Huawei AR6120 Router

CSPN Security Target

Issue date : 07/17/2019

Version : 1.8

Revision Record

Revision Version	Change description	date	Author
1.0	Initial Version		Shilisha
1.1	Update model name and version sent to ANSSI with application form	01/18/2019	guzhenlin
1.5	Several updates and cleaning, e.g Evaluated configuration		guzhenlin
1.6	Update life cycle		guzhenlin
1.7	Submitted to the evaluation	8/05/2019	guzhenlin
1.8	Update release version	08/10/2020	guzhenlin

Table of Contents

Figures & Tables

1 Introduction

1.1 Product identification

This Security Target is for the CSPN evaluation of the Huawei AR Series Service Router AR6120 software.

Manufacturer	Huawei
Organization URL	https://www.huawei.com/en/
Product’s commercial name	AR6120
Firmware version	V300R019C00SPC007T
Product’s category	Filtering Router

1.2 Abbreviations

AAA	Authentication Authorization Accounting
ACL	Access Control List
CAP	Concurrence Accelerate Platform
CLI	Command Line Interface
LMT	Local Maintenance Terminal
LPU	Line Process Unit
RMT	Remote Maintenance Terminal
SRU	Switch Router Unit
SSH	Secure Shell
TSF	TOE Security Functions
VRP	Versatile Routing Platform
VTY	Virtual Teletype Terminal

1.3 Reference

[Crypto_spec_AR6120]	Huawei AR6120 Router Cryptographic specification
[PROC_CSPN]	First Level Security Certification For Information Technology Products, ANSSI-CSPN-CER-P-01/1.1

[CRIT_CSPN]	Evaluation Criteria for the First Level Security Certification, ANSSI-CSPN-CER-I-02/1.1
[AR6120_GUIDE]	AR6100 V300R019 Product Documentation

2 Product and TOE description

2.1 Product overview

Huawei AR Series Routers are the next-generation routing and gateway devices, which provide the routing, switching, wireless, and voice functions. Huawei AR provides a highly secure and reliable platform for scalable multiservice integration at enterprise and commercial branch offices of all sizes and small-to-medium sized businesses. It consists of both hardware and software. A router is a device that determines the next network point to which a packet should be forwarded towards its destination. It is located at any gateway (where one network meets another). A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet.

At the core the router is the VRP (Versatile Routing Platform) software deployed on MPU (Main Processing Unit), the software for managing and running the router's networking functionality. The VRP provides extensive security features. These features include different interfaces with access levels for administrators; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

VRP is supported by the Concurrence Accelerate Platform (CAP) for performance reasons. All L3 traffic that goes through the MPU goes through the Concurrence Accelerate Platform ('CAP') software first. CAP can either forward the traffic directly (if the route is known to CAP) or sends it to the VRP first. In the latter case, VRP determines the route to the destination, sends the packet back to CAP and CAP forwards it to the intended destination. The route information is then also stored on the CAP for future use.

The following figure shows the front side of the AR6120. '1' denotes USB 2.0 connectors for USB mass storage devices for external storage of audit information. '2' denotes USB 3.0 connectors for USB mass storage devices for external storage of audit information. '3' denotes the reset switch for the device

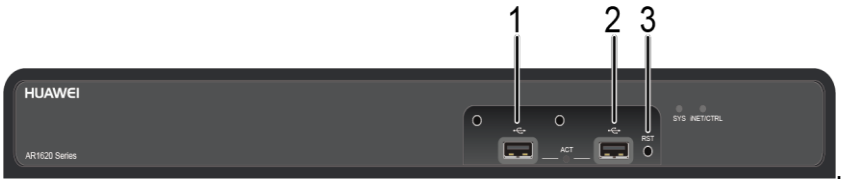


Figure 1 : Front side of the AR6120

Figure 2 below shows the back plane of the device:

- 4’ denotes two SIC slots for expansion cards,
- ‘5’ reflects the product model (i.e. AR6120),
- ‘6’ denotes an electrical ground point,
- ‘7’ denote connectors for the console,
- ‘8’ denotes two fixed GE electrical interfaces (i.e. GBit/s Ethernet connectors),
- ‘9’ denotes one fixed GE electrical interfaces (i.e. 10GBit/s Ethernet connectors),
- ‘10’ denotes one fixed GE fiber interfaces (i.e. 10GBit/s Ethernet connectors),
- ‘11’ denotes eight fixed FE electrical interfaces (i.e.100MBit/s Ethernet connectors),
- ‘12’ denotes the power jack, 13’ denotes a jack reserved for a power cable locking latch,

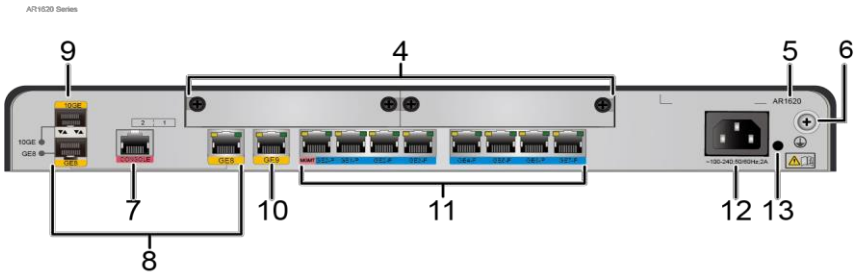


Figure 2 : Back plane of the AR6120

There are no connectors to the AR6120 on the left side, right side, bottom or top of the device.

2.2 Hardware Architecture of the AR6120

The hardware architecture of the AR6120 includes the following components:

- Processor: Hisi1213
- 512MB memory
- Two different kinds of flash, 2MB storage for bootrom and 512MB storage for software package
- 2 SIC slots
- Fixed interface: 8FE+2GE
- Forwarding Performance: 450K PPS

2.3 Software Architecture of the AR6120

The AR6120 software architecture consists of the VRP, CAP software and the underlying OS. As shown in Figure 3, the MPU hosts the components VRP and CAP. The TOE is running on the four cores of the CPU. The TOE provides several security functions which are described in more detail in chap 5.

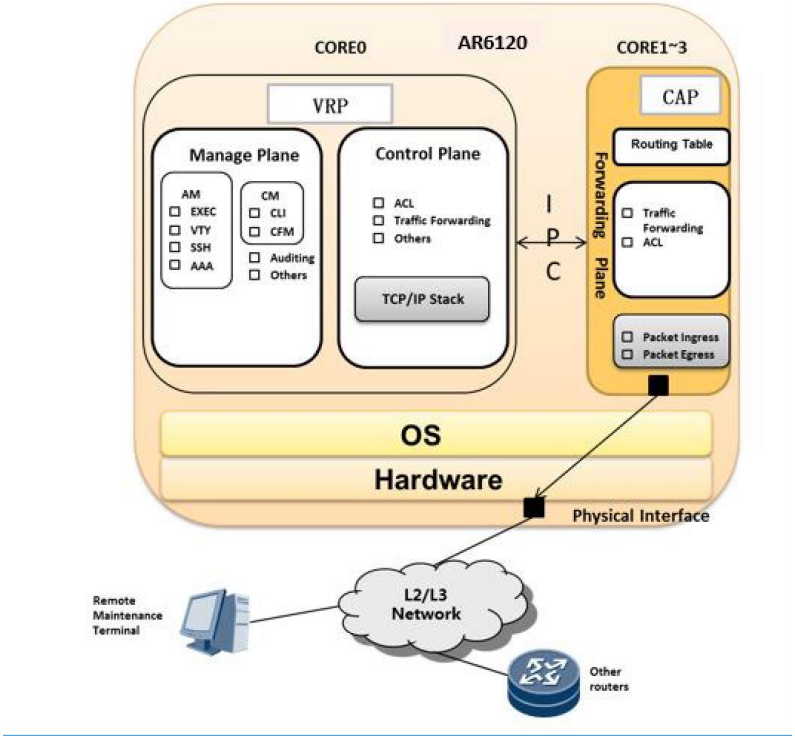


Figure 3 : AR6120 Architecture

Figure 3 reflects the basic structure of the product software architecture with respect to subsystems:

- AM: Access Management,
- CM: Command Management,
- IM: Information Management,
- OS: Operating System.

The VRP is the control and management platform that runs on the SRU (switcher routing Unit)/MCU. The VRP supports IPv4/IPv6, and routing protocols such as RIP, Border Gateway Protocol (BGP), Open Shortest Path First (OSPF). The ISIS calculates routes, generates forwarding tables, and delivers routing information to the SRU(s). The VRP includes Service Control Plane (SCP), System Manage Plane (SMP), General Control Plane (GCP) and other sub-systems.

The VRP is supported by the Concurrence Accelerate Platform (CAP) for performance reasons. VRP and CAP are relying on the underlying RTOS.

The AR6120 handles L2 and L3 traffic. Since L2 traffic is handled by the SRU itself without additional security related control or management functionality, **only L3 forwarding capabilities are within the scope of this evaluation**.

2.4 TOE features

The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in the forwarding engine of the CAP. System control and security management are performed either through an LMT (Local Maintenance Terminal connected through the console port) which is connected to the Management plane of the TOE or through RMT (Remote Maintenance Terminal) via a secure channel enforcing SSH.

The **TOE's software architecture** consists of the two logical planes to support the centralized forwarding and control and the distributed forwarding mechanism:

- Data plane
- Control and management plane

The control and management plane is the core of the entire system. The control and management unit processes protocols and signals, configures, maintains, reports and controls the system status.
The data plane is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or de-capsulates packets, forwards IPv4/IPv6 packets, performs Quality of Service (QoS) and scheduling, completes inner high-speed switching, and collects statistics.

The TOE security features are:

- **ACL filtering**: TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), in order to provide controlled communications between two networks that are physically separated. For that, the TOE offers an Access Control List (ACL) feature for filtering incoming and outgoing information flow to and from interfaces. ACL is a packet filter that filters packets based on rules, defining which traffic flow is allowed and which traffic flow if forbidden. One or more rules describe the packet matching conditions, such as the source address, destination address, and port number of packets. Details are provided in chapter 5.1
- **Authentication**: Only authenticated users can execute commands on the TOE. User identity information is configured and stored in the product. Details are provided in § 5.2
- **Access Control**: The TOE manages user privileges by access level. An access level is assigned to each user and to each command. All authenticated users with an access level equal or higher to the access level of the command are allowed to execute the corresponding command. Details are provided in chapter 5.3
- **Audit**: The VRP generates audit records for security-relevant management actions. All audit records contain not only the information on the event itself but also a timestamp and – where possible – additional information like user ID, source IP, etc. The TOE

supports the configuration of a local logging policy. It is possible, in particular, to log security and administration events. Details are provided in 5.4

- **Communication Security**: The TOE enforces communication security by implementing the SSH2.0 protocol, providing a security channel for the users accessing the AR6120 device through RMT. Details are provided in 5.5.
- **Cryptographic support**: the security features of the TOE require some cryptographic functions, e.g. scrypt, Diffie-hellman, RSA, AES and HMAC-sha2. More detailed description is provided in [crypto_spec_AR6120].

All other product functionalities not mentioned above such as IPSec implementation, or DHCP are out of the scope of the evaluation.

2.5 Product Usage

The TOE is (part of) the software of the AR6120 router product. At delivery to the user (administrator) the product is installed in a secure physical environment, initialized and configured through the console interface (LMT) by the administrator. After successful installation and configuration (secure parameter, ports, SSH keys, etc.), the router will forward the traffic of the network, filter unwanted traffic and logging all the events. Generally speaking, the router filters the traffic between three kind of networks, administrative, enterprise and public networks. The product can be accessed either through LMT (i.e. the 'console') or RMT (i.e. via virtual terminals, 'VTYs'). The product supports one console and up to 15 VTYs. All the maintenance and administrative future actions are from a secure RMT [AR6120_GUIDE].

Figure 4 below shows the operational context of the AR product. Two kind of users access the router product, the end user for which the router is transparent and the administrators, users in the enterprise intranet with specific privileges that will perform administrative and maintenance tasks.

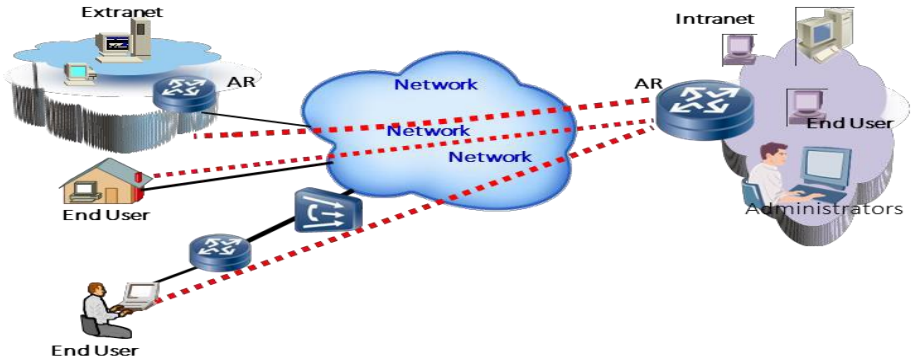


Figure 4 : Product Usage

2.6 TOE environment

The TOE environment is made of:

- All other software components interacting with the TOE for its main functionalities
- Other switches and routers used to connect the TOE for L2/L3 network forward
- Local PCs used by administrators to connect to the TOE though the command line interface, either through TOE's console interface (LMT) or TOE's ETH interface via a secure channel enforcing SSH.
- Remote PCs used by administrators to connect to the TOE for access to the command line interface through interfaces on LPU within the TOE via a secure channel enforcing SSH.

2.7 Maintenance and Vulnerability management

2.7.1 Maintenance

In terms of maintenance, when the customer/end User encounters an issue with the device operation, a assistance service is provided by Huawei. Global Technical Assistance Cent (GTAC) offer a 24-hour technical service, customer could ask for technical help by Phone and Email (**Tel:** 0080066668899, 0040-214550200, **Email:** tac_support@huawei.com). Once the problem is confirmed and rectified, the GTAC pushes related patches or firmware versions to the customer for upgrade.

Huawei also provides Huawei Online Upgrade Platform(HOUP). The device is connected to the platform through a preset certificate so that the latest patch and firmware version can be obtained and automatically upgraded (HOUP: https://houp.rnd.huawei.com)

2.7.2 Surveillance

Huawei Product Security Incident Response Team (PSIRT) manages the receipt, investigation, internal coordination and disclosure of security vulnerability information related to Huawei offerings and it is the only window to disclose the vulnerability of Huawei products. Huawei hopes that security researchers, industry organizations, government agencies and vendors can proactively contact Huawei PSIRT to report potential Huawei product security vulnerabilities.

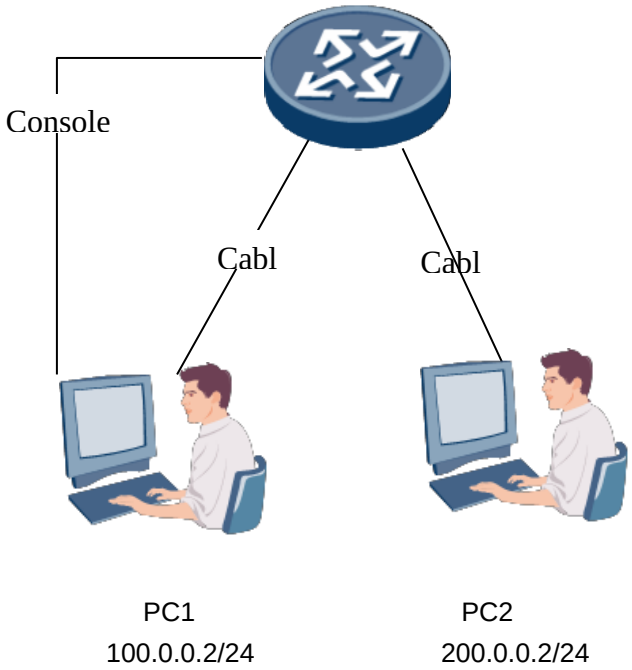
Huawei adheres to a *responsible vulnerability disclosure* common practice. Huawei will disclose the vulnerability after certain verification procedures to stakeholders such as customers, OEM partners and CERTs. Huawei will inform the impacted customers of the vulnerability through private communication or public security advisory.

Once a security flaw is confirmed by PSIRT, a DTS (Defect tracking System) workflow will be triggered. The security flaw is submitted to the DTS system that assigns a unique DTS that will make the flaw tractable during its whole life cycle. It will describe the status of the flaws, including the basic information and the problem description, such as the raise time and close time, status information, etc.

3 TOE Evaluated Configuration

3.1 Test environment

The topology of the test equipment is illustrated below:



The above topology needs the following devices and tools:

Name	Description	Version	Amount
AR	Huawei AR Service Routers(AR6120)	V300R019C00SPC0007T	1
PC	Host	OS of windows 7	2
Console cable	Cable connects to the router through the RJ45 connector	NA	2

Table 1 : Material checklist of the Test topology

Name	Description	Amount
SecureCRT	SSH client and Console Terminate Tool	1
powershell	Tool of SSH used on PC. (This tool is supported only by the Windows 10. Could be replaced by any equivalent tool).	1

Table 2 : Tools checklist of the Test topology

The tool of SecureCRT can configure the cipher and MAC with different algorithms using the advance option.

3.2 Initial configuration

The initial configuration for evaluation has the following preconditions:

1. AR configures SSH Server with SSH user password, the interface IP that connected to PC ;
2. PC configures the IP that connected to Router A

PC logins into the Router successfully and can show the files of Router through the following command:

```
<Huawei>dir
```

PC can show the system files (system software package and configuration file) of Router through the following command

```
<Huawei>display startup
```

PC can show the device status of Router through the following command

```
<Huawei>display version
notes:
Run the display version command to view the device version.
Run the display device command to view the basic device information.
Run the display memory-usage command to view the memory usage.
Run the display temperature all command to view the working temperature of a module.
```

Note: the command results attached files of “the results of device status monitoring”
Note: the version under test is V300R019C00SPC007T.

The initial configuration of Router is as following:

The following for the two interfaces.

```
#
interface GigabitEthernet0/0/0
 description to PC1
 ip address 100.0.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
description to PC2
 ip address 200.0.0.1 255.255.255.0
#
```

The following for SSH Server with SSH user of password (admin123/ huawei123).

```
#
 stelnet server enable
 ssh server rekey-interval 1
  ssh user admin123 authentication-type password-rsa
  ssh server permit interface gigabitethernet 0/0/0
#
user-interface vty 0 4
 authentication-mode aaa
  protocol inbound ssh
```

```
#
  user-interface con 0
 authentication-mode aaa
 idle-timeout 1 30
#
aaa
 local-user admin123 password irreversible-cipher huawei123
 local-user admin123 privilege level 15
 local-user admin123 service-type terminal ssh
#
```

3.3 Configuration of the main features:

- LAN feature : default configuration
  - VLAN and MAC :on
  - STP, SEP, Link,LLDP, QinQ : off
- WAN : default configuration:
  - all interfaces : on
  - Link Layer protocol, dialing, PON, Network Bridge and HDLC over TCP: off
- IP applications
  - ARP, IPv4/IPV6 adress management, TCP/UDP, ICMP, ping and tracert, UDP : on
  - IP FRR, IPv6 over IPv4 and IPv4 over IPv6 : off
  - DNS, DHCP, NAT : off
- IP routing :
  - IPv4 and IPv6 static routing functions : on
  - All other such as RIP, OSPF, BGP, PBR are off
- Multicast functionalities : default configuration : off
- QoS functionalities : default configuration : Off
- Security :
  - Local AAA
  - Raduis and TACAS : not configured
  - Firewall : default config : off
  - Traffic suppression : default config: off
  - Physical attacks protection : default config : on
  - ARP default configuration : on
  - IP security : default configuration : on
  - PKI : default configuration : on
  - HTTPS : default config : off
  - ACL: empty, to be configured
  - IPS default config : Off
- Reliability (backup) : default config : off
- Device management :
  - Information Center Monitoring : on
  - Telnet : default config : off
  - SSH
    - SSH1 disabled
    - SSH2 implemented : HMAC-SHA2, AES-128-CTR, DH14, RSA2048
  - Version Management :on

  - Mirroring, remote PoE, WEB management, Automatic deployment, energy saving management, active/standby switchover : default config: off
- Network Management services: CWMP, NTP, etc default config : off
- MPLS and VPN : default config : OFF

4 SECURITY PERIMETER

4.1 Typical Users

The users that may interact with the TOE are the following:

- **Administrator:** authenticated user that has access to administer and configure the product as well as delegate admin access control rights to Administrators. Different levels of administrators on the device have different rights, details are in 5.3
- **End User:** Typical end user accessing the network resources via a connection, End User don't need authentication.

*N*ote: From the TOE's point of view, an administrator is simply a user with specific rights, authorized to perform certain administrative actions on the TOE. Moreover, the same entity may own several user accounts corresponding to different profiles.

4.2 TOE Assets

The **information assets** to be protected are the information stored, processed or generated by the TOE:

- **Wanted L3 network traffic:** The TOE is providing network traffic processing capacity. The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds to a configured route for the destination IP address of the packet.
- **Configuration data:** Configuration data for the TOE, security functions data, such as user account information and passwords, audit records, etc.
- **Log:** The logs stored in the TOE.

4.3 Threat Model

4.3.1 Attackers

The following attackers are considered:

- Evil **Non Authorized/Authenticated User**: Unauthenticated user gains access to the TOE and authenticated user that tries to obtain a service higher than his privilege level.

4.3.2 Threats

The ARs are located between an enterprise network and a public network, functioning as the only ingress and egress for data transmitted between the two networks. The main threats are :

- **UnwantedL3NetworkTraffic:** Unwanted L3 network traffic sent to the TOE by an *Evil end user* will not only cause the TOE's processing capacity for incoming network traffic

to be consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when this traffic is sent to the Control Plane. Attackers could send too much unwanted L3 network traffic to exhaust the resources of the TOE and by that compromising L3 forwarding capabilities of the TOE. As a result, *wanted L3 network traffic* could be dropped (compromising TOE availability).

- **Unauthenticated Access**: *Evil Non Authorized/Authenticated User* of the TOE gains access to the TOE and modifies TOE configuration data without permission (Compromising TOE's asset *configuration data* integrity and availability).
- **Unauthorized Access**: *Evil Non Authorized/Authenticated User* of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. By that he could modify TOE configuration data or log information without permission (Compromising TOE's assets *configuration data* or *logs* integrity, confidentiality and availability).
- **Eavesdrop**: *Evil End User* in the admin/management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and RMT (could affect confidentiality and integrity of *configuration data*, *logs data* and availability of *wanted L3 traffic*).

4.4 Assumptions on the environment

Physical Protection It is assumed that the TOE (including any console and any USB storage device attached) is protected against unauthorized physical access. The device is assumed not to contain any residual information that could be used for an attack when it is removed from the physically protected environment (e.g. for repair by a third party or at the end of life when the device is disposed).

Network Elements The environment is supposed to provide secure and correct working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. Examples of such devices are:

- AR6120 internal LAN Switches for L2 and L3 switching
- Peer router(s) for the exchange of dynamic routing information;
- Remote entities (PCs) used for administration of the TOE.

Logs checking: It is assumed that administrators check regularly the local and remote logs produced by the device and react in accordance.

Administrators: users with administrator privileges are competent, trained and trustworthy. They follow instructions and administration manuals of the device and they are not hostile.

Network Segregation: It is assumed that the management interface in the TOE will be accessed only through intranet where the TOE is hosted. The intranet network is separate from the extranet networks where the interfaces in the TOE are accessible.

Correct Working: It is assumed that other functions, which is outside the scope of the evaluation, work correctly (including the product hardware).

5 TOE Security Functions

5.1 SF.Access Control List

To prevent unwanted network traffic, the TOE supports Access Control Lists (ACLs) to filter traffic destined to the TOE and to prevent internal traffic overload and service interruption. The TOE also uses ACLs to deny unwanted network traffic to pass through itself. When a packet flow reaches the TOE, the TOE applies the information flow security policy in the form of the an access control lists to the traffic before forwarding it into the remote network. Packet flows on Layer 3 arriving at a network interface of the TOE are checked to ensure that they conform to the configured packet filter policy.

1. The TOE supports ACLs by associating ACLs to whitelists and blacklists. This function is achieved by interpreting ACL configurations then storing interpreted values in memory.
2. The TOE supports screening and filtering traffic destined to the CPU.
3. The TOE supports ACLs, which are based on the upper-layer protocol number, the source and destination IP addresses, the source and destination port numbers, and the packet direction.
4. The TOE permits an information flow between controlled subjects if all information security attributes are permitted by ACL. Packets not matching the ACL are logged and discarded by the router.
5. The TOE restricts the ability to read, modify and delete entries in ACLs to users with insufficient access rights.

This security function counters the threat: *UnwantedL3NetworkTraffic*

5.2 SF.Authentication

The TOE can be accessed either through LMT (i.e. the ‘console’) or RMT (i.e. via virtual terminals, ‘VTYs’). The TOE supports one console and up to 15 VTYs. For managing the LMT or RMT, the user needs sufficient user level according to the TOE’s Access Control (see §5.3). For all types of terminals the user has to authenticate with username and password (AAA).
The TOE identifies users by a unique ID (ID are assigned starting from ‘1’ and incremented for each new ID assigned, only one user level can be assigned to a user account. So the user level of a user is unambiguous at any time) and enforces their authentication before granting them access to any TOE management interfaces. For managing the LMT or RMT, the user needs sufficient user level according to the TOE’s Access Control (see §5.3).

Detailed functions include:

1. The TOE supports authentication via username and password. This function is achieved by comparing user information input with pre-defined reference values stored in memory.
2. The TOE stores the following security attributes for individual uses:
    - User ID
    - User Level
    - Scrypt Hashes of passwords
    - Number of unsuccessful authentication attempts since last successful authentication
    - Time when users are logging in and logging off
3. The TOE supports the detection of 3 consecutive failed authentication attempts after the last successful user authentication, then termination of the secure channel required for authentication and blocking of the related user account for authentication for at least 5 minutes.
4. The TOE requires each user to be successfully authenticated before he can perform any other actions except authentication according to 1) when connecting to the TOE.
5. The TOE requires each user to be successfully identified before he can perform any other actions except authentication according to 1) when connecting to the device. The username is used for identification of the user.
6. The password is never stored in plaintext but a corresponding cipher text is stored in the TOE. The cipher text is the value exported using the scrypt algorithm.
7. The system checks the password complexity by default. The password must meet the following requirements:

    a) The password must contain at least six characters.

    b) The password must contain at least two types of the following characters:
        - at least one lowercase letter;
        - at least one uppercase letter;
        - at least one digit;
        - at least one of the following special characters: `~!@#$%^&*()-_=+\|[{}]; : '",<.>/? and space

    c) The password cannot be the same as the account name.

    If the password does not comply with the above rules, a warning is raised.

This security function counters the threats : *Unauthenticated Access* and *Unauthorized Access*

5.3 SF.Access Control

To prevent unauthorized access, the TOE enforces an access control by supporting the following functionalities:

1. The TOE supports the association of user levels with user IDs and the association of command access levels with commands. Only one access level number can be

associated with a command at a time and only one user level can be associated with a user, so the assignment is unambiguous.

2. The TOE supports up to 16 hierarchical access levels for users and commands. This function is achieved by storing numbers 0-15 as level in memory. It is not necessary to assign all possible access levels to commands or users. User level '0' is the lowest level and '15' is the highest level. The user level 'n+1' comprises all the access rights for user level 'n' plus the additional access rights for 'n+1' (if any) ('n' represents an integer value between 0 and 14).
3. The access policy mandates that a user can only execute a specific command if his user level is equal or higher than the command access level of the specific command.
4. The access policy mandates that a user cannot execute operations that would exceed his user level. This includes that – even if he would have sufficient user level to execute the corresponding command in general – he cannot modify user accounts of users with higher access level than his own user level. This also includes that – even if he would have sufficient user level to execute the corresponding command in general – he cannot modify the command access level of a command to a value above his own user level. As a consequence, a user could lower his own user level but not raise his own user level (under the assumption that he would have sufficient user level to perform changes to user accounts in general). This protects on the one hand higher level user accounts but also prevents users to increase their own user level.
5. The TOE requires each user to be successfully identified before he can perform any actions except authentication according to Authentication 1 when connecting to the TOE. The username is used for identification and the user level of the user is used for access control.
6. The four default hierarchical access control levels are reflected by the following table:

User level	**Level name**	**Intended Purpose**	**Commands for access**
0	Visit	Network diagnosis and establishment of remote connections.	ping, tracert, language-mode, super, quit, display
1	Monitoring	System maintenance	Level 0 and display, debugging, reset, refresh, terminal, send
2	Configuration	Service configuration.	Level 0, 1 and all configuration commands.
3~15	Management	System management (file system, user management, internal parameters, fault diagnosis …).	All commands.

This security function counters the threats: *Unauthenticated Access* and *Unauthorized Access*

5.4 SF.Audit

The TOE can provide auditing ability by receiving all types of logs and processing them according to user's configuration:

1) The TOE supports generation of audit records for the following events:
   - User login and logout
   - Adding, deleting or modifying a user account (including password reset and change of user level)
   - Password change by the user
   - Operation Authority Change
   - Session Termination
   - Adding, deleting or modifying a command group (including changes to command levels)
   - Modification of Authentication Policy
   - Resetting the TOE device to factory settings
   - Configuration of the TOE device (i.e. operation requests)
   - Modification of logging policy
2) The TOE records within each audit record the date and time of the event, type of event, subject identity (of applicable) and the outcome (success or failure) of the event. The TOE provides reliable time stamps for that purpose. Depending on the definition of the event records might include the interface, workstation IP, User ID or CLI command name.
3) The TOE supports association of audit events resulting from actions of identified users with the identity of the user that caused the event.
4) The TOE allows only authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for reading audit records) to read the audit records.

This security function supports the security management countering *all identified threats*.

5.5 SF.Communication Security: SSH

The TOE provides communication security by the following mechanisms:

1) The TOE provides mechanisms to establish a trusted path between itself and a RMT[1] using the SSH 2.0 protocol.
2) The TOE permits remote users to initiate communication with the TOE to establish the trusted path.
3) The TOE supports mechanisms to verify the validity of the authentication information of SSH and can generate evidence about that can be verified by SSH.

[1] The LMT is connected to the Management plane of the TOE directly via the Console interface and there is no traffic filtering performed for the traffic via the console port. For management through the console, no logically secured communication channel is required and authentication is always enabled.

4) The TOE denies the establishment of a trusted path in case of the authentication fails or if the source IP address is not allowed to establish a trusted path according to the ACL policy.
5) The TOE supports termination of an interactive session after a given interval of user inactivity. This results in a loss of user authentication (for both connections, via LMT console as well as via RMT).
6) The TOE makes temporary session keys stored in volatile memory inaccessible upon termination of SSH sessions.
7) AES-128 in CTR mode is used for encryption and decryption within SSH communication.
8) The TOE performs data integrity generation and verification in accordance with the cryptographic algorithm HMAC-SHA2-256
9) The TOE generates cryptographic keys in accordance with the cryptographic key generation algorithm diffie-hellman-group14-sha256
10) The TOE performs asymmetric authentication in accordance with RSA and cryptographic key sizes 2048 bits.

This security function supports the security management countering *all identified threats*

6 Rationale

6.1 Assets vs Threats

Threat Asset	UnwantedL3NetworkTraffic	Unauthenticated Access	Unauthorized Access	Eavesdrop
WantedL3 NetworkTraffic	Av			I, C
Configuration data		Av, I,	Av, I,C	I, C
Logs		Av,I,C	Av, I,C	
Av: Availability, I: Integrity, C: Confidentiality				

6.2 Threats vs security functions

Threat Security Function	UnwantedL3NetworkTraffic	Unauthenticated Access	Unauthorized Access	Eavesdrop
SF.Access Control List	X			
SF.Authentication		X	X	
SF.Access Control		X	X	
SF.Audit (log)		X	X	
SF.Communication Security (SSH)				X