Merlin – Security Hardening Guide

AN-005-WIE

Hardware Models	Merlin Series
Revision	1.02
Approval status	Approved
Date	26 November 2025
Brief description	Security Hardening Guide
Author	Artur Wachowski

1 Overview

This Security Hardening Guide describes the features and “know how” to introduce basic security configuration to Merlin series routers.

IMPORTANT NOTE

This Security Hardening Guide provides a basic, non-exhaustive example of typical recommendations, security and operational policy considerations, intended solely as a guidance reference.

The content shall be used as a general guide only, and does not constitute a recommendation, instruction, or endorsement of any specific configuration or security controls.

To the maximum extent permitted by applicable law, Westermo Ireland Ltd. shall not, under any circumstances, be held liable for loss of profits, data, business opportunity, or for any incidental, indirect, or consequential damages arising from the use of this material, even if advised of the possibility of such damages.

1.0 Firmware information

Firmware version: SXL-**25.05.15.000** or newer.

1.1 Assumptions

This security hardening guide can be applied to all routers in the Merlin Series.

1.2 Corrections

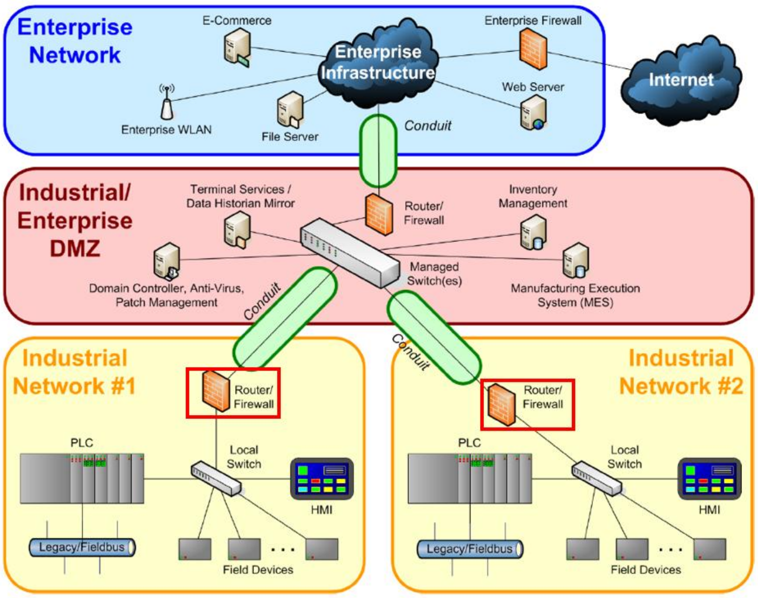
Requests for new application notes or corrections or amendments to this application note are welcome and should be addressed to support.ie@westermo.com

1.3 Report Vulnerability

Report security issues or vulnerabilities in Merlin devices to: PSIRT.ie@westermo.com

2 Intended Operational Environment

High-level manufacturing example showing zones and conduits (source: ISA/IEC 62443-3-2)

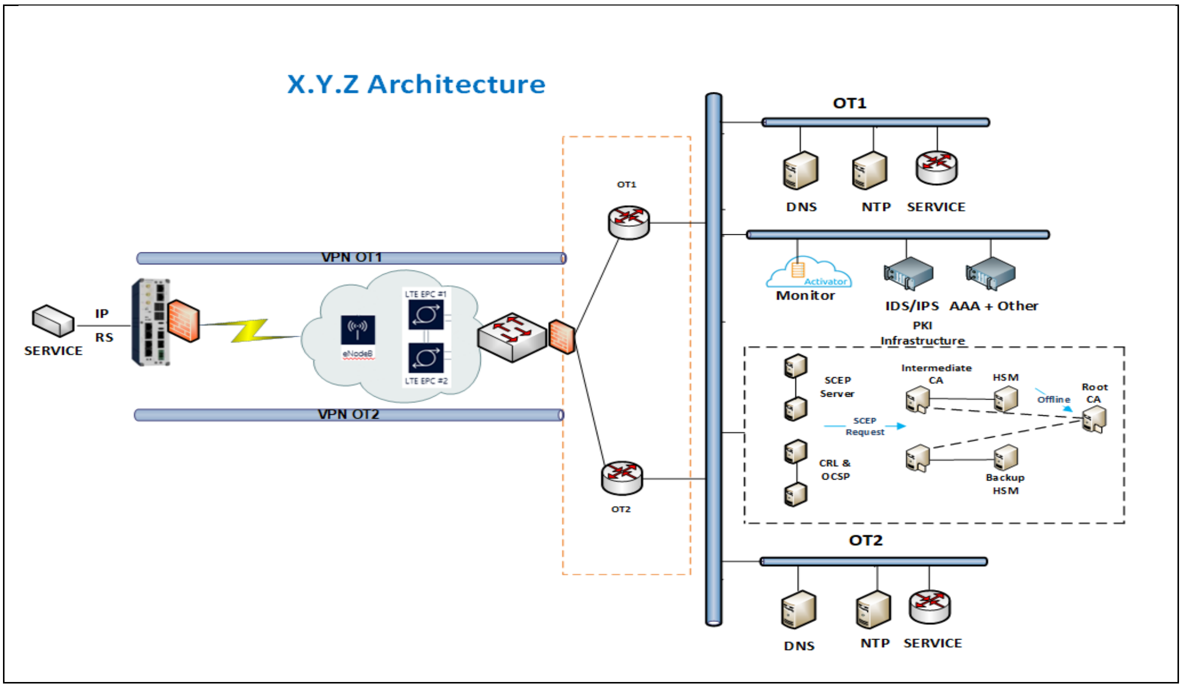


IEC 2033/13

The above figure shows a typical Merlin installation in an industrial network, marked with red square.

The Merlin Series cellular routers provide secure remote access and always-on communication solutions for any industrial environment. Incorporating advanced security features such as TPM chips, Secure Boot, VPN, and a stateful inspection firewall, these routers ensure robust protection for data transmitted over both public and private networks. Legacy serial ports and an industrial protocol gateway facilitate the migration from traditional modem-based communications to IP networks, making the Merlin Series ideal for demanding applications like modern manufacturing applications, smart grids and event trackside systems. When integrated with the dedicated Device Management Platform, Activator, Merlin devices also enable zero-touch deployment, streamlining initial setup and simplifying ongoing software and configuration updates.

2.0 Intended operational enviroment example



Note: Every Merlin series router features dual SIM for dependable, rapid failover redundancy.

The above diagram illustrates a simplistic deployment scenario for Merlin Series routers within typical industrial network. In this example, the Merlin router operates as a security gateway, chiefly managing traffic between the remote site and the operations centre, while also enabling secure remote access over Private LTE network as a second main function.

The Merlin Series is equipped with a range of advanced cybersecurity features, which are designed to meet common industry security standards. These functions should be assessed according to the selected security objectives and requirements defined for the deployment environment. The design process should include specifying security expectations, translating them into technical requirements, and verifying their implementation to ensure that the desired security posture is achieved before deployment.

This document provides guidance to help end users configure the Merlin router and integrate it into their wider system. It also outlines important assumptions and mandatory requirements concerning the system, operations, and installation environment, as determined by the component vendor. These aspects are essential for achieving the intended security capabilities of the product.

Ultimately, the end user is responsible for ensuring the product is correctly integrated into its operational environment and used appropriately.

Westermo Ireland offers a range of professional services. For all project enquiries or other needs, please contact us at support.ie@westermo.com.

3 Device Operations Assumptions

Staff Competency: Assumes operational staff are qualified to design, manage, secure, and troubleshoot OT/IT networks, including verifying security capabilities and performing basic threat modelling on Merlin Series routers.

Secure Installation: It is assumed that each device is installed within a secure enclosure to mitigate risks associated with physical access and tampering. Access to the enclosure should be monitored through Digital Input functionality, which is available in selected Merlin Series routers.

Compliance with Security Protocols: Assumes devices and systems follow all established cybersecurity guidelines and defence-in-depth practices.

Key Management: The Public Key Infrastructure must be implemented in accordance with industry standards, recommendations, and best practices.

Authenticator Service: Third-party authentication services are to be deployed following recognized industry standards and guidelines.

Zero Touch Deployment (ZTD): All components should be provisioned and managed using ZTD methodologies, minimizing direct human interaction and enabling centralized management of software and configuration assets.

Configurations: End users are responsible for reviewing and complying with security guidelines, ensuring that only essential services remain operational.

Malware, Antivirus, and Continuous Monitoring: The operational environment must utilize centralized solutions for network segmentation, deep packet inspection, advanced firewalls, and comprehensive traffic monitoring. It is assumed that all components are segregated from public and enterprise networks.

Physical Diagnostic and Test Interfaces: Diagnostics and testing within the production environment are strictly prohibited and must be enforced through monitoring and system-level policies.

Certificates and Password Management: System and security administrators are accountable for maintaining the validity and timely renewal of certificates and passwords, with enforcement of appropriate strength and update policies.

Legal Disclaimer: End users accept full responsibility for the operation and security of Merlin series routers. Compliance with all applicable laws and regulations pertaining to the deployment and use of these devices is required. Any non-compliance is at the sole risk of the end user. The information provided in this security hardening guide is intended to assist end users in making informed decisions regarding the implementation of required security capabilities.

4 Device installation, commissioning, operations, and decommissioning

Physical Installation: The Merlin Series router has been engineered for straightforward DIN rail mounting and does not necessitate any non-standard installation solutions. Comprehensive instructions are available in the User Guide documentation.

Product Configurations: Shipping configurations are typically established during the procurement phase. Users are responsible for verifying and commissioning device configurations prior to production deployment.

Commissioning: In addition to standard Site and Functionality Acceptance Testing, dedicated Cybersecurity Acceptance Testing should be conducted. Ideally, an external contractor should verify the operational environment's cybersecurity.

Product Operations and Maintenance: Merlin Series routers do not require additional physical maintenance. Ongoing tasks such as configuration and software updates shall be managed via the centralised platform. Maintaining up-to-date product software is essential, with detailed guidance provided during the procurement process.
Note: Release Notes, supplied with each software release, detail identified bugs, errors, and security issues.

Product Removal from Operational Environment: Disconnect the product carefully in accordance with the local procedures, these should include powering down the device, disconnecting all connected systems, and physically removing the product from its installation location.

Clearing Configuration Data: To erase stored configuration data, follow the reset procedure outlined in the Management Guide or overwrite with a blank configuration.

Secured Data: Ensure erasure of sensitive material stored in the TPM chip by performing the TPM delete procedure as described in the Management Guide.

Safe Disposal of the Product: End-users are solely responsible for ensuring the safe and lawful disposal of the device in accordance with local regulations. Westermo Ireland complies with the EU WEEE Directive and accepts returns of end-of-life devices under applicable terms and conditions. Devices also adhere to ISO 14001 recommendations and may be repurposed for extended service durations, subject to terms and conditions.

5 Security hardening recommendations

5.0 Generic recommendations

It is recommended to always use the latest version of software, for more details contact support.ie@westermo.com or visit the products page at www.westermo.com

Westermo Ireland considers a VPN technology as a mandatory solution for protecting your data-in-transit and delivering a minimum of cyber security for end-devices. Westermo Ireland's devices provide VPN method flexibility and interoperability with all major VPN technologies, the devices offer support for industry standard technologies such as IPsec, DMVPN or OpenVPN.

It is recommended using certificates as an alternative to text-based passwords, with an on-board TPM for certificate protection.

It is recommended to avoid enabling or leaving enabled any of 'unused' services or port and performing all configuration tasks with a 'minimum on' approach; meaning that, anything that is unused would be completely removed from configuration files. This approach significantly limits number of running services and reduces number of potential cyber-attack vectors.

Recommendations provided in this guide will not provide 100% of cyber security. It is recommended to **always** introduce a secondary and tertiary detection and monitoring mechanism such as IDS/IPS services and external PKI, Access Control solutions, often referred as defence-in-depth strategy. These are outside of scope of this documentation.

Personal Data concerns: Westermo Ireland devices function exclusively as network devices, mainly for data transit and serving as communication gateway for specialised applications or services; they are not designed to store or process personal data nor content of the data in transit. Administrators are strongly encouraged to use generic identifiers, such as "operator1", "site-B" instead of personal identifiers like "JohnDoe" or "mainStreetDublin1". Other configuration components consist of standard network and security settings, which are not regarded as personal data.

Westermo Ireland devices offer comprehensive configuration capabilities, allowing users to specify or select cryptographic algorithms, ciphers, and key lengths as required. End-users are encouraged to adhere to established best practices for cryptography.

Westermo Ireland devices offer advanced networking capabilities tailored for radio communication technologies. It is expected that administrative personnel possess the necessary qualifications to design, manage, secure, and troubleshoot OT/IT networks, including assessing security features and conducting fundamental threat modelling on targeted production environment with Merlin Series routers prior to full deployment. Devices should only be installed following the successful completion of all provisioning procedures and acceptance testing, as per local requirements, that include necessary on-site/production security testing.

5.1 Westermo configuration services

Pre-configured devices offer significant advantages in terms of security, operational efficiency, and cost savings. By opting for devices that are configured before delivery, customers can be confident that all recommended security settings, user roles, and network policies are correctly applied from the outset.

From a security perspective, pre-configured devices minimise the risks, reduce exposure to cyber threats, and ensure compliance with industry standards. Critical features such as strong password policies, certificate-based authentication, firewall rules, and secure remote access are set up according to best practices, greatly reducing the attack surface and the likelihood of misconfiguration vulnerabilities.

In addition to enhancing security, the simplified configuration process offered by pre-configured devices saves significant time and money by reducing manual configuration efforts. This service streamlines deployment, enabling devices to become operational much faster.

For organisations managing large-scale or distributed networks, the benefits are even greater when integrating configuration services with Device Management platform discussed in section 5.13. Centralised management ensures consistency across all devices, simplifies ongoing management, and supports rapid scaling of secure infrastructure. The reduction in direct human interaction with end devices also lowers operational risks and costs associated with travel, training, and maintenance.

Westermo Ireland strongly recommends the use of its configuration services to ensure devices are delivered ready for secure operation, helping customers achieve robust security and substantial operational savings from day one.

5.2 Remote access

For LTE devices such as Westermo Ireland routers, remote access is a key feature. Device not only enables remote site connectivity, saving significant costs on labour and travel, but also allows for critical security operations, legacy asset protection, and site monitoring. There are two main methods for accessing the device: remotely or locally, via the Command Line Interface (CLI) or the Web User Interface (WebUI).

CLI access is mainly provided through the SSH protocol, using the Dropbear package. By default, SSH is available on port 22 across all interfaces. It is strongly recommended to:

- Enable remote access only on selected interfaces
- Change the default port number
- Use strong passwords
- Enable additional security features such as RSA key authentication or Multi-Factor Authentication (MFA)
- Apply strict firewall rules, especially since this access method is often exposed externally
- Configure advanced security logging and monitoring for these interfaces
- Implement user and role management features

To configure SSH (Dropbear):

- Go to WebUI > Security > SSH.
- Go to CLI > Dropbear package.

WebUI access is managed via the uHTTPd package. By default, the router listens on ports 80 (HTTP) and 443 (HTTPS) on all IP addresses (0.0.0.0). It is strongly recommended to:

- Disable unencrypted HTTP access on port 80
- Enable WebUI access only on specific interfaces using secure HTTPS (port 443)
- Assign non-standard port e.g. 4443 and/or restrict access to specific IP addresses, such as the router's LAN IP if only local access is needed.
- Disable WebUI entirely, recommended for high-security environments.

To configure WebUI (uhttpd):

- Go to WebUI > Security > HTTP Sever.
- Go to CLI > uhttpd package.

For more information on configuring SSH or WebUI, refer to the relevant sections in the device's Management Guide.

5.3 Time synchronisation

Time synchronisation is a critical and often overlooked feature. It plays a fundamental role in the correct functioning of many services, especially those involving VPN connections secured with certificates, telemetry services, as well as logging and monitoring systems. Accurate timestamps are essential for effective troubleshooting, audit trails, and forensic analysis.

Time synchronisation should be treated as a primary and mandatory component in any system architecture or design. Without it, services relying on time-sensitive operations may fail or behave unpredictably, and logs may become unreliable or misleading.

Westermo Ireland routers support NTPv4 (Network Time Protocol version 4), which includes basic password authentication and is implemented via the well-known Chrony package. Chrony is a versatile and efficient NTP client and server that is suitable for systems with intermittent connectivity or variable latency, such as LTE-based routers.

For more information on configuring NTP, refer to the relevant sections in the Management Guide.

5.4 VPN (Data-in-Transit)

Westermo Ireland considers a VPN technology as a mandatory solution for protecting data-in-transit and delivering a minimum of cyber security for end-devices.

The router supports multiple methods for encrypting data, including IPSec, DMVPN and OpenVPN. For IPSec, IKEv2 is the preferred protocol due to its efficiency and streamlined negotiation process. It is recommended to use X.509 certificates for authentication, which enhances security and scalability. The router also supports SCEP (Simple Certificate Enrollment Protocol), allowing for automated certificate management and renewal.

When configuring IPSec or OpenVPN, it is important to select strong and compliant cryptographic algorithms. Recommended encryption algorithms include:

- AES (Advanced Encryption Standard) with key lengths of 128, 192, or 256 bits
- SHA-2 family (e.g. SHA-256, SHA-512) for hashing and integrity
- ECDSA or RSA for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) groups such as ecp256 or ecp521 for key exchange
- HMAC-SHA2 for pseudorandom functions (PRF)

Outdated algorithms such as DES, 3DES, MD5, and SHA-1 should be avoided, as they are considered weak and may expose the VPN to vulnerabilities. Following recomendation such as CNSSP 15 – NSA " CONFIGURING IPSEC VIRTUAL PRIVATE NETWORKS" and regularly reviewing cryptographic settings is strongly advised.

To select and configure VPN:

- Go to WebUI > VPN > select a relevant VPN technology.

For more details refer to relevant sections in the Management Guide.

5.5 Password - Initial Access

As part of our regulatory obligations, all Westermo Ireland products falling within the scope of RED comply with the relevant harmonised standards and technical requirements, as further specified in EN-18031.

Available options for device procurement:

Unique Password (On request)

Ordered devices will be configured with unique passwords. During manufacturing, a specialised tool will automatically generate a distinct password for each unit. A separate document listing these passwords will be included in the shipping file.

Single-Use Password (Default)

Devices will be shipped with a standard Single-Use password, identical across all units. However, the device's access interface will enforce a password change upon first login, requiring the user to set a new password.

Note: This option is not compatible with the Device Management System - Activator.

Custom Password (Recommended)

Offered as part of our custom configuration service, this option allows customers to specify their own factory settings, including passwords. Customers are expected to provide a list of passwords along with any other required configuration parameters.

5.5.1 Password management

The password for accessing the router should be changed regularly to meet industry security requirements, as of 2025 the passwords should be at least 16 characters long. The password can be updated via the router's WebUI and CLI. It is recommended to use unique and cryptographically strong password **per** device.

The following CLI command will generate a 16 character long unique string

```
< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c${1:-16};echo;
```

To change password:

- Go to WebUI > Security > Administration page a relevant password.
- Go to CLI > System package and enter a relevant password.

For more details on this, refer to the **Configuring the password** section in the Management Guide.

Password management can be performed using the Westermo Device Management Platform Activator, which allows for periodic updates of passwords. Further details are provided in section 5.13.

5.6 Certificates

It is always recommended to use certificates instead of traditional text-based passwords, as they offer a more robust and scalable solution for securing device access. Certificates rely on asymmetric cryptography, where a private key (stored securely on the device, such as in a Trusted Platform Module (TPM)) and a public key (shared as part of the certificate) are used for authentication. This method greatly reduces the risk of password theft, brute-force attacks, or credential reuse, as there is no password transmitted or stored in plain text.

The inclusion of an on-board TPM enhances this security model by securely generating, storing, and managing cryptographic keys. The TPM ensures that the private key associated with the certificate never leaves the hardware, mitigating risks associated with key extraction or malware attacks. When a device attempts to authenticate, the TPM uses the private key to sign a challenge, which is then verified by the corresponding public key in the certificate, ensuring that only authorised devices with the proper credentials can gain access.

Additionally, Merlin Series routers offer SCEP functionality for certificate auto-enrolment and renewal, which facilitates device integration with advanced PKI systems.

For more information on configuring certificate-based authentication and TPM integration, refer to the relevant sections in the Management Guide.

To upload a certificate or configure SCEP:

- Go to WebUI > Security > Certifcates.

5.7 User management

Role	*Implementation*	*Privileges and Responsibilities*
1st Line Support Personnel	Configured as Web Users with access restricted to the web interface and specific status pages, along with access to a process page.	Enabled to gather logs, conduct basic investigations, and optionally restart services via the process page.
2nd Line Personnel	Configured as Web Users with access restricted to the web interface and specific configuration pages.	Their access list inherits 1st line personnel rights and is extended to include additional service configuration pages. This allows them to edit configurations, restart services, or access the device as needed
3rd Line Administration Personnel	Configured as Web Users and Linux Users with unrestricted access.	Grants administrators' full control over all aspects of the device.

The Merlin Series device defines one system user, "root," by default, which cannot be disabled or removed. The device does not define nor hardcode any other on-device usernames or roles. It is the responsibility of the end-user to scope, design, and implement User Management configurations that adhere to organizational and management requirements. Furthermore, it is recommended to disable any remote access capabilities for the system user.

The table above illustrates typical roles, implementation method along with their corresponding privileges and responsibilities.

User Management package creates restricted users accounts and provides means for local access control. For more details, refer to the Management Guide document.

To configure local users:

- Go to CLI User Management package.

5.7.1 Remote Access Control (AAA Services)

Local Access Control, as discussed in the earlier section, does not require any additional services and can be configured directly on the device. It offers complete flexibility and fine-grained control over access rights. However, for recommended and more advanced scenarios, the use of third-party AAA services such as RADIUS or TACACS+ is advised.

For networks where web services are not permitted and authorisation service is necessary, the TACACS+ module is recommended. This module allows for user authentication and provides the capability to authorise each individual command a user attempts to execute. In such cases, the router's configuration is limited to enabling and directing traffic to the TACACS+ service. The actual authorisation settings, including the list of permitted commands, are managed on the TACACS+ server itself.

The remote access control services are configurable via se configurations are outside the scope of the router’s Management Guide documentation.

To configure remote access control interace:

- Go to WebUI > System > System and configure PAM Authentication section.

5.8 Firewall

Westermo Ireland LTE routers use Netfilter (commonly known as iptables) for packet filtering, NAT, and general traffic handling. The system is configured through the UCI interface, which simplifies setup by hiding the complexity of the underlying packages.

Westermo Ireland devices are highly configurable, giving users a lot of flexibility. However, making changes outside the recommended configuration methods may lead to unexpected behaviour.

The firewall is zone-based type. Users must assign physical or logical interfaces to zones. These zones are used to define and apply traffic rules, including:

- Forwarding rules between zones (interfaces)
- Blocking rules for incoming or outgoing traffic
- Traffic redirection and NAT rules

If an interface is not assigned to any zone, default settings will apply.

The default configuration includes two predefined zones: LAN and WAN. These come with non-restrictive settings to simplify initial access. It is the end user's responsibility to implement firewall rules according to their local security and networking requirements.

It is recommended to start with a "block-all" approach and then gradually allow only the required connections or conduits in selected zones.

For more advanced configurations, it is recommended to use logical interfaces (commonly known as loopbacks) in separate zones and control the connectivity between them.

The next sections will briefly explain how to lock down device access using the firewall.

5.8.1 Firewall lock down

The traffic **Flow** in Firewall is distinguished by the following concepts:

INPUT – traffic trying to reach the router itself through a specific zone

OUTPUT – traffic originating from the router and going out through a specific zone

FORWARD – traffic passing between different zones

Firewall **Actions** are applied to this traffic. The available actions are:

ACCEPT – allows the traffic to pass through

DROP – silently discards the traffic without notifying the sender

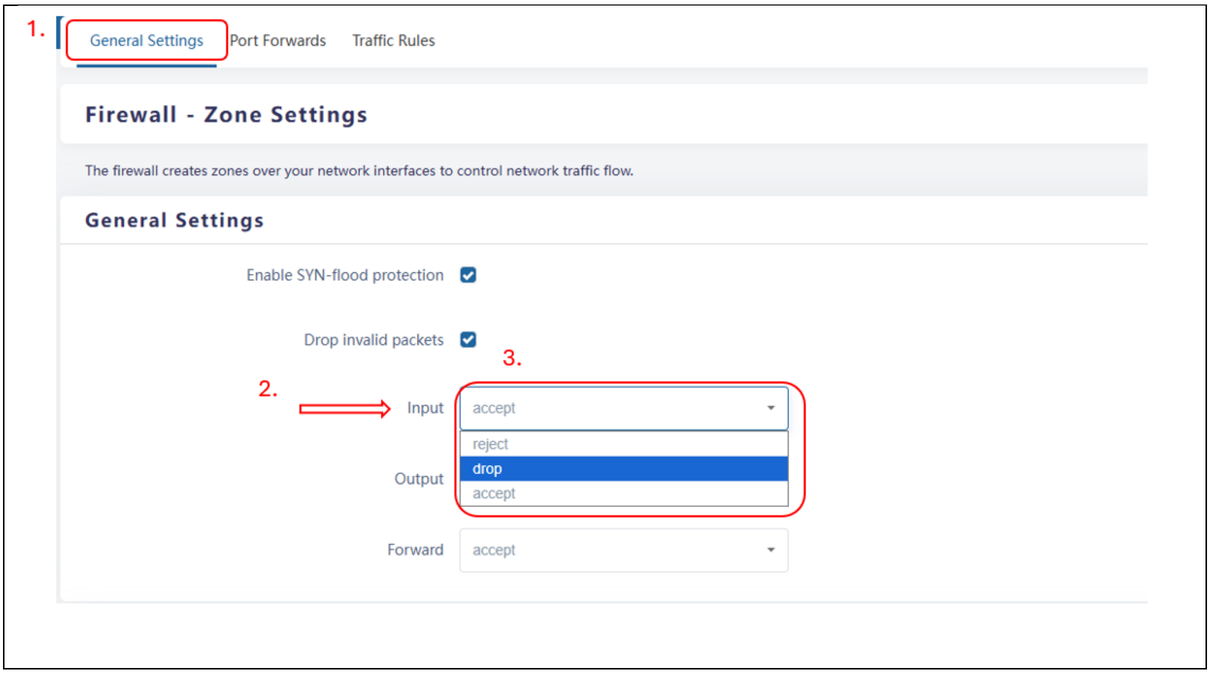
REJECT – blocks the traffic and sends an error response back to the sender

Note: Using DROP is generally recommended because it provides no feedback to the sender, making it harder for attackers to determine whether a device/service is present or filtering traffic. In contrast, REJECT informs the sender that the traffic was blocked, which may reveal information about the network setup.

5.8.1.1 Default settings

Note: Changing firewall rules may result in loss of connectivity. Users should proceed with caution and be aware of the impact of their changes. Factory reset procedures are described in the Management Guide.

Default settings apply to the traffic that has not been allocated to any zone. To access Firewall WebUI settings, from main WebUI window go to Security > Firewall.



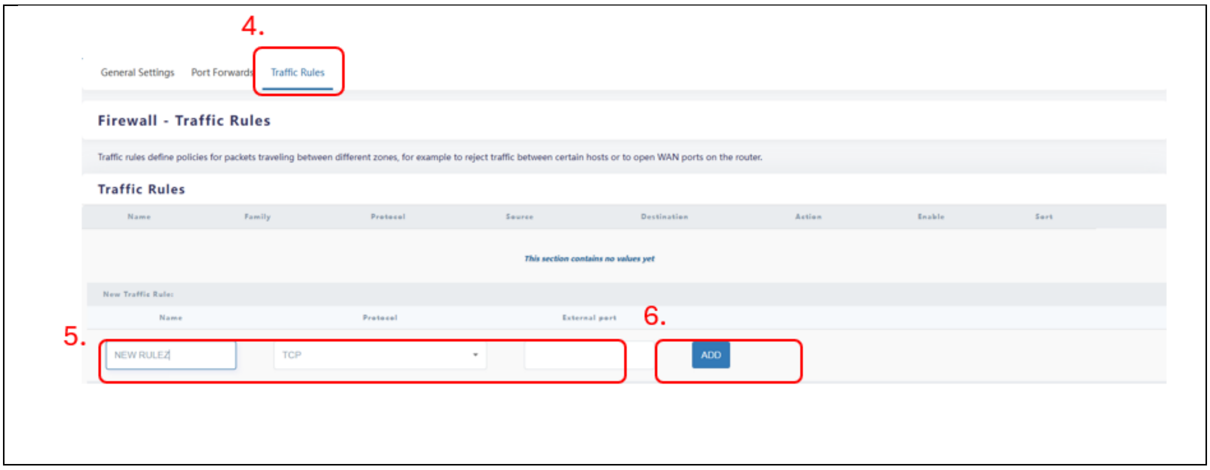
1. In **General Settings** tab.
2. Select Traffic Flow e.g. **INPUT**.
3. From drop down menu, select default Action e.g. **DROP**.

5.8.1.2 Zone settings and adding new rule

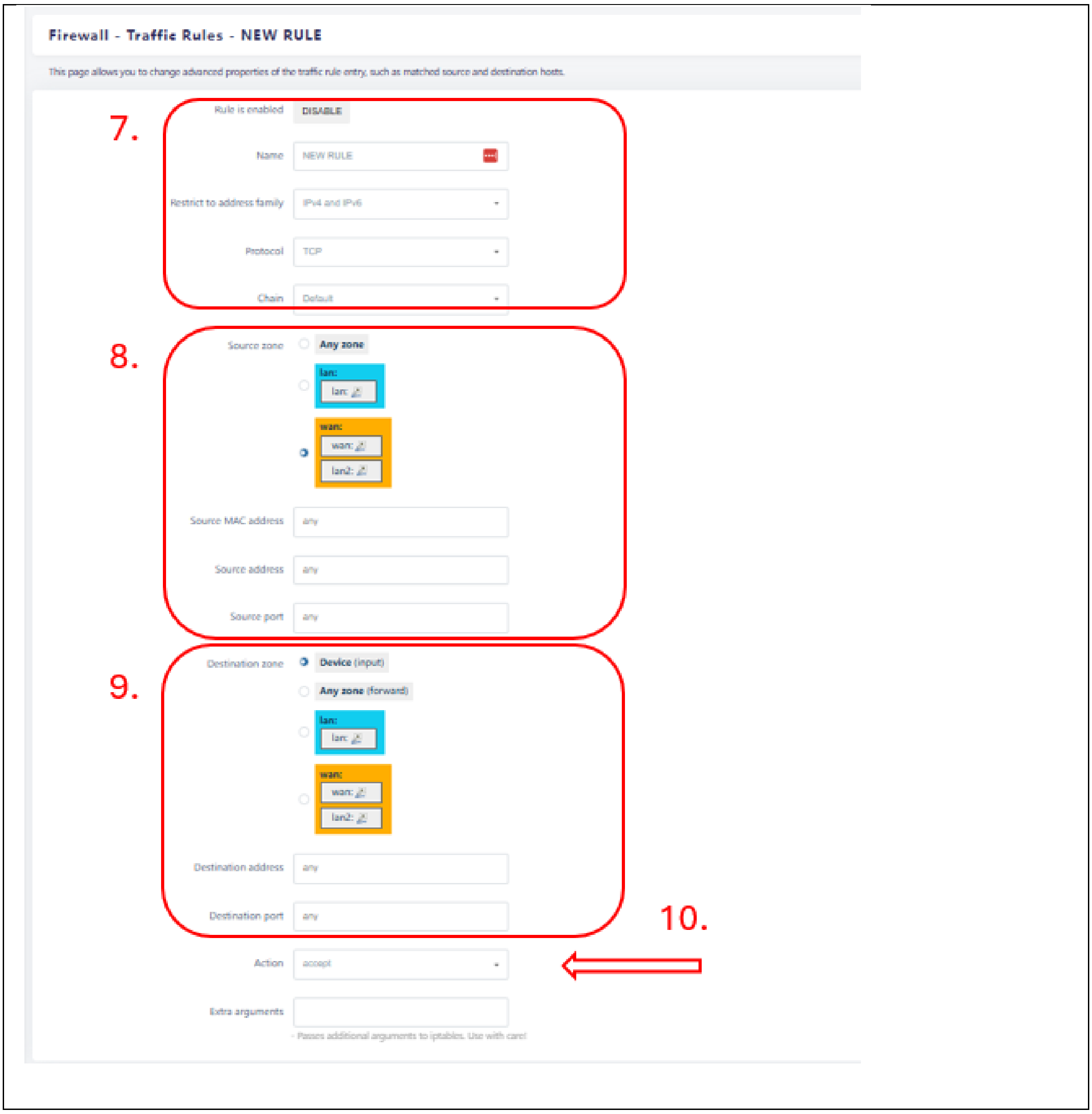
Zone settings are located below general settings on the Firewall landing page.

1. To add new zone, click **ADD** and follow instructions.
2. To modify Traffic Flow and Action settings, use the Dropdown selectors.
3. To access detailed ZONE setting, click **EDIT** on the right-hand side.

Assuming the WAN zone has been configured to drop all incoming traffic by setting the **INPUT** flow to **DROP** action, the next step is to create a rule that ensures continued access to the **WebUI** after saving the configuration.



4. Go to **Traffic Rules** tab.
5. Configure new rule's name e.g. **NEW RULE**.
6. Click **ADD.** This will open new form with detailed instructions.



7. In the **New Rule** form, adjust general settings.

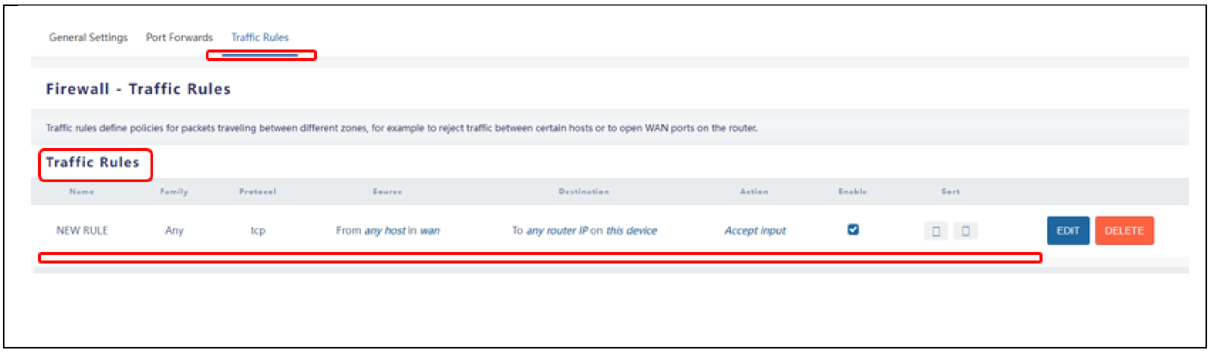
   7. In the **Source** section, specify parameters for the traffic arriving at **WAN** zone.

   8. In the **Destination** section, define the traffic is targeting **port 80 (HTTP)** or **443 (HTTPS)** to access the **WebUI**.

8. In the **Action** section, since the default behaviour of **WAN** zone has been changed to **DROP**, this rule must explicitly allow the specified traffic. Select **ACCEPT** as the action.

Click **Save & Apply** of your new configurations at the bottom of the page.

Repeat for additional connections or services as needed.



The newly added rule will appear in the traffic rules section.

Note: the placement of each rule is essential, as rules are matched in a top-to-bottom sequence; therefore, the most specific rules should be listed first. To adjust the position of any rule, use the buttons in the Sort column.

5.8.1.3 IPSec Firewall settings

When using **IPSec**, additional firewall rules may be required depending on the specific setup. The number and type of rules will vary based on the following factors:

- Whether IPSec traffic always originates from the router side
- Whether **DPD (Dead Peer Detection)** is configured
- Whether the network uses **NAT-T (NAT Traversal)**

In a scenario where all traffic originates from behind the router, no extra rules are needed.

However, if traffic needs to be sent from a **remote subnet**, the following firewall rules should be added:

1. A rule to allow **ESP (Encapsulating Security Payload)** traffic to pass through
2. A rule to allow the **decrypted traffic** to be forwarded

```
config rule
	option name 'ESP'
	option target 'ACCEPT'
	option src 'wan'
	option proto 'esp'
	option enabled '1'

config rule
	option name 'Allow-Decrypted'
	option src 'wan'
	option target 'ACCEPT'
	option proto 'all'
	option extra '-m policy --dir in --pol ipsec'
```

For networks that use NATT, the esp rule will need to be replaced with a port 4500 rules as below.

```
config rule
        option name 'NATT-4500'
        option target 'ACCEPT'
        option src 'wan'
        option dest_port '4500'
        option proto 'udp'
        option enabled '1'
```

Note: if DPD is configured, this port will be kept open via conntrack.

5.9 Network segmentation (VRFs and VLANs)

Network segmentation is fundamental in securing any network, segmentation is limiting the exposure and accessibility of devices to only the expected nodes or networks. It helps reduce the attack surface and contain potential breaches. Segmentation should be applied on a per-service basis to further minimise the impact of potential security incident.

The specific segmentation strategy depends heavily on the device's operational environment and other factors that should be identified during the system design and architecture phases.

Westermo Ireland routers support industry-standard solutions for network segmentation:

- VLAN (Virtual LAN) for Layer 2 segmentation
- VRF (Virtual Routing and Forwarding) for Layer 3 segmentation

The choice between VLAN and VRF depends on the type of services and applications running on the network or device. VLANs are ideal for separating traffic within the same broadcast domain, while VRFs are particularly useful in multimodal use cases where complete routing isolation is required. VRFs create separate virtual routing tables, making them the preferred option for advanced network designs.

When using VLANs, each segment can be treated as a separate logical network, even if they share the same physical infrastructure. This allows for better control over traffic flow and access policies. VLAN tagging (IEEE 802.1Q) enables traffic from multiple VLANs to traverse shared links more securely.

VRFs, on the other hand, allow multiple instances of routing tables to coexist on the same router. This is especially useful in scenarios where different services or tenants require isolated routing domains, such as in critical infrastructure or multi-tenant environments.

Note: Multiple VLANs can be nested in a single VRF.

For more information on configuring VLAN and VRF, refer to the relevant sections in the Management Guide.

5.10 Local services

It is recommended to avoid enabling, or leaving enabled, any unused services or ports. Configuration should follow a "minimum-on" approach, meaning that anything not actively required should be completely removed from configuration files. This strategy significantly reduces the number of running services and limits potential cyber-attack vectors.

To identify open ports and active services, tools such as port scanners or the onboard CLI commands **netstat, top, ps** can be used. Any open port may indicate a running service, and appropriate action should be taken to disable or secure it.

Particular attention should be given to reviewing user-space configurations, especially network settings, to ensure that all unused ports are disabled. In many cases, default configurations bridge all LAN ports, which may be unnecessary, especially in environments where only a single port is required for operation.

Disabling unused interfaces, services, and ports not only improves security posture but also simplifies system management and reduces the risk of misconfiguration. This is especially important for devices deployed in remote or critical infrastructure environments, where exposure to external networks must be tightly controlled.

Example: The CLI **top** command displays running processes and their resource usage.

```
Mem: 92624K used, 138944K free, 376K shrd, 8684K buff, 27780K cached
CPU:   0% usr   0% sys   0% nic  99% idle   0% io   0% irq   0% sirq
Load average: 0.02 0.04 0.00 2/115 28483
  PID  PPID USER     STAT   VSZ %VSZ %CPU COMMAND
   41     2 root     SW       0   0%   0% [kworker/0:1]
28483 20561 root     R     1324   1%   0% top
 3843     1 snmp     S     5044   2%   0% /usr/sbin/snmpd -Lsd0-6 -p /var/run/s
13719     1 iecd     S    12028   5%   0% /usr/sbin/iecd
 4462     1 root     S N   7724   3%   0% /usr/sbin/uhttpd -f -t 60 -T 30 -R -p
 1962     1 root     S     5104   2%   0% /usr/sbin/va_eventd
```

5.11 Local communication – 802.1x

802.1X can be used to authenticate host devices attempting to connect to the router's wired LAN or wireless WLAN interfaces. This adds an important layer of access control, ensuring that only authorised devices are permitted to communicate with the network.

802.1X is an IEEE standard for port-based network access control. It uses the Extensible Authentication Protocol (EAP) to exchange credentials between three components: the client device (known as the supplicant), the network switch or access point (the authenticator), and a backend authentication server (typically RADIUS). This process ensures secure authentication before a device is granted access to the network.

Implementing 802.1X helps prevent unauthorised access, supports centralised credential management, and is especially valuable in environments where strong identity verification is required. A practical example of 802.1X usage would be enforcing authentication during a maintenance site visit. In such a case, a service engineer's laptop would need to be provisioned with a certificate to establish Layer 2 connectivity with the device. The same principle can be applied to modern RTUs that support 802.1X, further strengthening the security of remote-site LAN networks.

For more information on configuring 802.1X, refer to the relevant sections in the Management Guide.

5.12 Logging and monitoring

Effective logging and monitoring are essential for maintaining visibility into system activity, detecting security anomalies, and supporting troubleshooting and compliance efforts. In general, monitoring can be used to track interface statuses, uptimes, and all other operational parameters of the device. Westermo Ireland routers offer several standard mechanisms to support these functions.

SNMP (Simple Network Management Protocol) is supported in read-only mode (GET/GETBULK). This allows external monitoring systems to query device status and performance metrics without the risk of altering configurations.

Syslog is supported for forwarding all logs to a remote server, enabling centralised collection and analysis of system events.

The **VA_Eventd** application acts as an onboard filter for Syslog messages. It allows users to define custom filters, referred to as Events. When a defined Event finds a match in real-time syslog data, an alert is triggered and sent to a remote historian service. VA_Eventd can deliver these alerts via Syslog, SNMP, email, or SMS. This application is particularly useful in bandwidth-constrained environments or where it is necessary to reduce log noise and focus on critical events.

For detailed guidance on configuring Syslog, SNMP, and VA_Eventd, refer to the relevant sections in the Management Guide.

5.13 Device management

Secure and centralised device management is essential for maintaining operational efficiency, reducing human error, and strengthening cybersecurity posture. Westermo Ireland's solution for this is Activator, a purpose-built platform developed in-house since the early 1990s. It forms the foundation of the company's Zero-Touch deployment methodology and has been successfully deployed in large-scale projects managing over 20,000 devices.

Activator's primary role is to automate secure provisioning and post-provisioning services. Devices are shipped to remote sites with minimal configuration, and once installed, Activator automatically and securely updates their configuration settings. This eliminates the need for direct user interaction with field devices, significantly reducing the risk of misconfiguration and unauthorised access.

By acting as a management proxy, Activator isolates the device environment from external networks and users. It becomes the central point of control, enforcing consistent policies and limiting access paths—thereby narrowing the scope for potential attack vectors.

Activator is highly scalable and supports automation. It manages scheduled configuration changes and software updates across the infrastructure, reducing operational costs and minimising human-to-device contact, which is critical for maintaining cybersecurity in remote and industrial environments.

The system also supports integration with third-party tools and protocols, including RESTful APIs, allowing external systems to feed and orchestrate via Activator.

For more information on Activator and integrating it with your infrastructure contact support.ie@westermo.com

5.14 Cryptography

Cryptography is the science of securing information by transforming it so that only authorised parties can access it. In network devices, cryptography is used to protect data confidentiality, ensure data integrity, and authenticate users and devices.

There are several types of cryptographic algorithms (ciphers) used in Merlin Series routers:

- **Encryption ciphers**: Protect the confidentiality of data by making it unreadable to unauthorised users (e.g., AES256).
- **Integrity ciphers**: Ensure that data has not been altered in transit (e.g., SHA-2 family, HMAC).
- **Authentication algorithms**: Verify the identity of users or devices (e.g., RSA, ECDSA, X.509 certificates).
- **Key exchange algorithms**: Securely establish shared keys between parties (e.g., Diffie-Hellman, ECDH).

Major packages and features where cryptography can be configured:

- **SSH**: Used for secure CLI access.
- **WebUI**: Secures web-based management via HTTPS.
- **IPsec**: Provides VPN encryption for data in transit.
- **802.1X**: Authenticates devices on wired and wireless networks.
- **SCEP**: Automates certificate enrolment and management.

Note:

- AES (Advanced Encryption Standard) is recommended for all new deployments.
- SHA-1 and 3DES are supported for legacy compatibility but should be avoided in new configurations.
- X.509 certificates are always recommended over standard passwords.

For detailed configuration steps and the latest list of supported algorithms, refer to the relevant package documentation and the Management Guide.

5.14.1 IPSec - IKEv2 algorithms

<table>
<tr><th>Cryptography</th><th>Algorithms</th></tr>
<tr><td>Encryption</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>DES -3DES</td><td>56-168</td></tr><tr><td>AES</td><td>128-256</td></tr><tr><td>Blowfish</td><td>128-256</td></tr></table></td></tr>
<tr><td>Hasher</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>SHA</td><td>128-512</td></tr><tr><td>MD5</td><td>128</td></tr></table></td></tr>
<tr><td>DH-Group</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>MODP</td><td>768-8192</td></tr><tr><td>EPC</td><td>192-521</td></tr></table></td></tr>
<tr><td>PRF</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>HMAC_MD5</td><td>128</td></tr><tr><td>HMAC_SHA1</td><td>160</td></tr><tr><td>HMAC_SHA2</td><td>256-512</td></tr><tr><td>KEYED_SHA1</td><td>160</td></tr><tr><td>AES128_XCBC</td><td>128</td></tr><tr><td>FIPS_SHA1</td><td>160</td></tr></table></td></tr>
<tr><td>Digital Signature</td><td><table><tr><td>Description</td></tr><tr><td>RSASig</td></tr><tr><td>ECDSA</td></tr></table></td></tr>
</table>

5.14.2 SCEP algorithms

Cryptography	Algorithms

<table>
<tr><td>Encryption</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>DES 3DES</td><td>56-168</td></tr><tr><td>AES</td><td>128-256</td></tr><tr><td>Camellia</td><td>128-256</td></tr></table></td></tr>
<tr><td>Digest</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>SHA</td><td>128-512</td></tr><tr><td>MD5</td><td>128</td></tr></table></td></tr>
<tr><td>Signature</td><td><table><tr><td>Description</td><td>Length (bits)</td></tr><tr><td>SHA</td><td>128-512</td></tr><tr><td>MD5</td><td>128</td></tr></table></td></tr>
</table>

5.14.3 HTTPS (UHTTPD) algorithms

<table>
<tr><th>Cryptography</th><th>Algorithms</th></tr>
<tr><td>1.0</td><td><table><tr><td>Description</td></tr><tr><td>TLS_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>TLS_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td></tr><tr><td>TLS_RSA_WITH_RC4_128_SHA</td></tr><tr><td>TLS_RSA_WITH_RC4_128_MD5</td></tr><tr><td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td></tr></table></td></tr>
<tr><td>1.1</td><td><table><tr><td>Description</td></tr><tr><td>TLS_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>TLS_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td></tr><tr><td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td></tr></table></td></tr>
</table>

1.2	Description TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
1.3	Description TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_8_SHA256 TLS_AES_128_CCM_SHA256

5.14.4 SNMP algorithms

Cryptography	**Algorithms**
Hasher (auth_proto)	Description: Length (bits) SHA: 128-512 MD5: 128
Encryption (priv_proto)	Description: Length (bits) DES: 56 AES: 128-256

5.14.5 IEEE 802.1X algorithms

Cryptography	**Algorithms**

TLS	Description TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
PEAP	Description TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384
TTLS	Description TLS_AES_128_GCM_SHA256 TLS_CHACHA20_POLY1305_SHA256

5.14.6 SSH algorithms

Cryptography	**Algorithm**	
Cipher	Description	Length(bits)
	aes128-ctr	128
	aes256-ctr	256
	chacha20	256
Host Key Algo	Description	Length(bits)
	ssh-rsa	128
	rsa-sha2-256	256
	ssh-ed25519	256
Key Exchange Algorithms (KEX)	Description	Length(bits)
	curve-ed25519	256
	DH14-sha1	2048
	DH14-sha256	2048

5.14.7 TPM algorithms

Cryptography	**Algorithm**

Encryption	Description / Length(bits): AES 128-256; ECC 256-521; RSA 1024-2048
Hasher	Description / Length(bits): SHA 128-512
DH Groups	Description / Length(bits): ECDH 256-521

5.15 Storage (Data-at-Rest)

Flash Memory: Overlay encryption is a method used to protect user space content—such as configuration files and private keys—from potential threats by storing this data in encrypted form on flash memory. This approach provides protection against external hardware-based attacks.

By default, user space content remains unencrypted; users must enable overlay encryption according to their local requirements. While encrypted storage may result in minor performance and boot time impacts, these are typically negligible for standard installations.

Instructions for configuring overlay encryption are detailed in the Management Guide.

Note: The security seed for encryption is automatically generated, unique to each device, and safeguarded by an onboard TPM chip.

Important: Storage decryption is not supported. Disabling the encryption feature requires erasing the device's storage and restoring factory settings, which will result in the loss of all current user space data.

Trusted Platform Module (TPM) is an onboard hardware chip that functions as a secure, isolated storage solution for certificates primarily used in securing communications such as VPN and TLS connections. The TPM safeguards the private key associated with each certificate by ensuring it remains within the hardware itself, thereby reducing vulnerabilities related to key extraction or malware threats. It is strongly recommended that users prioritize the use of TPM-integrated certificates over conventional text-based passwords.

6 Vulnerability Management

6.0 Purpose

This section outlines Westermo Ireland's policy and procedures for managing product vulnerabilities in Merlin series routers. It ensures compliance with IEC62443, ETSI EN 303 645 and supports Coordinated Vulnerability Disclosure (CVD) practices specified in ISO/IEC 29147, ETSI TR 103 838 and defined by PSIRT Services Framework (First.org)

6.1 Vulnerability reporting and disclosure

Westermo Ireland Vulnerability Disclosure Policy:

- **Contact information** for reporting issues:
  - Dedicated PSIRT email for Merlin devices: PSIRT.ie@westermo.com
  - Westermo group: https://www.westermo.com/support/report-vulnerability
- **Timelines** for initial acknowledgement of receipt (within 7 days).
- **Status updates** provided at regular intervals until resolution.

Reports may originate from:

- Security researchers
- Industry peers
- Internal testing
- External penetration testing

All reports are evaluated using CVSS and EPSS scoring methodologies and prioritised in accordance with the Known Exploited Vulnerabilities (KEV) index and established internal vulnerability management qualification criteria.

6.2 Coordinated vulnerability disclosure (CVD)

Westermo Ireland is committed to supporting Coordinated Vulnerability Disclosure (CVD) and Multi-Party Coordinated Vulnerability Disclosure (MPCVD) practices. The company differentiates between single-product and systemic vulnerabilities to ensure appropriate and effective handling.

6.2.1 Handling of Vulnerabilities

- Single-Product Vulnerabilities: These are addressed directly with the relevant stakeholder to facilitate a prompt and focused response.
- Systemic Vulnerabilities: Issues affecting broader systems or multiple parties are escalated to competent industry bodies, such as the GSMA or the IoT Security Foundation, to coordinate an industry-wide response.

6.2.2 Vulnerability Disclosure Mechanisms

Vulnerability disclosures are primarily communicated through Release Notes documents. In cases where vulnerabilities are deemed critical, Security Advisory Statements (SA) are published at https://www.westermo.com/support/security-advisories.

6.2.3 Disclosure Policy and Information Minimisation

Given that Westermo devices are predominantly used within critical infrastructure environments, the company's disclosure policy is designed to limit the amount of information released. This minimisation strategy is intended to prevent potential adversaries from exploiting CVD processes or using the information gathering platform for malicious purposes.

6.2.4 Contents of Published Security Advisories

- Affected software versions
- Vulnerability description
- CVE reference (if applicable)
- Mitigation steps (if applicable)

Release Notes documents provide comprehensive information about all software changes, including both security and vulnerability fixes. These Release Notes are considered the primary channel for vulnerability disclosure.

6.3 Vulnerability remediation timelines

Westermo Ireland commits to:

- **Software fixes** within 90 days of disclosure based on criticality, including new image creation, regression testing, and release.
- **Hardware fixes** are addressed based on complexity and deployment feasibility.

6.4 Continuous software composition monitoring

Westermo Ireland:

- Maintains a **Software Bill of Materials (SBOM)** for all Merlin products.
- Uses industry recognised tools for software composition scanning and risk assessment.
- Monitors for vulnerabilities throughout the defined support period and beyond, as where feasible.

7 Security Policies and Practices

This section provides a basic, non-exhaustive example of typical security and operational policy considerations, intended solely as a guidance reference.

The content shall be used as a general guide only, and does not constitute a recommendation, instruction, or endorsement of any specific configuration or security controls.

To the maximum extent permitted by applicable law, Westermo Ireland Ltd. shall not, under any circumstances, be held liable for loss of profits, data, business opportunity, or for any incidental, indirect, or consequential damages arising from the use of this material, even if advised of the possibility of such damages.

All policies, configurations, and security decisions remain the responsibility of the implementing organization and its authorized administrators.

7.0 Network Equipment Policy – Basic Example

Configurations will typically be carried out in collaboration with cross-functional teams, including Design/Architecture, Operations, Monitoring (including Security), and Critical Operations and Services.

Network equipment shall only be installed after the successful completion of:

- All provisioning procedures,
- Acceptance testing as defined by local requirements,
- Required on-site or production security verification testing,

including appropriate security validation within the live production environment, where applicable.

All equipment shall be configured to meet the following minimum standards:

a) Communications and Cryptographic Controls

- Configure all remote communication channels to use secure ciphers, including:
  • minimum AES-256 encryption
  • minimum SHA-2 family hashing
  • digital signatures
- Enable and configure X.509 digital certificates where supported.
- Integrate certificate operations with a Certification Authority (CA) where possible.

b) Ports, Protocols and Services

- Disable unused physical ports.
- Disable all non-essential services.
- Enable only required secure services: SSH, HTTPS, VPN, SNTP, SNMPv3*.
- Disable all insecure or unencrypted services, including HTTP.

- Ensure that no unsecured services are accessible outside of the VPN, unless explicitly approved.

c) Logging

- Forward all system logs to a centrally managed Remote Syslog server.
- Enable and configure local security event processing and alarms (e.g., VA_EVENTD).

d) Monitoring

- Integrate equipment into the Monitoring Platform.
- Configure monitoring for operational, performance, and security-related events.
- Create severity-based notifications.
- Implement physical anti-tampering monitoring (e.g., Digital Input).

e) Authentication and Access Control

- Define a user management policy with separate privilege levels.
- Configure superuser passwords in accordance with local security requirements.
- Define a password management policy, including password lifetime and complexity.
- Configure device access notifications (login/session alerts).
- Enable centralized authentication via AAA.
- Enable centralized authorization (e.g., TACACS+).
- Apply security warning banners to all management access interfaces.

f) Network Segmentation / Firewall-Specific Settings

- Define and enforce filtering and access permissions for the firewall.
- Apply a default-deny inbound model (allow only explicitly required traffic).
- Utilize firewall zone-based separation.
- Introduce VLAN/VRF segmentation (if applicable).
- Introduce port forwarding (if applicable and required by design).

g) Backups

- Define and implement a configuration backup policy.

h) Redundancy

- Define and implement a redundancy and resiliency policy.

i) Firmware / Software

- Define and implement a remote update policy.

j) Inventory, Commissioning and Decommissioning policy

- Define and implement inventory management policy.

7.1 Cyber Security Management System (CSMS)

The security performance of any product is determined by technical operations, management quality systems, and the processes, procedures, and policies in place. It is the responsibility of user organizations to maintain the cybersecurity environment and implement their processes in a clear and approachable manner. The IACS Cyber Security Management System (CSMS), derived from IEC 62443-2-1, lists following policies as mandatory.

Cyber Security Management System (CSMS)
General Security Policy
Risk Management Policy
Management Of Change Policy
Personnel Security Policy
Audits
Information Management Policy
Reference Architectures
Access Management and Control
Boundary Device Criteria
Personnel Security Management
Cybersecurity Incident Response
Malware Protection
Management of Change
Cybersecurity Training
Cyber Asset Management
Zone & Conduit Criteria
Cybersecurity vulnerability & risk assessment process
Business Continuity
Key Performance Indicators
Wireless Security
Security Commissioning for IACS and Electrical Systems
Access Administration Procedure
High Level Risk Assessment Procedure
Cybersecurity Factory Acceptance Testing (CFAT)
Cybersecurity Site Testing (CSAT)

Backup & Restore Procedures
Management of Change
Human Resource Security Procedure
Incident Response Procedure
Management of Functional Lifecycle ICS Cybersecurity
Communication / Data Flow Analysis Procedure
Design Vulnerability Assessment Procedure
Detailed Level Risk Assessment Procedure
Security Level Verification Procedure
Countermeasure Inspection & Test Procedure
Patch Management Procedure
Anti-virus Update Procedure
Job Cyber Assessment Procedure
Training Management Procedure
Audit/Compliance Procedures
Site Cybersecurity Vulnerability Assessment Procedure
Cybersecurity Vulnerability Assessment Revalidation Procedure