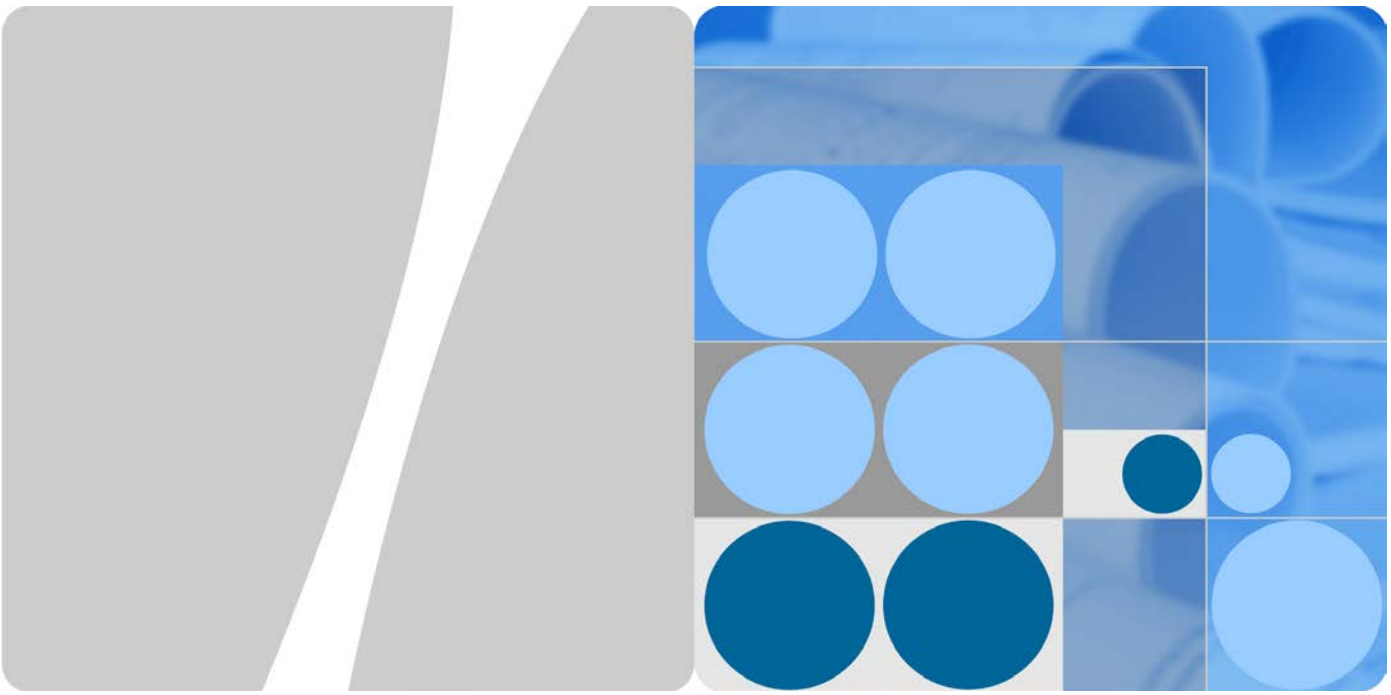

HUAWEI ROUTER SECURITY CAPABILITIES FOR NERC CIPv5

Issue 01

Date 2018-08-01

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the commercial contract made between Huawei and the customer. All or partial products, services and features described in this document may not be within the purchased scope or the usage scope. Unless otherwise agreed by the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 HUAWEI ROUTER SECURITY CAPABILITIES OVERVIEW

HUAWEI NE router provides strong mechanisms to protect the management, control, and data planes to mitigate security threats.

1.1 Security Defense Capabilities of the Management Plane

- AAA(authentication, authorization, accounting).
- RBAC(Role Based Access Control)The management plane controls user rights based on roles to ensure that users at different levels have different rights.
- SYSLOG
- Security management channel using Simple Network Management Protocol Version 3 (SNMPv3), Secure Shell (SSH), or Secure File Transfer Protocol (SFTP)
- Advanced encryption algorithm(SHA256/AES256)
- Terminal Access Controller Access Control System (TACACS) authorization management
- Management plane access control

1.2 Security Defense Capabilities of the Control Plane

- Application layer association
- Defense against malformed packet attacks
- Routing protocol authentication
- Generalized TTL Security Mechanism (GTSM)
- Attack source tracking and alarm reporting
- CAR for packets sent to the CPU (CPCAR)

- Blacklist and whitelist
- ACL-based user-defined flow

1.3 Security Defense Capabilities of the Forwarding Plane

- Access control list (ACL)
- IPSEC
- L2/L3 MPLS VPN

2 NERC CIP V5 Requirements Analysis

Standard	Req #	Requirement	Applicable Security Measures
CIP-002-5.1 Bulk Electric System [BES] Cyber System Categorization	All	It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System (…)	Responsible Entity Organizational function
CIP-003-5 Security Management Controls	R1	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies (…)	Responsible Entity Organizational function.
	R2	Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months.	Responsible Entity Organizational function Cyber security awareness: The NE family of routers provides robust security capabilities. They are designed to be integrated into common cyber security systems and practices.
	R3	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	Responsible Entity Organizational function

	R4	The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	Responsible Entity Organizational function
CIP-004-5.1 Personnel & Training	R1 – R3	Awareness, Training and Personnel Risk Assessment	Responsible Entity Organizational function
	R2	Training	Responsible Entity Organizational function
	R3	Personnel Risk Assessment	Responsible Entity Organizational function
	R4	Access Management Program	Responsible Entity Organizational function
	R5	Access Revocation	Responsible Entity Organizational function
CIP-005-5 Electronic Security Perimeter	R1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP	Responsible Entity Organizational function The NE family routers are designed to be installed inside of an ESP. They have appropriate cyber security functionality to reside inside of an ESP.
	R1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Responsible Entity Organizational and Project Engineering function. The NE family routers are not intended to operate as an EAP, and should only be employed inside of an ESP.

	R1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default	Access to an NE router is granted through RADIUS or TACACS+ to authenticate users.
	R1.4	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	Access to an NE router is granted through RADIUS or TACACS+ to authenticate users.
	R1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	
	R2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Responsible Entity Project Engineering function.
	R2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	Responsible Entity Project Engineering function.
	R2.3	Require multi-factor authentication for all Interactive Remote Access sessions	Responsible Entity Project Engineering function.
CIP-006-5 Physical Security of BES Cyber Systems	All	All	Responsible Entity Project Engineering function.
CIP-007-5 Systems Security Management	R1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	The NE family of routers allows users with proper access to enable and disable communications ports. Note that this is a virtual disabling of the port, not a physical disabling. However, a port that is disabled will not accept incoming traffic, it will not publish outgoing traffic.
	R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	

	R2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	HUAWEI support to provide patches or new software version.
	R2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Responsible Entity Organizational function. The latest firmware versions, and documentation for the firmware versions, are always available on the HUAWEI support website.
	R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: Apply the applicable patches; or Create a dated mitigation plan; or Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Responsible Entity Organizational function. The criticality of any cyber security function improved, enhance, or added during a firmware revision will be indicated in the former release notes for the NE family.
	R2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Responsible Entity Organizational function.
	R3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Responsible Entity Organizational and Process Engineering function, for e.g. control electronic access to resources. In addition: There is no backdoor access capability through debug ports All TCP/UDP ports are closed except for those used by the configured and running applications User access policies are

			implemented through RBAC
	R3.2	Mitigate the threat of detected malicious code.	Responsible Entity Organizational and Process Engineering function.
	R3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Responsible Entity Organizational and Process Engineering function.
	R4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: Detected successful login attempts; Detected failed access attempts and failed login attempts; Detected malicious code	The NE family provides an event log locally and support to send syslog, Detected successful and unsuccessful login attempts are recorded.
	R4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): Detected malicious code from Part 4.1; and Detected failure of Part 4.1 event logging.	The NE family provides the alarms related to: Hardware and device, basic configuration, system management, interface and data link, IP routing, security and others. The NE family supports RMON for remote monitoring.
	R4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Responsible Entity Organizational and Process Engineering function. The NE family support to send syslog to the log server.
	R4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber	Responsible Entity Organizational and Process Engineering function. The NE family support to send

		Security Incidents.	syslog to the log server.
	R5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	The NE family uses RADIUS and TACACS+ for authentication, as well as user accounts for access.
	R5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Responsible Entity Organizational and Process Engineering function. The following roles exist in NE family; a given user can be assigned to a role: Management level (full rights) Configuration level(Service configuration commands are of this level.). Monitoring level(Commands of this level are used for system maintenance, such as display commands.) Visit level(Commands of this level include ping, tracert, and Telnet (commands used to access a remote device).)
	R5.3	Identify individuals who have authorized access to shared accounts.	Responsible Entity Organizational and Process Engineering function.
	R5.4	Change known default passwords, per Cyber Asset capability.	Responsible Entity Organizational and Process Engineering function. The NE family does not have passwords that cannot be changed.

	R5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	The NE family complies and exceeds all R5.5 requirements for password complexity when Local based authentication is used.
	R5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	The NE family support to configures the period after which a password expires. The Responsible Entity can meet this requirement also by using centralized RBAC and procedures enforcing the timely changes.
	R5.7	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	The NE family complies to R5.7 requirement by limiting the number of unsuccessful authentication attempts and logging unsuccessful authentication attempts.
CIP-008-5 Cyber Security Incident Response Plan Specifications	R1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Responsible Entity Organizational function.
	R1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Responsible Entity Organizational function.
	R1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Responsible Entity Organizational function.
	R1.4	Incidenthandling procedures for Cyber	Respnsible Entity

		Security Incidents.	Organizational function.
	R2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months (…)	Responsible Entity Organizational function.
	R2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Responsible Entity Organizational function.
	R2.3	Retain records related to Reportable Cyber Security Incidents.	Responsible Entity Organizational function.
	R3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response (…)	Responsible Entity Organizational function.
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan (…)	Responsible Entity Organizational function.
CIP-009-5 Recovery Plan Specifications	R1.1	Conditions for activation of the recovery plan(s).	Responsible Entity Organizational function
	R1.2	Roles and responsibilities of responders.	Responsible Entity Organizational function
	R1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Responsible Entity Organizational function
	R1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Responsible Entity Organizational function
	R1.5	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede	Responsible Entity Organizational function

		or restrict recovery.	
	R2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: By recovering from an actual incident; With a paper drill or tabletop exercise; or With an operational exercise.	Responsible Entity Organizational function
	R2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	Responsible Entity Organizational function
	R2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Responsible Entity Organizational function
	R3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery (…)	Responsible Entity Organizational function
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	Responsible Entity Organizational function

CIP-010-1 Configuration Change Management and Vulnerability Assessments	R1.1	Develop a baseline configuration, individually or by group, which shall include the following items: Operating system(s) (including version) or firmware where no independent operating system exists; Any commercially available or open-source application software (including version) intentionally installed; Any custom software installed; Any logical network accessible ports; and 1.1.5. Any security patches applied.	Responsible Entity Organizational Function.
	R1.2	Authorize and document changes that deviate from the existing baseline configuration.	Responsible Entity Organizational Function.
	R1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	Responsible Entity Organizational Function.
	R1.4	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the NE family products within a live BES Cyber System.
	R1.5.1	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected;	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the NE family products within a live BES Cyber System.

	R1.5.2	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the ML3000 family within a live BES Cyber System.
	R2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Responsible Entity Organizational and Engineering Function and Process.
	R3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Responsible Entity Organizational and Engineering Function and Process.
	R3.2	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process.
	R3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	Responsible Entity Organizational and Engineering Function and Process.

	R3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Responsible Entity Organizational and Engineering Function and Process.
CIP-011-1 Cyber Security — Information Protection	R1.1	Method(s) to identify information that meets the definition of BES Cyber System Information.	Responsible Entity Organizational and Engineering Function and Process.
	R1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Responsible Entity Organizational and Engineering Function and Process.
	R2	R2.1: Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. R2.2: Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Responsible Entity Organizational and Engineering Function and Process.