   Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
2. Configure the Layer 3 firewall filter.
3. Create the allowlist policies.
4. Set up a DMZ to 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:

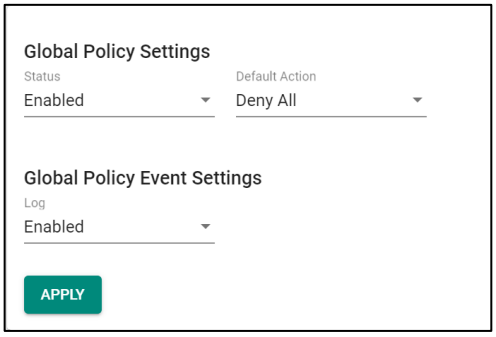
1. The DMZ is configured to allow bidirectional communication with the WAN.

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.



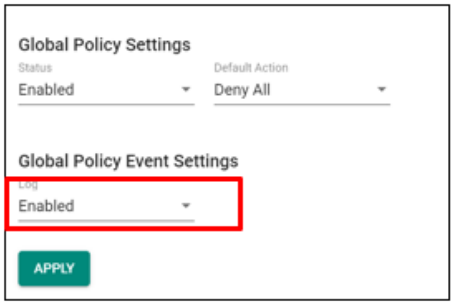
3. Click the **Add** (**+**) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
   - WAN-to-DMZ
   - DMZ-to-WAN
   - DMZ-to-LAN
   - LAN-to-DMZ

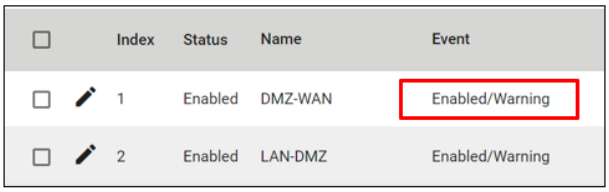
   The firewall rules are subject to the network environment. Refer to the overview below as a reference for how to configure the firewall rule parameters.

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

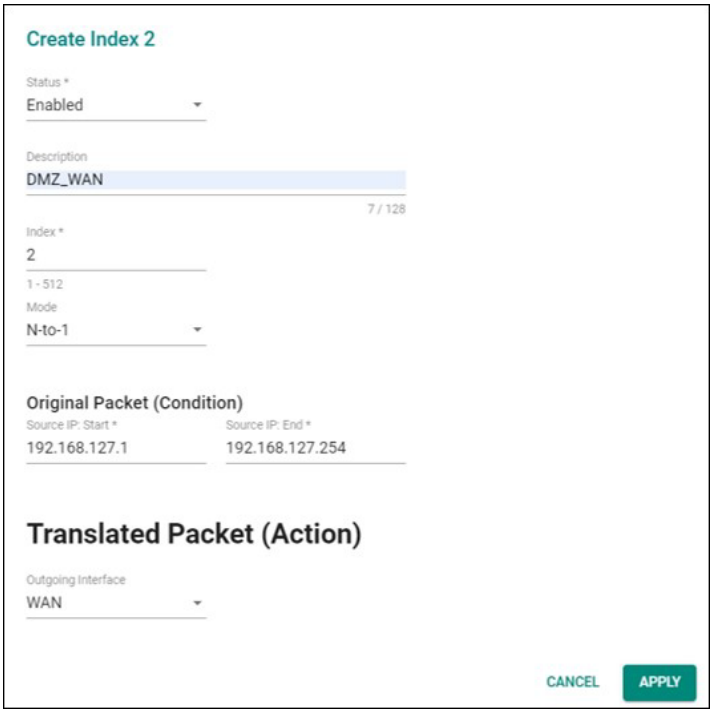
NOTE The L3-7 firewall is a stateful firewall which allows bidirectional communication. When configuring a unidirectional communication rule (e.g. DMZ-to-LAN), a connection between the specified interfaces must be established first before the interfaces can communicate in the opposite direction.

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



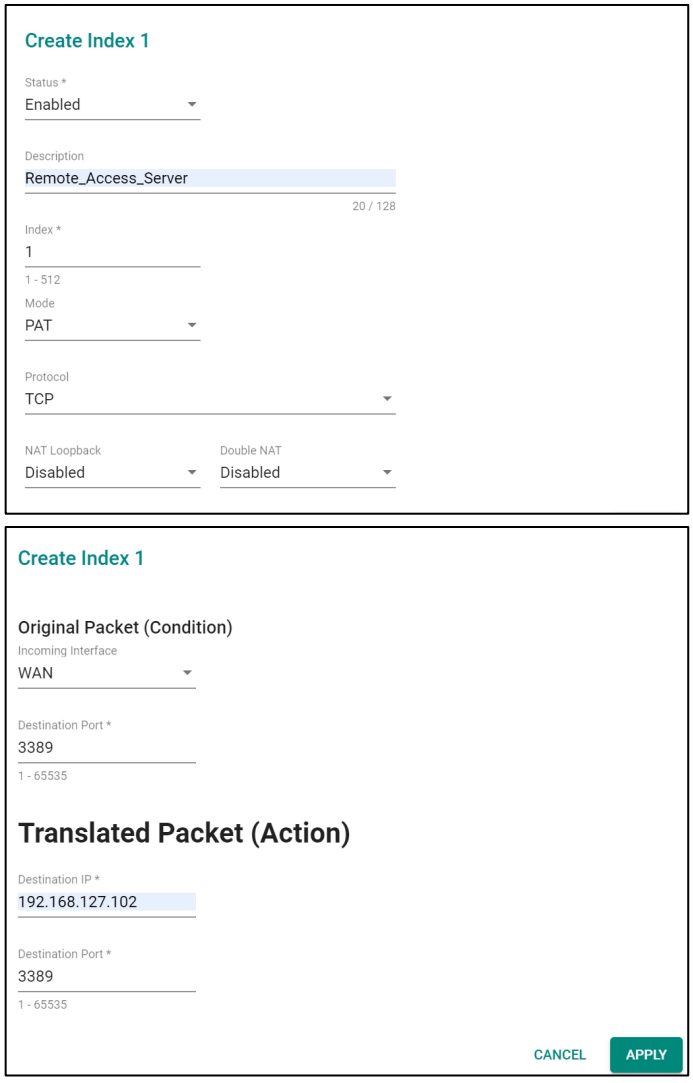


4. Navigate to **NAT Settings** and click the **Add** (**+**) icon to create a new NAT rule for the DMZ to access the Internet.
   i. Set the **Mode** to **N-to-1** and enter the Source Start and End IP address in the **Original Packet** field. This range will determine the IP addresses in the DMZ that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

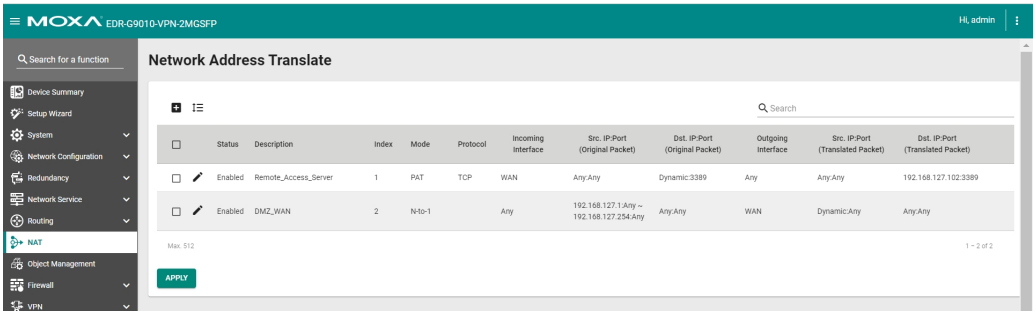


   ii. Set the **Outgoing Interface** to **WAN**.
   iii. Click **APPLY** to create the rule.

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.

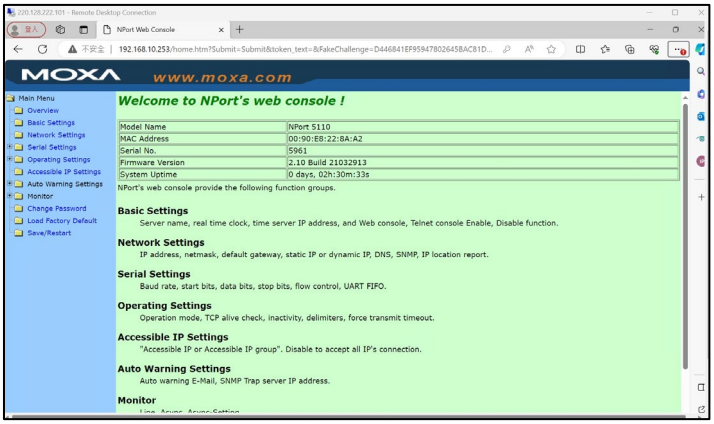


6. The created NAT rules will appear in the NAT rule table.

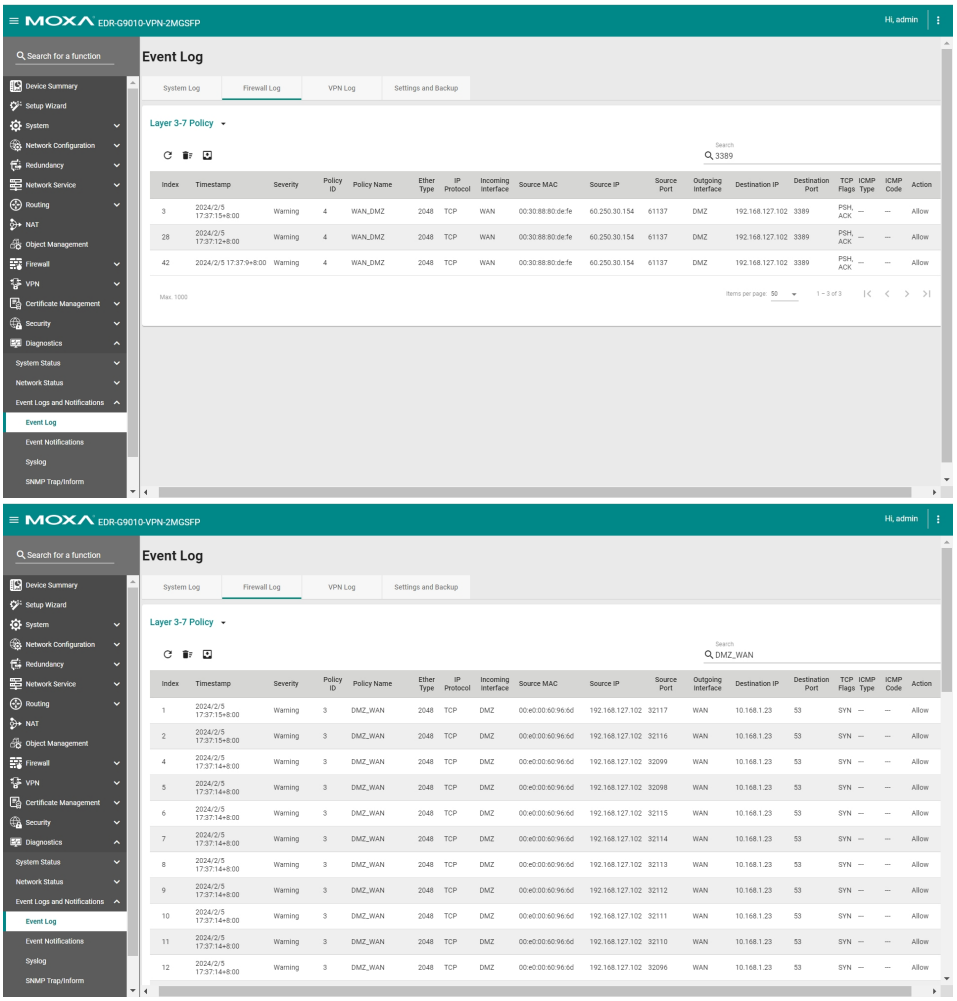


3.3 Expected Result

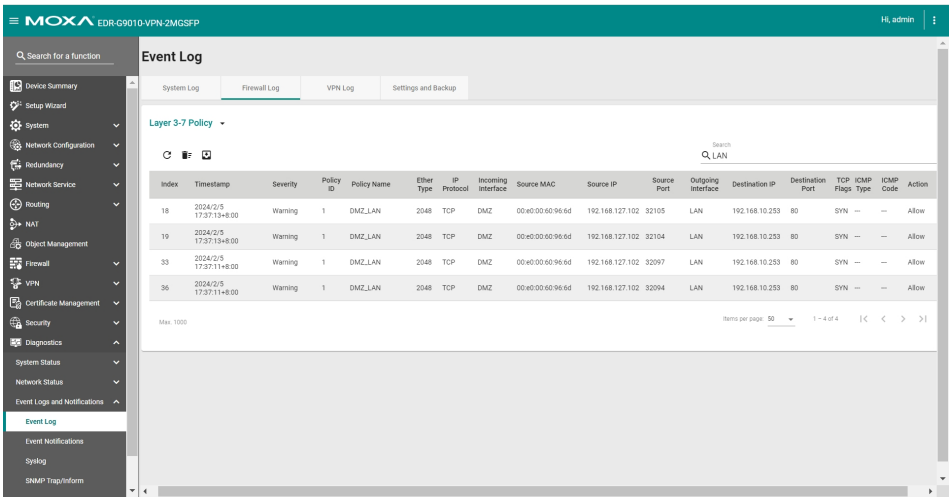
1. The image below shows users can remotely access the server in the DMZ from the Internet via the NAT PAT function. In this scenario, we accessed the NPort's web console in the LAN via the remote server in the DMZ.



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



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



4. LAN devices cannot communicate with the WAN interface.

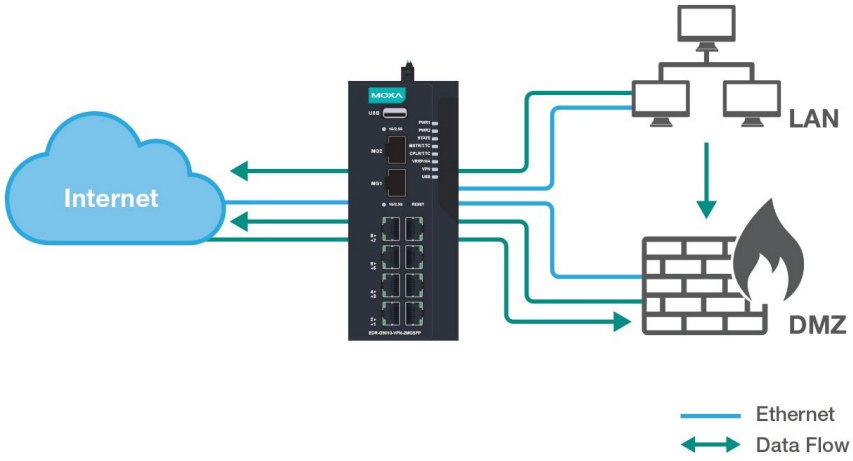
```
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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:

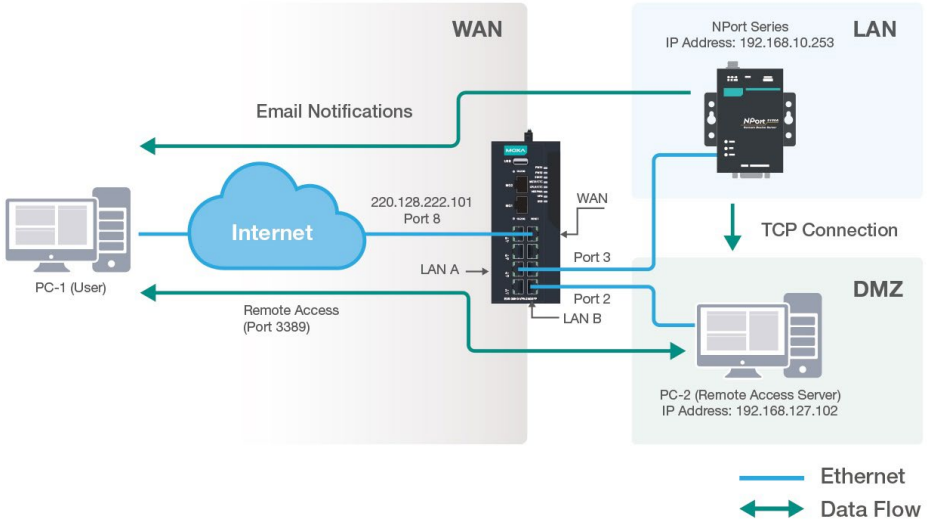
1. Configure 3 network interfaces: WAN, LAN, and DMZ.
   Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
2. Configure the Layer 3 firewall filter.
3. Create the allowlist policies.
4. Set up a DMZ to 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.

Refer to the network topology for this scenario below:



Network Topology

Communication Principles:

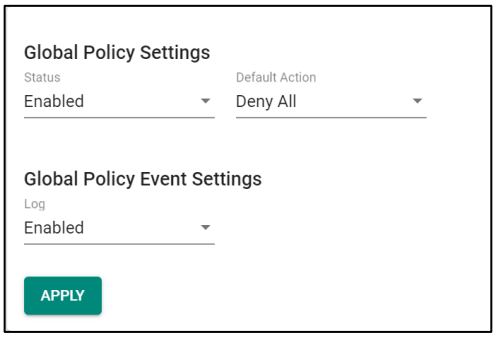
1. The DMZ is configured to allow bidirectional communication with the WAN.

2. The 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**.
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 to access the DMZ.

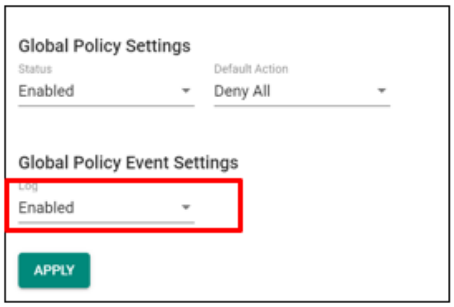


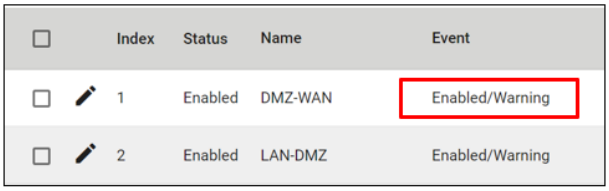
3. Click the **Add** (**+**) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
   - WAN-to-DMZ
   - DMZ-to-WAN
   - LAN-to-DMZ
   - LAN-to-WAN

   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.

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

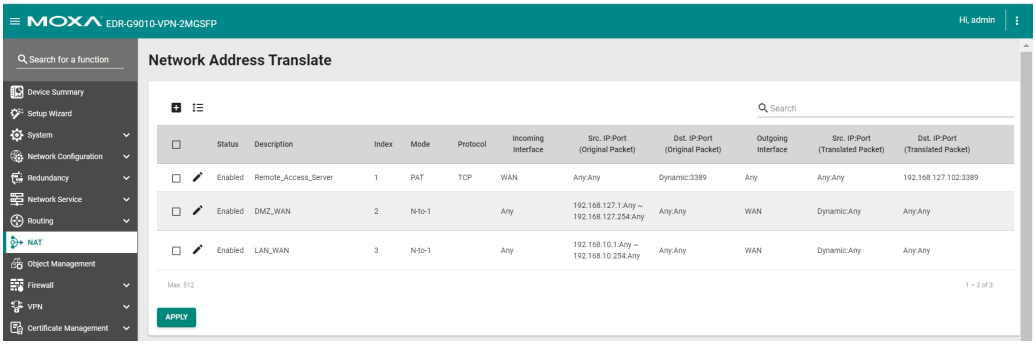
NOTE If you want to monitor the Layer 3-7 firewall events, enable the **Global Policy Event Settings** option.





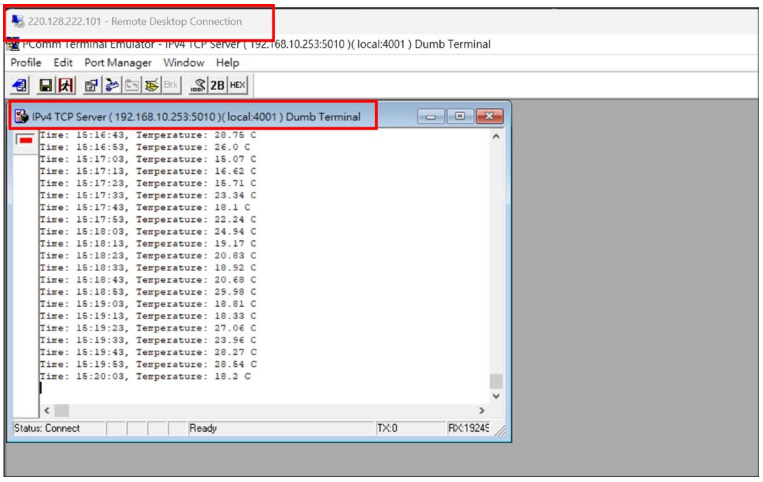
4. Navigate to **NAT Settings** and click the **Add** (**+**) icon to create a new NAT rule for the LAN interface to access the Internet.
   i. Set the **Mode** to **N-to-1**.
   ii. Specify the **Source IP Start** and **End** to determine the LAN IP address range that can access the Internet.
   iii. 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.



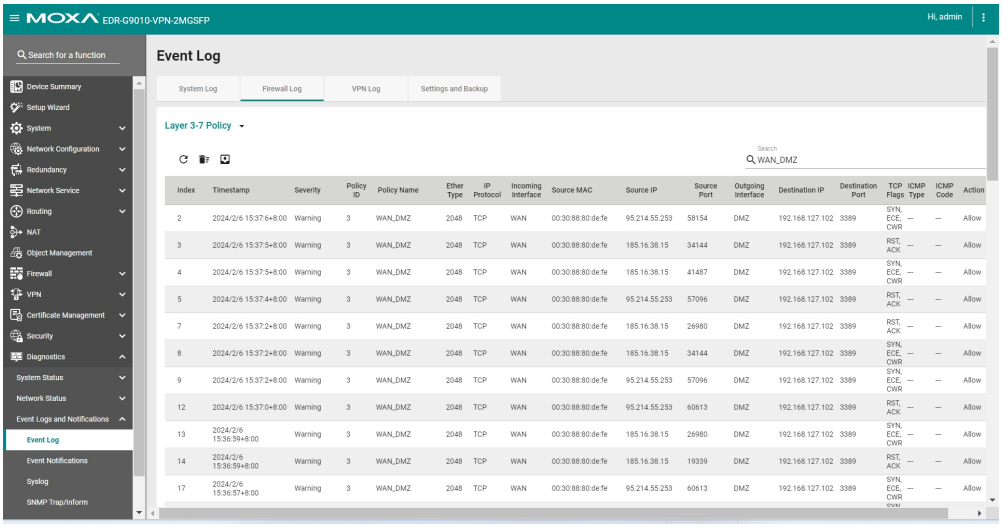
4.3 Expected Result

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.

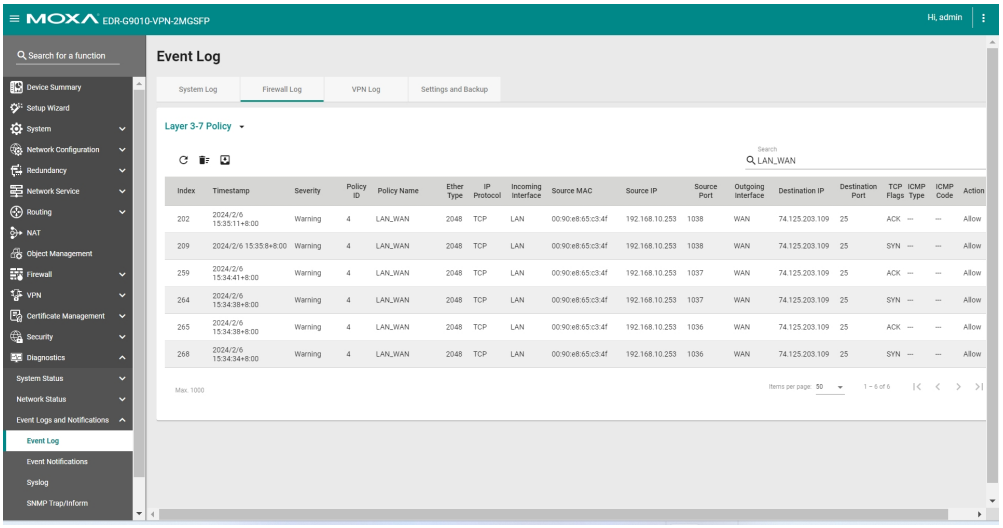


2. The firewall log shows devices in the LAN and DMZ can successfully connect to the Internet. Additionally, devices in the LAN can communicate with devices in the DMZ.

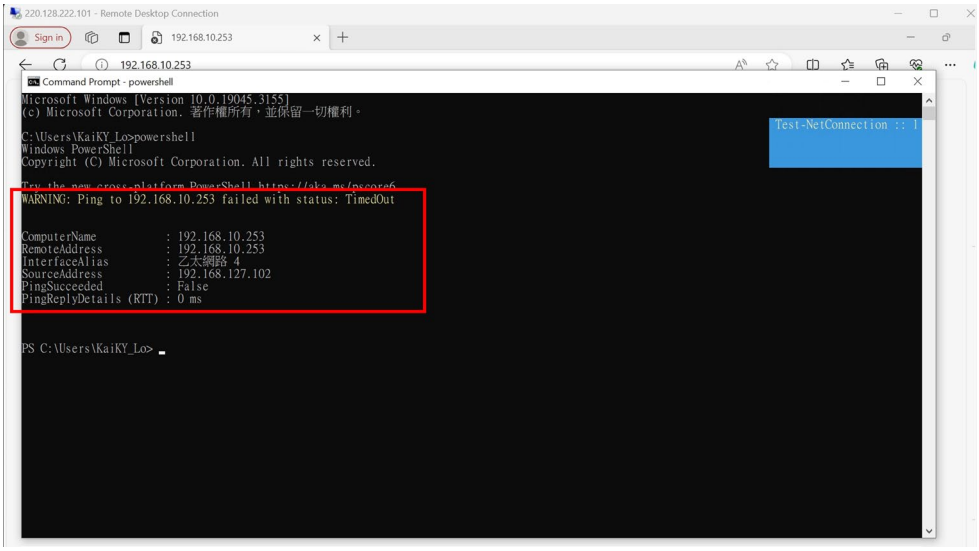
WAN-to-DMZ



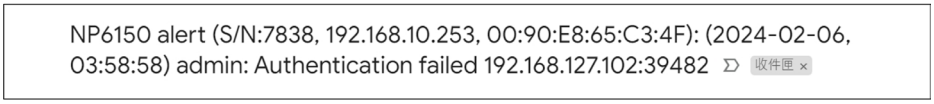
LAN-to-WAN



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.

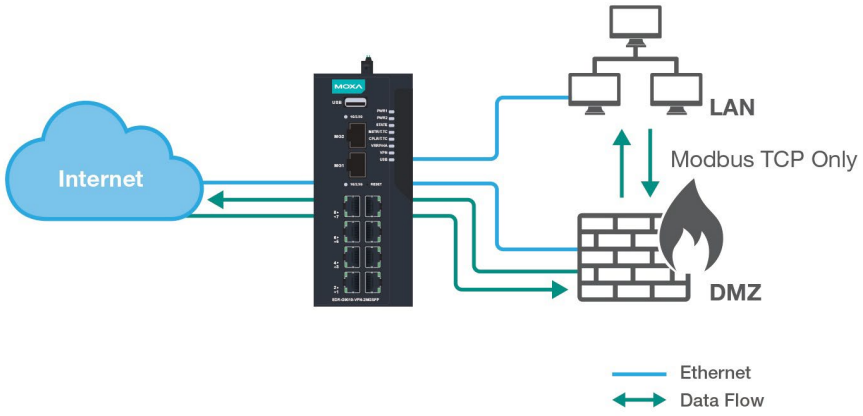


5 Reference Scenario 3: LAN Fully Isolated From the Internet, With Modbus Communications

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.



Reference Diagram

Key Actions:

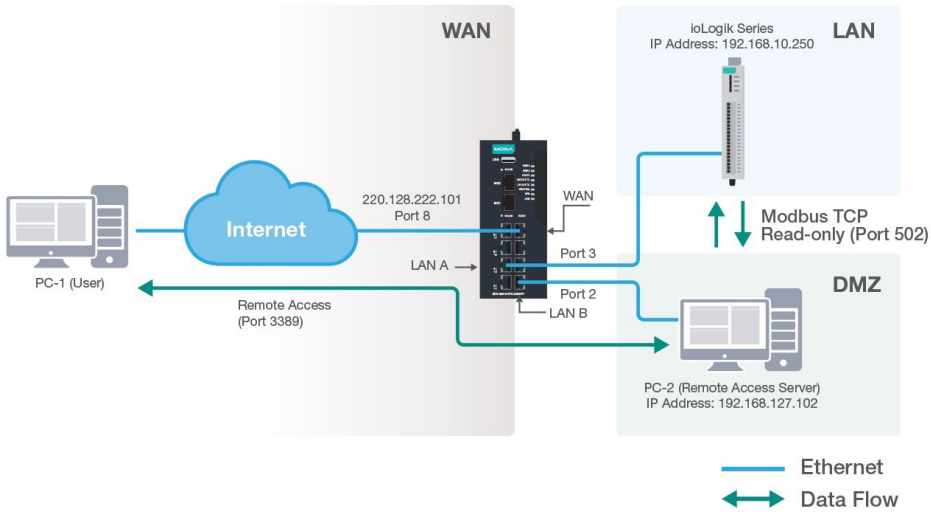
1. Configure 3 network interfaces: WAN, LAN, and DMZ.
   Refer to the **Network Configuration > Network Interface** section in the MX-ROS user manual for more information on how to create these interfaces.
2. Configure the Layer 3 Firewall filter.
3. Create the allowlist policies.
4. Set up a DMZ to 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:

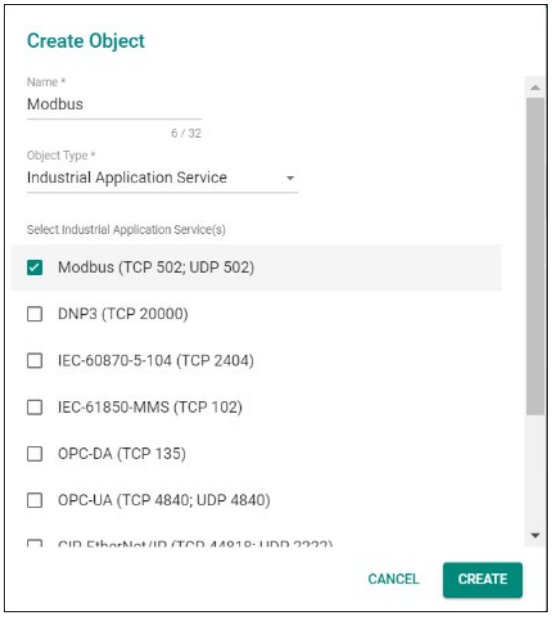
1. The DMZ is configured to allow bidirectional communication with the WAN.

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

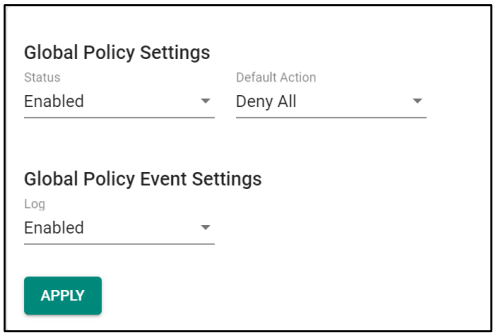
3. The LAN is not allowed to communicate with the WAN.

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)**.



   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.

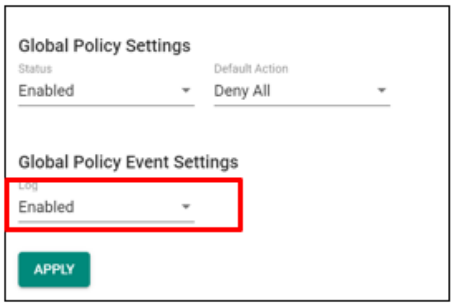


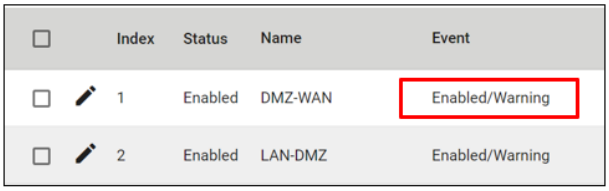
5. Click the **Add** (**+**) icon to create a new firewall rule. Create the following firewall rules to establish the correct communication policy between the LAN, DMZ, and WAN:
   - WAN-to-DMZ
   - DMZ-to-WAN
   - DMZ-to-LAN: Uses the Modbus object created in step 2 as the Destination Port.
   - LAN-to-DMZ: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

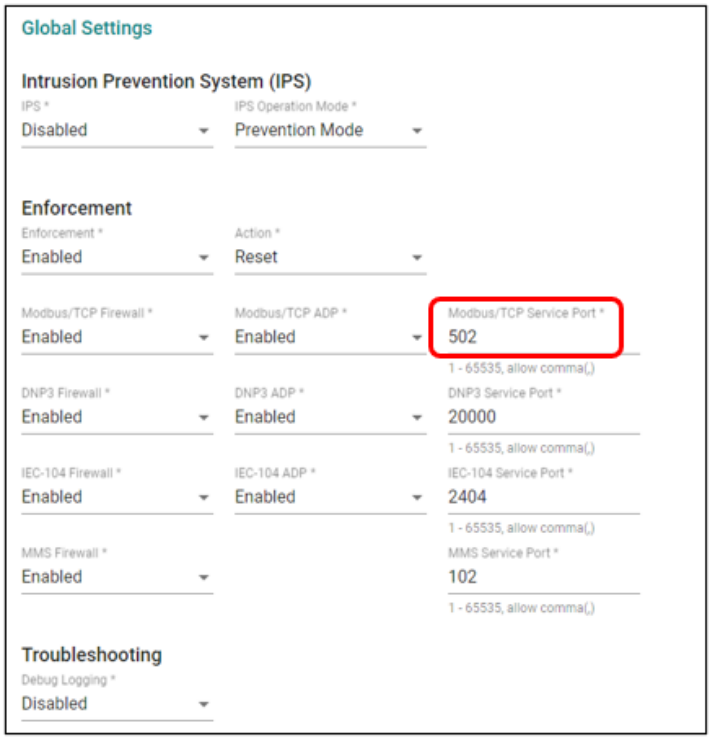
NOTE If you want to monitor the Layer 3-7 firewall events, enable the **Global Policy Event Settings** options.



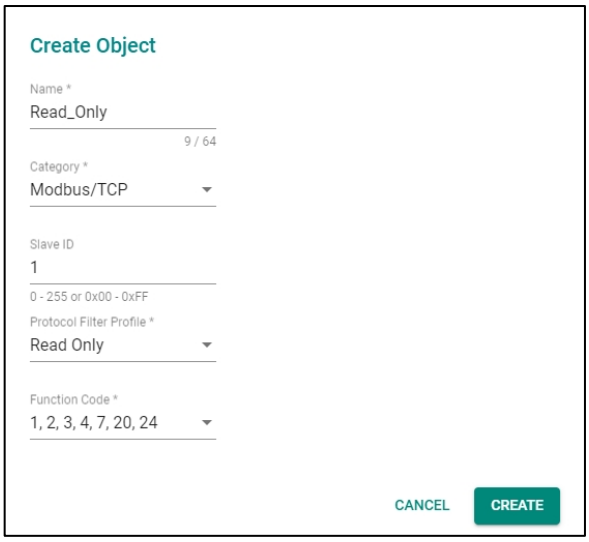


6. Navigate to **Firewall > Advanced Protection > Configuration > Global Settings**.
7. In the Enforcement section, set **Enforcement** to **Enable** to enable advanced protection.

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

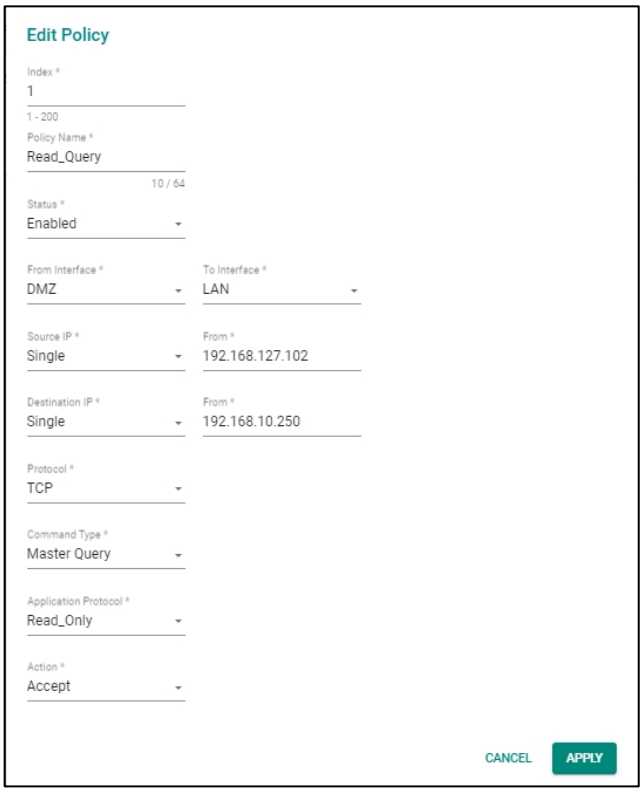


9. Navigate to **Firewall > Advanced Protection > Configuration > Protocol Filter Object**.
10. Click the **Add** (**+**) icon to create a new Modbus TCP protocol filter object.
    i. Select **Modbus/TCP** as the Category and set the Protocol Filter Profile to **Read Only**.



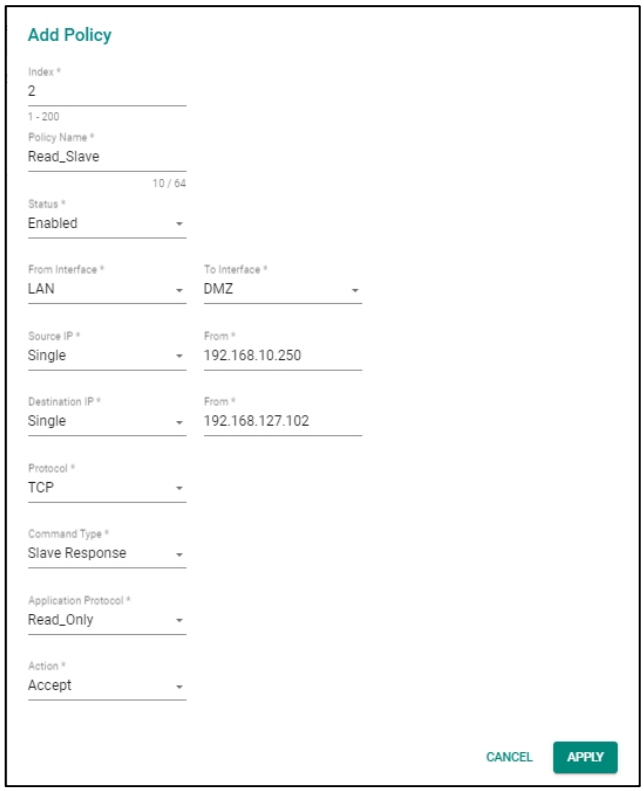
    ii. Click **CREATE** to create the object.
11. Navigate to **Firewall > Advanced Protection > Protocol Filter Policy**.

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.



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.

v. Click **APPLY** to create the rule.

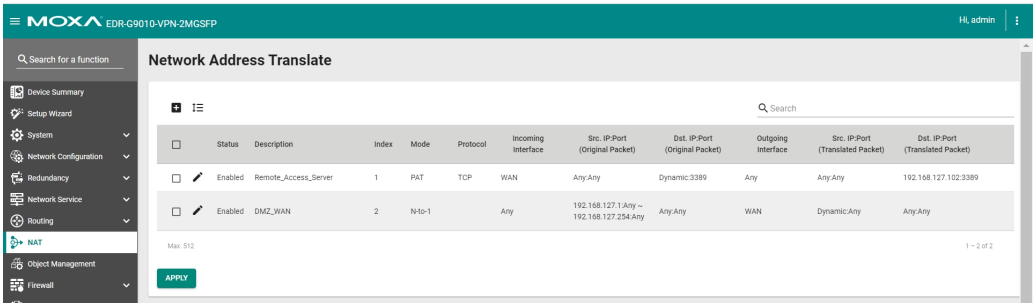


Both rules will appear in the protocol filter policy table.

	Index	Policy Name	Status	Protocol Filter Object	From Interface	To Interface	Source IP	Destination 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.

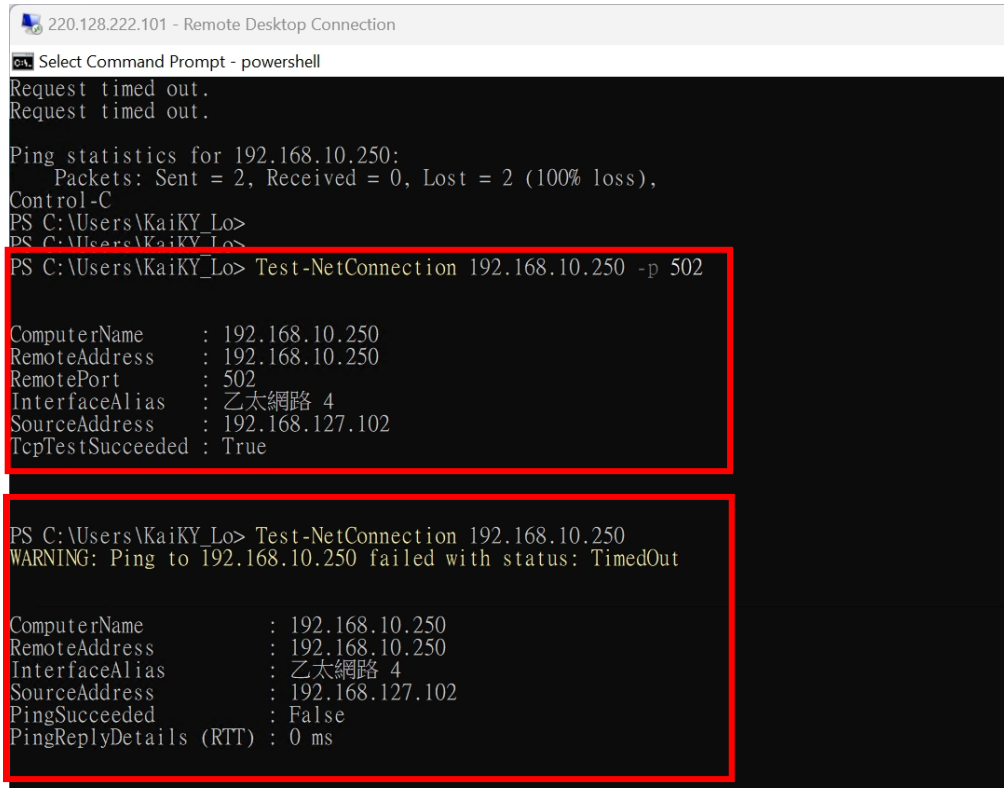
16. The created NAT rules will appear in the NAT rule table.



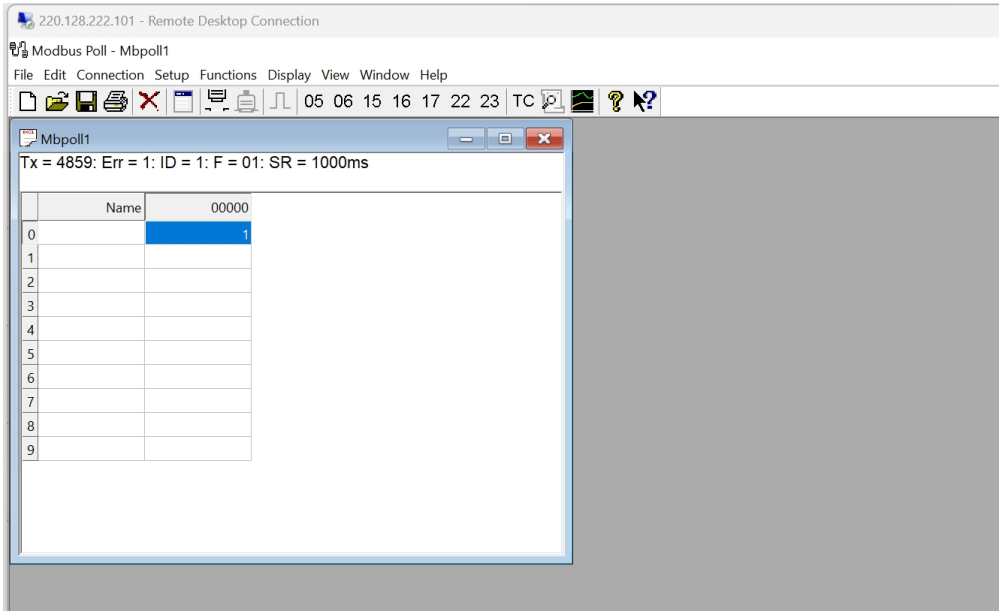
5.3 Expected Result

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 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.

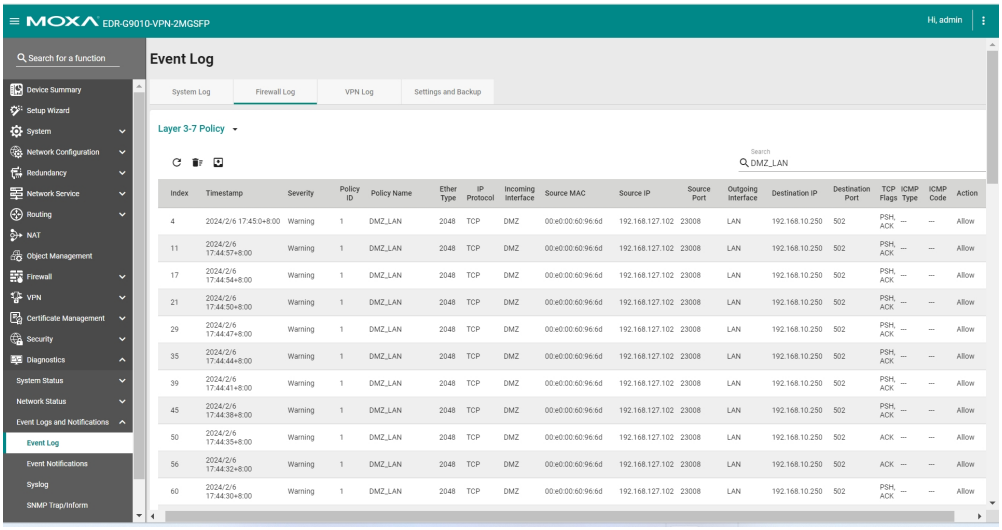
   Able to access but unable to ping the ioLogik device



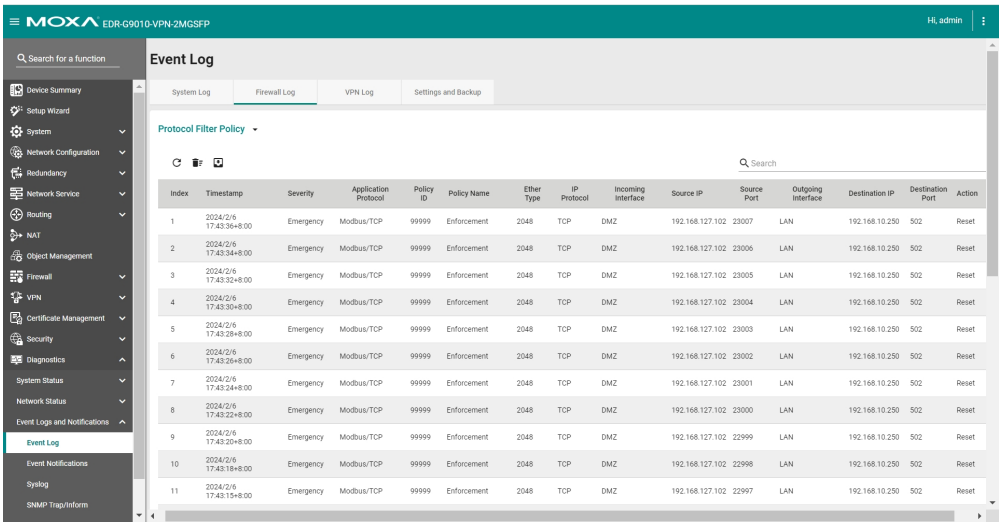
2. Monitoring Modbus TCP communications between PC and ioLogik



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



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.



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.