National Information Assurance Partnership


# Common Criteria Evaluation and Validation Scheme
# Validation Report

## Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4

**Report Number:** **CCEVS-VR-04-0053**
**Dated:** **30 January 2004**
**Version:** **1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

# ACKNOWLEDGEMENTS

**Validator**
Margaret T. Webster-Butler
National Security Agency
Ft. Meade, MD 20755

## Common Criteria Testing Laboratory

**Evaluation Team**
Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

# Table of Contents

# 1. Executive Summary

The Target of Evaluation (TOE), Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4, was evaluated by Computer Sciences Corporation (CSC) Common Criteria Testing Laboratory (CCTL) in the United States, beginning on 03 April 2003, and completed on 30 January 2004. The evaluation was for the Evaluation Assurance Level 2 (EAL2). The evaluation was conducted in conformance with the Common Criteria (CC) for Information Technology Security Evaluation, parts 1, 2, 2a, and 3; and, the Common Evaluation Methodology for Information Technology Security (CEM), parts 1 and 2. The evaluation was conducted in accordance with the rules and regulations of the NIAP Common Criteria Evaluation and Validation Scheme, and the conclusions of CSC in their Evaluation Technical Report (ETR) were consistent with the evidence adduced. CSC concluded that the Common Criteria requirements of EAL2 had been met for the TOE.

The TOE, the Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4, is a hardware component that slides into a slot within the chassis of a Foundry BigIron or FastIron router or switch. The TOE's operating system is Foundry Networks' IronWare™ operating system (IOS), Version 07.6.04f (which incorporates Foundry Networks' IronShield™ security module). The evaluation focus is on the management module running the IOS Version 07.6.04f software, as the TOE. The TOE's purpose is to securely manage itself and its accessibility to the Foundry routers and switches that it is configured to interact with. The J-BxGMR4 management module is for use with the Foundry BigIron 4000, 8000, and 15000 series chassis, and the J-FxGMR4 management module is for use with the Foundry FastIron 400, 800, and 1500 series chassis.

The Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4 Security Target (ST) and Section 10 of this report, (Validator's Comments/Recommendations), identifies the specific version and models of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

The cryptography used in this product to encrypt passwords (MD5 authentication strings), has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

### 1.1. Evaluation Highlights

**Dates of Evaluation:** 03 April 2003 through 30 January 2004
**Evaluated Product:** Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4
**Developer:** Foundry Networks Inc., 2100 Gold Street, P.O. Box 649100, San Jose, CA 95164-9100
**CCTL:** CSC, 132 National Business Parkway, Annapolis Junction, MD 20701
**Evaluation Class:** EAL2
**PPs Claimed:** None
**Validator:** Margaret T. Webster-Butler, National Security Agency

## 2. Product Identification

**ST:** Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4 Security Target v1.0, dated 08 January 2004.

**TOE Identification:** Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4

The TOE, the Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4, is a hardware component that slides into a slot within the chassis of a Foundry BigIron or FastIron router or switch. The TOE's operating system is Foundry Networks' IronWare™ operating system (IOS), Version 07.6.04f (which incorporates Foundry Networks' IronShield™ security module). The management module running the IOS Version 07.6.04f software is the TOE, and its purpose is to securely manage itself and its accessibility to the Foundry routers and switches that it is configured to interact with. The J-BxGMR4 management module is for use with the Foundry BigIron 4000, 8000, and 15000 series chassis, and the J-FxGMR4 management module is for use with the Foundry FastIron 400, 800, and 1500 series chassis.

## 3. Security Policy

The following identifies the organizational security policies that are determined to be relevant for the TOE:

| | |
|---|---|
| P.LOCAL_ACCOUNTS | The system will have local accounts, and passwords; the passwords will be encrypted. |
| P.PRIVILEDGE_LEVELS | The system must have the ability to limit Authorized Administrator(s) management privilege level(s). |

| | |
|---|---|
| P.REMOTE_ACCESS | Management access methods, other than the Serial access to the Command Line Interface (CLI), will be secured via AAA security methods. Though there may be external methods, there will be a local method. If an external I&A mechanism is utilized, the System will enforce the decision of that mechanism. |
| P.SYS_CLOCK | The time and date will be set on the Management module's onboard system clock. |
| P.SYSLOG | The Management module's syslog capability will be enabled and have the local message buffer configured to retain 100 messages. |

# 4. Assumptions and Clarification of Scope

## 4.1 Usage Assumptions

The environmental assumptions listed below are required to ensure the security of the TOE:

| | |
|---|---|
| A.INSTALL | The TOE hardware and software have been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures. |
| A.MANAGE | There will be one or more competent Authorized Administrator(s) assigned to manage the TOE and the security functions it performs. |
| A.EXTERNAL_I&A | External Identification and Authentication mechanisms function correctly and accurately. |
| A.NO_EVIL_ADM | An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation. |
| A.PROCEDURE | Procedures exist for granting Authorized Administrator(s) access to the TOE Security Functions (TSF). |
| A. PHYSICAL_PROTECT | The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access. |

## 4.2 Clarification of Scope

The TOE is the J-BxGMR4 and J-FxGMR4 management modules running the IOS Version 07.6.04f software. The TOE's purpose is to securely manage itself and its accessibility to the Foundry routers and switches that it is configured to interact with. The IronWare™ operating system alone, was not the focus of this evaluation and its purpose, to control the switching and routing of layer 2 and layer 3 frames and packets through Foundry chassis-based switches and routers, was not addressed in this evaluation. The focus of this evaluation is on the two management modules running the IronWare™ operating system, Version 07.6.04f, (which incorporates Foundry Networks' IronShield™ security module) and its security features only.

## 4.3 Interpretations

The CSC evaluation team performed an analysis of the international and national interpretations and identified those that were applicable and had an impact on the TOE evaluation. Those interpretations were applied when the CEM work units were started.

The following sections provide the number and title of the applicable interpretations and the CEM class in which they were considered.

**Applicable National Interpretations**

None.

**Applicable International Interpretations**

003 ACM_CAP.2-7 clarification
116 ADO_DEL.1-2 deletion

## 4.4 Threats

## 4.4.1 Threats Addressed by the TOE

The threat to the TOE is considered to be users with public knowledge of how the TOE operates and possess the skills and resources to alter TOE configuration settings/parameters. The threat agents do not have physical access to the TOE.

| | |
|---|---|
| T.ALTER_CONFIG | An unauthorized user may attempt to access the TOE through an external interface in order to alter the TOE configuration to circumvent the configured policy so they can access networks/resources they for which they are not authorized. |

### 4.4.2 Threats Addressed by the IT Environment

None.

## 5. Architectural Information

The TOE, the Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4, is a hardware component that slides into a slot within the chassis of a Foundry BigIron or FastIron router or switch. The TOE's operating system is Foundry Networks' IronWare™ operating system (IOS), Version 07.6.04f (which incorporates Foundry Networks' IronShield™ security module). The management module running the IOS Version 07.6.04f software, is the TOE. The TOE can be configured to function as either a router or switch. The TOE securely manages itself and its interactions with other Foundry routers and switches. The J-BxGMR4 is for use with the Foundry BigIron 4000, 8000, and 15000 series chassis, and the J-FxGMR4 is for use with the Foundry FastIron 400, 800, and 1500 series chassis.

The TOE interfaces are:

| | |
|---|---|
| Serial Interface | The SI is a single 9 pin male DB9 connector located on the front panel of the TOE and commonly referred to as the console. It is configured as 9600 baud, 8 data bits, no parity, 1 stop bit and no flow control. This interface is used to locally manage the TOE using Command Line Interface (CLI) commands, which are issued to the switch or router from a host running a Terminal Emulation Program and connected to the interface using a straight through DB-9 to DB-9 female cable. This interface is compliant with the EIA/TIA RS-232 serial communications standard. |
| Ethernet Interface | The EI is any one of 8 mini-GBIC ports located on the front panel of the TOE and capable of supporting IEE802.3z 1000BaseSX and 1000BaseLX optical fiber modules. This interface is used to connect to other network devices or to end hosts, such as servers and clients. This interface can also be used to facilitate a TELNET session through which an authorized user can remotely manage the TOE. The TOE must be configured with an IP address prior to attempting remote management. This interface is compliant with the IEEE-802 ethernet specification. |
| Backplane Interface | The TOE module's backplane interface is not visible to the administrator or user when the TOE is installed in the chassis. Foundry's architecture is such that all local processing of user data stays local and does not rely on the module backplane connection to the chassis. If user traffic is destined for a port on another module, then it traverses the physical connection to the chassis. System management traffic is sent to and from the TOE to other modules in the chassis using the management bus connection to the backplane through the backplane connector. |

| | |
|---|---|
| Reset Interface | The RI is a physical reset button located on the lower right hand corner of the TOE front panel. It is used to reset or warm start the operation of the TOE. This is performed by pushing the button momentarily. Upon pushing the button, the CPU managing the TOE will halt all processing and reload the system software. This action is identical to issuing the CLI command "reload." The default action is to reload the system software in the primary flash location and parse the startup configuration file for system-wide configuration parameters. |

## 5.1 Physical Boundaries

The TOE, the Foundry Networks, Management Module IV: J-BxGMR4 and J-FxGMR4, is a hardware component that slides into a slot within the chassis of a Foundry BigIron or FastIron router or switch. The TOE's operating system is Foundry Networks' IronWare™ operating system (IOS), Version 07.6.04f (which incorporates Foundry Networks' IronShield™ security module). The management module running the IOS Version 07.6.04f is the TOE and it's purpose is to allow for the secure management of the Foundry routers and switches that it is configured to interact with. The J-BxGMR4 is for use with the Foundry BigIron 4000, 8000, and 15000 series chassis, and the J-FxGMR4 is for use with the Foundry FastIron 400, 800, and 1500 series chassis.

## 5.2 Logical Boundaries

The TOE provides the following security functions:

***User Data protection***: TSF_UDP_REMOTE, TSF_UDP_MAC, TSF_UDP_PRIV, TSF_UDP_FLOW;
***Identification and Authentication***: TSF_FIA_USERS, TSF_FIA_AUTH;
***Security Management***: TSF_FMT; and
***Auditing***: TSF_FAU.

**User Data Protection (TSF_UDP_REMOTE)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the capability to specify an access control security functional policy in order to restrict management functions from remote sources (NETWORK_MGMT SFP), including Telnet, the Web management interface, and SNMP. The following methods for restricting remote access are supported:

Using ACLs to restrict Telnet, Web management interface, or SNMP access;
Allowing remote access only from specific IP addresses;
Allowing remote access only to clients connected to a specific VLAN;
Disabling the Telnet, Web, or SNMP server if no remote access is required.

Access decisions for ACLs are based on entries in the device's configured Access Control List(s) (ACL). Access control parameters include entries specifying the allowed or disallowed source host or network IP address.

**User Data Protection (TSF_UDP_MAC)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the capability to specify an access control security functional policy (MAC_PORT_LOCK SFP) in order to lock port-level access to the device by determining if the MAC address of the connecting host and the hardware port through which the connection request is made, is in the device's startup configuration file; only the authorized administrator-specified MAC address or MAC address that was initially learned using the port security autosave feature will be allowed to connect through the port. Autosave allows the switch to dynamically learn MAC addresses which are connected to ports configured for autosave, and write them in to the configuration file. Thereafter, only the initially learned address is allowed to connect to the port.

**User Data Protection (TSF_UDP_PRIV)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the capability to specify an access control security functional policy in order to limit user access to specific levels of the command line interface (CLI) (PRIVILEGE_LEVEL SFP).

**User Data Protection (TSF_UDP_FLOW)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 Management Modules have the ability for the Authorized Administrators to specify the information flow control security functional policy [INFOFLOW SFP] used to control the flow of user data across the ports of the device. ACLs are used by Foundry to control forwarding of network data at specified ports on network equipment. There are two types of ACLs that can be configured, *standard* and *extended*. *Standard* ACLs permit or deny packets based on source IP address only. *Extended* ACLs take more factors into consideration including IP protocol information.

**Identification and Authentication (TSF_FIA_USERS)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules allow the assigning of user names and passwords to control access to the management functions of the device. Additionally, a user definition can contain the management privilege level assigned to that user.

**Identification and Authentication (TSF_FIA_AUTH)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules allow the Authorized Administrator to configure Authentication-Method lists. These lists are used to specify the order in which the authentication methods are employed whenever there are one or more authentication methods defined.

**Security Management (TSF_FMT)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules include a number of functions to manage security policy and its implementation. Policy management and implementation are controlled through the use of various ACLs, and several security role definitions/privileges.

**Auditing (TSF_FAU)** – The Foundry Networks J-BxGMR4 and J-FxGMR4 management modules have the ability to generate syslog-based audit log entries for each defined ACL entry.

## 6. Delivered Product

The delivered product to the CSC CCTL for this evaluation consisted of the following items:

1. The product was delivered to CSC palletized as three boxes, with two straps holding it onto the pallet and surrounded on all sides with cellophane wrapping.
2. The main box contained the chassis with the J-BxGMR4 (8 slot management module) and the J-B24FX (24 port 100Base-FX interface module for fiber connectivity) already inserted.
3. The J-FxGMR4 (8 slot management module) and the E1MTG-SX (Mini-Gigabit Interface Converter (GBIC) module) came in their own separate boxes and were sealed with string tape.
4. A packing slip on the shipment provided a full listing of the components in the shipment and a Quality Assurance check test document was included.

## 7. IT Product Testing

## 7.1 Examination of Vendor Tests

Foundry Networks, the vendor, provided functional and independent test plans, procedures, test results and a test coverage document for the testing of each Security Functional Requirements (SFR) within the TOE Security Functions (TSF). Functional testing covered the following TSFs:

**Test 1 MAC Port Locking (TSF_UDP_MAC**) tests the ability of the TOE to detect/learn a MAC address at the port level, and then to "watch" the port noting any change in MAC. If a change occurs, the TOE then follows the startup configuration file instructions to lock the port by disabling the flow across the port. Also, Test 1 tests the ability of the TOE to unlock a locked port.

**Test 2 Access Control Lists (TSF_UDP_REMOTE and FLOW)** tests Access Control List (ACL) usage. Again, the startup configuration file is utilized. For this test, an ACL is defined to deny in bound traffic for TCP ports 7 and 11 on physical Ethernet interface 2/1, and to log any violations. The testing forces the violation by using telnet directed to TCP

ports 7 and 11. The violations were verified in the log. This scenario exercised TSF_FAU (Auditing) and TSF_FMT (Security Management).

**Test 3 Password Verification (TSF_UDP_PRIV)** tests authentication of local accounts and passwords. As noted in the first 2 tests, the startup configuration file is utilized. Three local accounts and passwords are defined. The test validates that all three of the accounts function when the correct password is entered. This scenario exercised TSF_FIA_USERS (I&A users), TSF_FIA_AUTH (I&A authorization) and TSF_FMT (Security Management).

The evaluation team examined the test coverage analysis and found that Foundry Networks provided a correspondence between the tests provided for evaluation and the functional specification.

The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TOE Security Functions was appropriate for this EAL2 evaluation.

## 7.2 Evaluation Team Independent Tests

The evaluation team performed all three of Foundry Network's functional tests that were provided. In addition, the evaluation team used the provided tests to create additional and enhanced independent tests. One set of independent tests were run on the J-FxGMR4, which was configured as a switch unit, then the same set of tests were run on the J-BxGMR4, which was configured as a router unit. The tests were conducted using 2 differing privilege level consoles as remote hosts and another console that functioned as the main operations console. The types of tests included:

1. Configuring and testing ACLs to control telneting to a host that allowed telnet, telnetting to a host that did not allow telnet and then viewing the results;
2. Verifying that Web Management was turned off ("no webman" command at main console), then trying to use it;
3. Configuring and testing ACLs, to test userids that can and can not use privileged commands;
4. Time out and denied port accesses were configured on the operations console and then tested at remote hosts;
5. Enable port learning using autosave; then performing configuration checks by physically swapping ports while the system is running, then swapping ports after a power down/power up procedure and checking the results;

6. Password tests by creating bogus userids and checking the results;
7. Authentication by creating userids with differing privileges, then testing those privileges
8. Testing remote host commands such as auto logout and enabling telnet;
9. Viewing logs from all 3 consoles.

The general test suite, which was run on each management module, is shown below ("x" indicates either router or switch mode when the test was run):

| **User Data Protection** | |
|---|---|
| xT1.1 Restrict Remote Management Functions | *Evaluation team created:*<br>Restrict telnet and web management via CLI |
| xT1.2 Limit User access and privilege | *Evaluation team created:*<br>Super-user and read-only privilege |
| xT1.3 Extended ACL | *Evaluation team enhanced vendor test 2:*<br>Block a range of ports using extended ACLS |
| xT1.4 Port Level Locking | *Evaluation team enhanced vendor test 1:*<br>Use of autosave with port security and recovery from power loss |
| **Identification and Authentication** | |
| xT2.1 Minimum Password Length | *Evaluation team created:*<br>Validate that a shorter than allowed password is denied |
| xT2.2 Local Authentication | *Evaluation team ran vendor test 3:*<br>Username and password with local authentication |
| **Security Management** | |
| xT3.1 Telnet password and Timeout | *Evaluation team created:*<br>Set telnet password and timeout via CLI |
| xT3.2 Serial console Timeout | *Evaluation team created:*<br>Set serial console timeout |
| **Auditing** | |
| xT4.1 Log buffer and remote syslog | *Evaluation team enhanced vendor test 2:*<br>Validate logging locally; remote syslog capability; write to remote syslog server |

In every case, the evaluation team concluded that the expected results matched the team's actual results.

The cryptography used in this product to encrypt passwords (MD5 authentication strings), has not been FIPS certified nor was it tested during this evaluation however, encrypted passwords were noted during testing. The password encryption has only been asserted as tested by the vendor.

## 7.3 Strength of Function

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim. The overall SOF claim for the TOE made in this ST was expressed as a medium SOF rating.

According to the Common Evaluation Methodology Part2, Annex B.8, Para. 1849 "A minimum claim of SOF-basic is required wherever components for AVA_SOF are claimed." This fact, and the Common Evaluation Methodology Part2, Annex B.8, Table B-2, "a SOF rating of SOF-basic is adequate protection against an attacker with an attack potential of low", led the evaluator to concur with the developer's SOF claim.

## 7.4 Vulnerability Analysis

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate any TOE Security Policies.

The evaluation team conducted the following independent vulnerability tests on each management module:

| | | |
|---|---|---|
| Network | P1.1 Switch Network Scan | Switch Network Scan using nmap |
| Network | P1.2 Switch Network Vulnerability Scan | Switch Network Vulnerability Scan using nessus |
| Network | P1.2 Switch Network Vulnerability Scan | Switch Network Vulnerability Scan using H.E.A.T. |
| Network | P1.3 Switch HTTP CGI Script Scan | Switch HTTP CGI Script Scan using nikto |
| Environment | P1.5 Switch / Router Disassemble Binaries | Switch / Router Disassemble Binaries using cxmon |
| Environment | P2.1 Switch Apply Load | Switch Apply Load using tcpreplay |
| Network | P1.1 Router Network Scan | Router Network Scan using nmap |
| Network | P1.2 Router Network Vulnerability Scan | Router Network Vulnerability Scan using nessus |
| Network | P1.2 Router Network Vulnerability Scan | Router Network Vulnerability Scan using H.E.A.T. |
| Network | P1.3 Router HTTP CGI Script Scan | Router HTTP CGI Script Scan using nikto |
| Environment | P2.1 Router Apply Load | Router Apply Load using tcpreplay |

In all cases, the evaluator's expected results were in line with the actual results.

## 8. Evaluated Configuration

The evaluated configuration used to test both models of the TOE was:

Foundry BigIron 4000 Chassis in either Router or Switch mode

- Router Configuration
  J-BXGMR4 Management Module IV in Slot 1,
  J-B24FX Jetcore 100M Fibre Module in Slot 2,
  Flash Software Version B2R07604f (router),
  Boot M2 BI Boot Code Version 07.06.02
- Switch Configuration
  J-FXGMR4 Management Module IV in Slot 1,
  J-B24FX Jetcore 100M Fibre Module in Slot 2,
  Flash Software Version B2S07604f (switch),
  Boot M2 BI Boot Code Version 07.06.02

Windows 98 – Serial Host connected to Management Module IV:
J-BxGMR4 / J-FxGMR4 Serial Interface Port

Linux RedHat 9.0 – TCP/IP Host connected to J-B24FX Port 1

Linux RedHat 9.0 – TCP/IP Host connected to J-B24FX Port 15

## 9. Results of the Evaluation

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures (CCEVS_PUB 3). The validator observed that the evaluation and all of its activities were in accordance with the CC, the CEM and CCEVS. The validator therefore, concludes that the evaluation and its results of **pass** are complete.

### 9.1 Assurance Content

The evaluation provides for Assurance at the EAL 2 level without augmentation. The assurance components are shown in the table below:

**EAL2 Assurance Requirements**

| Assurance Class | Assurance Components |
|---|---|
| Configuration Management (ACM) | ACM_CAP.2 Configuration items |
| Delivery and Operation (ADO) | ADO_DEL.1 Delivery Procedures |
| | ADO_IGS.1 Installation, generation, and start-up procedures |
| Development (ADV) | ADV_FSP.1 Informal functional specification |
| | ADV_HLD.1 Descriptive high-level design |
| | ADV_RCR.1 Informal correspondence demonstration |
| Guidance Documents (AGD) | AGD_ADM.1 Administrator guidance |
| | AGD_USR.1 User guidance |
| Tests (ATE) | ATE_COV.1 Evidence of Coverage |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| Vulnerability assessment (AVA) | AVA_SOF.1 Strength of TOE security function evaluation |
| | AVA_VLA.1 Developer vulnerability analysis |

# 10.Validator Comments/Recommendations

***Comments on the evaluated EAL2 configuration:***

The management module running the IOS Version 07.6.04f software is the TOE. The TOE's purpose is to securely manage itself and its accessibility to the Foundry routers and switches that it is configured to interact with. The IronWare™ operating system alone, was not the focus of this evaluation and its purpose, to control the switching and routing of layer 2 and layer 3 frames and packets through Foundry chassis-based switches and routers, was not addressed in this evaluation. The focus of this evaluation was for the IronWare™ operating system, Version 07.6.04f, (which incorporates Foundry Networks' IronShield™ security module) and its security features only.

Throughout this evaluation, both management modules have been referred to by their manufacturing model number, which is printed on the front of each one. Only the model numbers and corresponding software listed below are the evaluated EAL 2 configuration:

J-BxGMR4 Management Module IV or
J-FxGMR4 Management Module IV,
Flash Software Version B2R07604f (router) or
Flash Software Version B2S07604f (switch),
and the IOS version M2 BI Boot Code Version 07.06.02.

***Comments on the delivered product:***

The products delivered as indicated in Section 6 of this report were recorded for this evaluation only. A customer can expect delivery of either the J-BxGMR4 Management Module IV or the J-FxGMR4 Management Module IV, along with the other Foundry products ordered, in a manner similar to that expressed in Section 6. According to the Foundry Software Delivery Procedures, the IOS Version 07.6.04f software must be obtained separately.

***Obtaining the IOS Version 07.6.04f software:***

The Validator notes that the software to successfully configure and run the management modules is obtained in one of two ways: the service representative provides a CD to the customer, containing the CC evaluation software with the Installation, Generation and Start-up instructions; or the customer obtains the CC evaluated software via Foundry's Corporation Web site as explained in the Foundry Network's Corporation Installation, Generation and Start-up guide. It is the customer's responsibility to note during the Installation, Generation and Start-up that the proper CC evaluated boot and flash code is loaded.

***Comments on cryptography:***

The cryptography used in this product to encrypt passwords (MD5 authentication strings), has not been FIPS certified nor was it tested during this evaluation however, encrypted passwords were observed during testing. The password encryption has only been asserted as tested by the vendor.

***Recommendation:***

This evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The product has been evaluated at the assurance level of EAL 2 and it has been determined that it meets its functional claims.

The validator observed that the evaluation and all of its activities were in accordance with the CC the CEM, and CCEVS practices; and that the CCTL presented appropriate CEM work units and rationale. The validator therefore concludes that the evaluation and its results of **pass,** are complete and correct.

## 11. Security Target

The Security Target is provided separately.

**ST:** Foundry Networks Management Module IV: J-BxGMR4 and J-FxGMR4 Security Target v1.0, dated 08 January 2004.

## 12. List Of Acronymns And Glossary Of Terms

The following acronyms are provided for reference:

| | |
|---|---|
| ACM | Assurance Configuration Management |
| ADO | Assurance Delivery and Operation |
| AGD | Assurance Guidance Documents |
| ADV | Assurance Development |
| ATE | Assurance Tests |
| AVA | Assurance Vulnerability Assessment |
| CC | Evaluation Criteria for Information Technology Security (Common Criteria) |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology |
| CLI | Command Line Interface |
| CSC | Computer Sciences Corporation |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| FNC | Foundry Network, Inc. |
| IOS | Ironware Operating System |
| NIST | National Institute of Standards and Technology |
| SF | Security Functions |
| SFR | Security Functional Requirements |
| SFP | Security Function Policy |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | Target of Evaluation Security Functions |
| TSP | TOE Security Policy |

The following terms are provided for reference:

**Target of Evaluation (TOE)** - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions (TSF)** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy (TSP)** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

## 13. Documentation

The evidence used in this evaluation is based upon the product and the following documentation:

FNC Security Target version 1.0 revision 1.21;

CSC ETRs for ACM_CAP.2, ADO_DEL.1, ADO_IGS.1, ADV_FSP.1, ADV_HLD.1, ADV_RCR.1, ADG_ADM.1, AGD_USR.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_SOF.1, AVA_VLA.1 assurance requirements and ASE_ENV.1, ASE_OBJ.1, ASE_REQ.1, ASE_SRE.1, ASE_PPC.1, ASE_TSS.1, ASE_INT.1, ASE_DES.1 for ST evaluation;

[FNC_IGS] Foundry Networks, NIAP 92-01 Common Criteria Installation Startup Guidance Foundry BigIron 4000/8000/15000 Foundry FastIron 400/800/1500;

[FNC_SG] Foundry Networks, Security Guide dated June 2003;

[FNC_CLI] Foundry Networks, Switch and Router Command Line Interface Reference dated May 2003;

[FNC_ICG] Foundry Networks, Installation and Basic Configuration Guide dated May 2003;

[FNC_ECG] Foundry Networks, Enterprise Configuration and Management Guide dated May 2003;

[FNC_ADV] Foundry Networks, JetCore BigIron and FastIron TOE Design;

[FNC_BOM1] Foundry J-BxGMR4 BOM 31181-002P dated 4/15/03;

[FNC_BOM2] Foundry J-FxGMR4 BOM 31181-203P dated 4/15/03;

[FNC_SDP] Foundry Software Delivery Procedures;

[FNC_SRP] Foundry Networks, Software Release Process version 1.8;

[FNC_FOC] Foundry Oracle CM;

[FNC_SOF] Foundry Networks, Strength of Function Analysis v1.1;

[FNC_TST] Foundry Networks, NIAP Common Criteria Testing BigIron and FastIron Switching Routers;

[FNC_COV] Foundry Networks, Management Module IV: JBxGMR4 and J-FxGMR4 Security Target Test Coverage Document;

CSC CCTL Independent Test Plan and Report;

CSC CCTL Penetration Test Plan and Report;

CSC Final ETR;

13 Evaluation Discovery Reports.

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB 2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000

[CCEVS_PUB 3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, January 2002.

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.