PERSISTENT SYSTEMS

FIPS 140-2 Non-Proprietary Security Policy

Persistent Systems Wave Relay Dual Radio Board and Quad Radio Board

Level 1 Validation

Document Version 2.1

September 21, 2010

Prepared For:

Persistent Systems, LLC
303 Fifth Avenue Suite 207
New York, NY 10016
www.persistentsystems.com

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive, Suite 101
Apex, NC 27502
www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Wave Relay Dual Radio Board and Quad Radio Board.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) owns the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for all products pursuing FIPS 140 validation. *Validation* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Wave Relay Dual Radio Board and Quad Radio Board from Persistent Systems provides an overview of the product and a high-level description of how they meet the security requirements of FIPS 140-2. This document contains details on the modules' cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The Persistent Systems Wave Relay Dual Radio Board and Quad Radio Board may also be referred to as the "modules" in this document.

1.3 External Resources

The Persistent Systems website (http://www.persistentsystems.com) contains information on the full line of products from Persistent Systems, including a detailed overview of the Wave Relay Dual Radio Board and Quad Radio Board solutions. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/) contains links to the FIPS 140-2 certificate and Persistent Systems contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
MANET	Mobile Ad-hoc Network
NIST	National Institute of Standards and Technology
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 Persistent Systems Wave Relay Dual Radio Board and Quad Radio Board

2.1 Wave Relay Product Overview

The Wave Relay™ solution provides a scalable high performance solution for deploying large Mesh or MANET systems. The Quad Radio Board can contain up to 4 separate wireless radios all of which both participate in the routing and can provide connectivity to 802.11 based wireless clients. By utilizing 4 radios, the Wave Relay™ board can simultaneously provide a multi-channel high speed multi-hop backhaul and provide client connectivity to client devices. This provides a single solution to all of your mesh networking needs. Wave Relay™ provides a unique combination of deployment flexibility, dynamic self configuring routing, throughput optimized route selection, fault tolerance, and scalability.

The Wave Relay™ Mobile Ad Hoc Networking System is available in a Dual Radio Board form factor, providing a smaller and lighter form factor for applications where size weight power are at a premium (for example in small unmanned systems or sensors). The Wave Relay™ Dual Radio Board delivers mobility while providing high communication performance.

2.2 Cryptographic Module Specification

The modules are the Persistent Systems Wave Relay Dual Radio Board (HW P/N WR-BRD-DUAL, Version 1.0 and 1.1; FW Version 17.3.0) and Quad Radio Board (HW P/N WR-BRD-QUAD, Version2.0; FW Version 17.3.0). Each module is a multiple-chip embedded embodiment.

The physical cryptographic boundary is defined as the Wave Relay main board, which includes the hardware cryptographic accelerator chip, CPU, RAM, and on-board flash memory. The boundary does not include plastic port connectors, port connector pins, and metal Ethernet port connectors[*].

The following functionality is not permitted in FIPS mode:

- Use of the JTAG port as specified in Section 3.1.2 – General Crypto Officer and User Guidance

Each module only supports a FIPS-Approved mode of operation. It does not have any functional non-Approved modes or bypass capability. An operator can determine that the module is in the FIPS Approved mode by checking the firmware version and verifying that it matches the validated version.

[*] Connectors are specifically excluded to allow their removal without affecting FIPS validation. For example, a Dual Radio Board with the back Wireless Radio connector removed can effectively serve as a "Single Radio Board" FIPS module. This configuration can be used in applications where only one radio is needed and smaller size/weight/power is required.

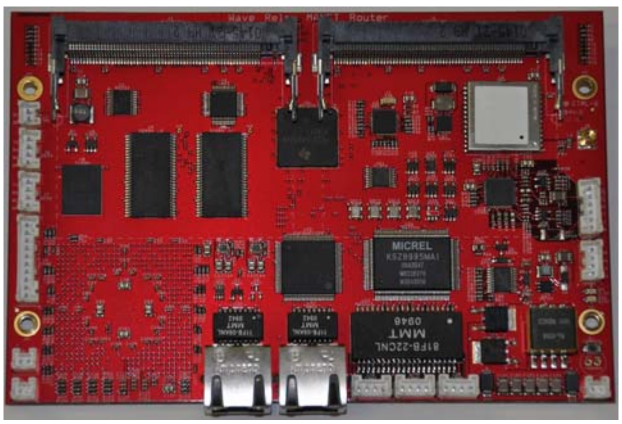
Front Version 1.0

Back Version 1.0

Front Version 1.1

Back Version 1.1

Figure 1 – Physical Boundary of Wave Relay Dual Radio Board



Front

Back

Figure 2 – Physical Boundary of Wave Relay Quad Radio Board

2.2.1 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	1*
Roles, Services, and Authentication	2
Finite State Model	1*
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1*
Electromagnetic Interference / Electromagnetic Compatibility	1*
Self-Tests	1*
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Level	**1**

Table 2 – Validation Level by DTR Section

* These sections do not have different requirements between level 1 and level 2, and by convention are assigned a level equal to the overall level of the module..

2.2.2 Algorithm Implementation Certificates

The modules' cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificates	Use
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-3	1140	Message digest
Keyed Hash	HMAC-SHA1, HMAC-SHA-224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	FIPS 198	725	Message integrity, module integrity
Symmetric Key	AES CTR, ECB, CBC, GCM mode with 128, 192, or 256-bit keys	FIPS 197	1241	Data encryption / decryption

Table 3 – Algorithm Certificates for Wave Relay Hardware Implementation

Algorithm Type	Algorithm	Standard	CAVP Certificates	Use
Asymmetric Key	DSA (1024 bits), RSA (1024 to 4096 bits)	Digital Signature Standard, PKCS1.5	409 (DSA) 595 (RSA)	DSA: Sign / verify, PQG Gen, Key Gen RSA: Sign / verify, Key Gen; key establishment (non-Approved)
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-3	1141	Message digest
Keyed Hash	HMAC-SHA1, HMAC-SHA-224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	FIPS 198	726	Message integrity
Symmetric Key	AES CBC, ECB, CFB8, CFB128, OFB modes each with 128, 192, or 256 bit keys	FIPS 197	1242	Data encryption / decryption
	TDES ECB, CBC, CFB8, CFB64, OFB	FIPS 46-3	889	Data encryption / decryption
RNG	ANSI X9.31 Appendix A.2.4	ANSI X9.31	689	Random Number Generation

Table 4 – Algorithm Certificates for Wave Relay Firmware Implementation

The following non-approved protocols/algorithms are available in FIPS mode of operation:

- RSA 2048 within TLS for Key establishment (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Hardware non-deterministic RNG (NDRNG) (allowed for seeding FIPS-approved RNG)
- SSH protocol*
- 802.11 Access Point security: WPA2/WPA/WEP protocols*
- MD5 with TLS*
- MD5*

*** No security is claimed from the use of these protocols/algorithms.**

2.3 Module Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by the modules are mapped to four FIPS 140-2 defined logical interfaces: Data Input, Data Output, Control Input, and Status Output. The mapping of logical interfaces to module physical interfaces is provided in the following table:

FIPS 140-2 Logical Interface	Dual Radio Board Module Physical Interface	Quad Radio Board Module Physical Interface
Data Input	Ethernet ports (2) Wireless Radio ports (2) GPS antenna Audio with Push To Talk and Serial Serial port	Ethernet ports (5) Wireless Radio ports (4) GPS antenna Audio with Push To Talk and Serial Serial ports (2)
Data Output	Ethernet ports (2) Wireless Radio ports (2) Audio with Push To Talk and Serial Serial port	Ethernet ports (5) Wireless Radio ports (4) Audio with Push To Talk and Serial Serial ports (2)
Control Input	Ethernet ports (2) Wireless Radio ports (2) Audio with Push To Talk and Serial Serial port Power/Zero Button port Tamper push button Power interface	Ethernet ports (5) Wireless Radio ports (4) Audio with Push To Talk and Serial Serial ports (2) Power/Zero Button port Tamper push button (2) Power interface
Status Output	Ethernet ports (2) Wireless Radio Ports (2) Audio with Push To Talk and Serial Serial port Status LED port Green LED (status) Green LED (power)	Ethernet ports (5) Wireless Radio Ports (4) Audio with Push To Talk and Serial Serial ports (2) Status LED port Green LED (status) Green LED (power)
Power	Power supply plane	Power supply plane
Non-relevant interfaces	JTAG port (not to be used in FIPS mode)	JTAG port (not to be used in FIPS mode)

Table 5 – Logical Interface / Physical Interface Mapping

2.4 Roles, Services, and Authentication

Each module only supports a FIPS-Approved mode. The modules are accessed via Web browser over HTTPS/TLS. As required by FIPS 140-2, each module supports a Crypto Officer role and a User role. In addition each module supports a Network Management role where an operator indirectly controls the module through another module. The modules supports role-based authentication, and the respective services for each role are described in the following sections.

All three roles can access all services in each module. The modules do not support a Maintenance role. The "Unauthenticated" role indicates services that the modules perform automatically after POST and services that an operator may perform without authentication (e.g. using Power/Zero Button port).

2.4.1 Operator Services and Descriptions

The services available to the roles in the module are as follows:

Service	Description	Roles
Initialize and configure	Initializes and configures the module	Crypto Officer User Network Management
Packet Forwarding	Provides packet forwarding and receipt. Forwarded packets are encrypted and signed, and incoming packets are decrypted and verified	Provided on behalf of an authenticated role
Generate Keys	Generates AES keys for encrypt/decrypt operations	Crypto Officer User Network Management
Firmware Upgrade	Upgrade firmware to newer release Note: If non-FIPS validated firmware is loaded, the module is no longer a FIPS validated module.	Crypto Officer User Network Management
Self Test	Performs self tests on critical functions of module	Crypto Officer User Network Management Unauthenticated
Status	Status of the module	Crypto Officer User Network Management Unauthenticated
Zeroize	Zeroize keys and CSPs in the module	Crypto Officer User Network Management Unauthenticated

Table 6 – Operator Services and Descriptions

Each module supports multiple concurrent operators. Each "view" or "set" of configuration by a user is a separate action, and the actual configuration is determined by the latest "set." The Web GUI will indicate that a User/Crypto Officer role has logged themselves in. As specified in Section 3 – Guidance and Secure Operation section of this document, only one operator can configure the module at one time. In the event that two operators are authenticated at one time for configuration, the module will save/store the parameters of the last operation.

2.4.2 Operator Authentication

Crypto Officer and User passwords must be a minimum of 8 characters (see Section 3 – Guidance and Secure Operation section of this document). The password can consist of alphanumeric values, **`a-z A-Z 0-9`**, yielding 62 choices per character. The probability of a successful random attempt is $1/62^8$, which is less than 1/1,000,000. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is $600/62^8$, which is less than 1/100,000.

The Network Management Role authenticates via a MAC on network management packets (listed in Table 7 – Key/CSP Management Details). The MAC on each packet is 96-bits and computed with a minimum key size of 256-bits. The probability of a successful random attempt is $1/2^{96}$, which is less than 1/7.9e28. Even at maximum theoretical 100 Mbps Ethernet packet rate (around 130,000 packets per second), the probability of a success with multiple attempts in a one-minute period is 1/1.0e22, which is less than 1/100,000.

2.5 Physical Security

The physical security of each cryptographic module meets FIPS 140-2 Level 1 requirements. The cryptographic modules consist of production-grade components. The physical boundary of each cryptographic module is the same as the physical boundary of the device. The following components are not included in the boundary: plastic port connectors, port connector pins, and metal Ethernet port connectors.

The modules do not include a maintenance interface; therefore, the FIPS-140-2 maintenance mode requirements do not apply.

2.6 Operational Environment

Each module runs in a limited, purpose-built operational environment. As such, the requirements of this section do not apply.

2.7 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters and Public Keys used within the modules:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Privileges
Network Key	AES CTR, CBC, GCM mode with 128, 192, or 256-bit key for encryption / decryption of network traffic	Internal generation by X9.31 RNG Electronic Key Entry via Web-GUI Imported via encrypted session to another network node (module)	**Storage**: Flash in encrypted form **Association**: The system is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: Electronic Key Entry via Web-GUI or imported via encrypted session to another network node (module) **Output**: via HTTPS to Web GUI or with legacy Network Key	R W D
Firmware Upgrade Public Key	RSA 4096-bit key for verifying firmware signature before upgrading	Not generated by the module; built into firmware	**Storage**: Flash in plaintext **Type:** Static **Association**: controlled by the operating environment	**Agreement**: NA **Entry**: NA **Output**: NA	None
Operator passwords	Alphanumeric passwords externally generated by a human user for authentication.	Not generated by the module; defined by the human operator	**Storage**: Flash in encrypted form **Type:** Static **Association**: controlled by the operating environment	**Agreement**: NA **Entry**: Electronic entry via Web-based GUI or imported via encrypted session to another network node (module) **Output**: NA	R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Privileges
MAC key	HMAC-SHA1, HMAC-SHA-224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, GMAC for message verification and integrity check	Internal generation by X9.31 RNG Electronic Key Entry via Web-GUI Imported via encrypted session to another network node (module)	**Storage**: Flash in encrypted form **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: Electronic Key Entry via Web-GUI or imported via encrypted session to another network node (module) **Output**: via HTTPS to Web GUI or with legacy Network Key	R W D
TLS Premaster Secret	RSA-Encrypted Premaster Secret Message (48 Bytes)	As part of TLS handshake	**Storage**: RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to peer encrypted by Public Key	None
TLS Master Secret	Used for computing the Session Key (48 Bytes)	As part of TLS handshake	**Storage**: RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Privileges
RNG XKEY	256-bit value to key the FIPS-approved ANSI X9.31 RNG	Hardware NDRNG	**Storage**: RAM in plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	None
RNG XSEED	128-bit x-seed	Hardware NDRNG	**Storage**: RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	None
TLS Public Key	RSA Public 2048-bit for sign / verify operations and key establishment for TLS sessions. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation by X9.31 RNG	**Storage**: Flash in encrypted form **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X.509 certificates.	**Agreement**: NA **Entry**: NA **Output**: As part of TLS handshake	R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Privileges
TLS Private Key	RSA Private 2048-bit for sign / verify operations and key establishment[†] for TLS sessions	Internal generation by X9.31 RNG	**Storage**: Flash in encrypted form **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	R W D
Store Key	AES CBC 256-bit key for encryption of Flash data store	Internal generation by X9.31 RNG	**Storage**: Battery backed RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	R W D
TLS Session Keys	AES 256 bit key used with TLS	Generated as part of TLS handshake	**Storage:** SRAM **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating environment via protected memory	**Agreement: N/A** **Entry: N/A** **Output: N/A**	None

Table 7 – Key/CSP Management Details (also includes public keys)

R = Read W = Write D = Delete (applies to all roles)

[†] Key establishment methodology provides at least 112-bits of encryption strength

Note that hardware NDRNG entropy source provides 384 bits of entropy to key and seed the RNG. This helps ensure sufficient strength of the seed so as to not compromise the output.

Network Keys can be exported from the physical boundary of the module when the Crypto Officer re-keys the module using the network management feature. The Network Key will be sent to other nodes (modules) on the network encrypted with the legacy Network Key.

All persistent keys and CSPs are stored in an encrypted store. This store is located in Flash and is encrypted via an AES 256-bit key. The key & IV used to encrypt the store are stored in battery backed RAM in order to make them persistent. Zeroization has been implemented to ensure no traces are left of the store key & IV. Zeroization is achieved by explicitly overwriting the specific memory area with a constant. The modules can be zeroized by entering a sequence of three short presses on the Power/Zeroize button port, or by releasing the tamper push button.

2.8 Self-Tests

Each module includes an array of self-tests that are run during startup and periodically during operations to prevent secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error and will shutdown. To access status of self-tests, success or failure, the application provides access to the Web-based GUI. No keys or CSPs will be output when the module is in an error state.

If the self-tests succeed, the operator will be presented with a login screen when accessing the module via HTTPS, and attempts to access the module via HTTP will be automatically redirected to HTTPS. If the self-tests fail, any attempt to access the module via HTTPS will fail because TLS is disabled, and any attempt to access the module via HTTP will result in a FIPS error message.

Since the modules only support a FIPS-approved mode of operation, the self-tests are always run. On failure the modules will always be non-operational as there is no non-FIPS or bypass mode available.

The following sections discuss the modules' self-tests in more detail.

2.8.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of each module and if any of the tests fail, the process will be halted and the module will not initialize. In this error state, no services can be accessed by the users. The module implements the following power-on self-tests:

- Hardware Implementation:
    - KAT for AES
    - KAT for SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

    - KAT for HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512

- Firmware Implementation:
    - Module integrity check via HMAC-SHA256
    - KAT for AES
    - KAT for TDES
    - KAT for DSA and RSA
    - KAT for RNG
    - KAT for HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512

Each module performs all power-on self-tests automatically when the module is initialized, and successful running of self tests will be indicated via the GUI. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by restarting the module.

2.8.2 Conditional Self-Tests

Conditional self-tests are run continuously when certain conditions are met during operation of each module. The modules perform the following conditional self-tests:

- Pairwise consistency test for RSA
- Pairwise consistency test for DSA
- Continuous RNG test run on output of ANSI X9.31 RNG implementation
- Continuous test to verify that the ANSI X9.31 RNG seed and seed key do not match
- Continuous test on RNG seeding mechanism (output of NDRNG)
- Firmware load / firmware upgrade test (RSA digital signature verification)

Note that each module performs conditional tests for firmware implementations of the algorithms listed in Table 4 – Algorithm Certificates for Wave Relay Firmware Implementation. The module’s algorithm implementations in hardware are not required to meet any conditional tests. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. While in an error state, no services can be accessed by the operators.

2.9 EMI/EMC

The modules meet Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part 15, Subpart A.

2.10 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure each module for FIPS-Approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-Approved mode of operation.

3.1 Crypto Officer and User Guidance

3.1.1 Initialization for FIPS Mode of Operation

The Crypto Officer or User must configure and enforce the following procedures:

1. When setting the password, the Crypto Officer or User must ensure that all passwords are a minimum length of 8 characters consisting of the following alphanumeric values: **`a-z A-Z 0-9`**

   Note: Stronger, more secure passwords should have a combination of letters and numbers and should not contain any recognizable words that may be found in a dictionary. The module does not enforce this; the Crypto Officer or User must follow his/her organization's systems security policies and adhere to the password policies set forth therein.

2. Ensure only version 17.3.0 is running.
3. After following these steps for the initial configuration for FIPS mode, the Crypto Officer or User must reboot the module to run the Power On Self Tests prior to operating in a FIPS mode of operation.

3.1.2 General Crypto Officer and User Guidance

After initialization for FIPS mode, the Crypto Officer should follow the guidance below:

1. When entering a network key over the configuration GUI, the operator must ensure that key was generated by FIPS-approved methods and that the key was not previously used.

2. The operator must ensure that all Radio MAC addresses used in a network are unique.
3. The Crypto Officer or User must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.
4. The JTAG port is not to be used in FIPS mode of operation. Using the JTAG port will remove the module from FIPS mode of operation.
5. The SSH service must not be accessed. Using SSH will violate the authorized use policy.