

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

Report Number: CCEVS-VR-VID10077-2008
Dated: 11 July 2008
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 6757
Fort George G. Meade, MD 20755-6757

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

ACKNOWLEDGEMENTS

Validation Team

**Dianne Hale
Jerome Myers**

Common Criteria Testing Laboratory

**SAIC, Inc.
Columbia, Maryland**

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

Table of Contents

1	Executive Summary	1
1.1	Interpretations	3
1.2	Threats to Security	3
2	Identification	4
3	Security Policy	4
4	Assumptions.....	5
4.1	Clarification of Scope	6
5	Architectural Information	6
6	Documentation	11
7	IT Product Testing	12
8	Results of the Evaluation	13
9	Validator Comments/Recommendations	13
10	Annexes.....	13
11	Security Target.....	14
12	Glossary	14
	Bibliography	15

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

1 Executive Summary

The evaluation of **Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers** was performed by SAIC, in the United States and was completed in May 2008. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Foundry Networks TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 10, March 2005. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 1.0.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 2 family of assurance requirements augmented with ALC_FLR.1. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Tripwire product by any agency of the US Government and no warranty of the product is either expressed or implied.

The technical information included in this report was obtained from the Evaluation Technical Report for Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers (ETR) Parts 1 and 2 produced by SAIC.

Evaluation Details

Evaluated Product:	Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers: BigIron RX family with IronWare OS version 2.5.00b, NetIron XMR family with IronWare OS version 3.8.00a, NetIron EdgeX family with IronWare OS version 4.1.00; FastIron SuperX series with IronWare OS version 4.1.00; FastIron MLX family with IronWare OS version 3.8.00a; FastIron GS/LS Family with IronWare OS version 4.2.00a; FastIron EdgeSwitch family with IronWare OS version 4.0.00a
Sponsor & Developer:	Foundry Networks, Inc 4980 Great America Parkway Santa Clara, CA 95054
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046

VALIDATION REPORT
 Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
 and Routers

Completion Date:	May 2008
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 2 augmented with ALC_FLR.1
Description	<p>The TOE is composed of a hardware appliance with embedded software installed on the management processor of all routers and switches. The hardware appliance is either a switch or a router and its software is a version of Foundry Networks' proprietary IronWare Operating System (IOS) and the software-based IronShield Security Module. The Foundry IOS controls the switching and routing of layer 2-3 and layer 4-7 network frames and packets through Foundry switch and router appliances.</p> <p>All switches and routers are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI) . However, the TOE should be configured in accordance with the evaluated configuration prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH v2.</p> <p>The TOE consists of the following product families of switches and routers:</p> <ul style="list-style-type: none"> • FastIron (Layer 2-3 Switches) • NetIron (IPv4/IPv6 and Multiprotocol Label Switching (MPLS)Routers) • BigIron (Layer 3 Switches) <p>The hardware platforms that support the TOE have a number of common hardware characteristics:</p> <ul style="list-style-type: none"> • Central processor that supports all system operations, i.e. PowerPC etc. • Dynamic memory, used by the central processor for all system operations • Flash memory, used to store the operating system image • Non-volatile memory, which stores configuration parameters used to initialize the system at system startup • Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

VALIDATION REPORT
 Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
 and Routers

	<p>The basic operation of the switches and routers is as follows:</p> <ol style="list-style-type: none"> 1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap. 2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation. <p>During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.</p>
Disclaimer	<p>The information contained in this Validation Report is not an endorsement of the Tripwire product by any agency of the U.S. Government and no warranty of the Gatekeeper product is either expressed or implied.</p>
PP:	none
Evaluation Personnel	Shukrat Abbas
Validation Team:	

1.1 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

1.2 Threats to Security

The following are the threats that the evaluated product addresses:

- T.ACCESS An attacker may attempt to access the TOE through an external interface in order to alter the TOE configuration or otherwise circumvent the TOE policies so they can access networks/resources for which they are not authorized.

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

T.AUDIT	Attempts by external entities to violate TOE security policies may not be detected.
T.REMOTE	Through the interception of network traffic, an attacker may attempt to obtain or modify TOE management/administrator secrets and configuration data that is either a parameter of TOE administrative commands, or part of a TOE administrative session, in order to gain access to TOE management functions and/or configuration data for the purpose of circumventing and/or altering TOE security policy.

2 Identification

The product being evaluated is Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers. Note that the actual target of evaluation is defined to be only certain parts of the whole product.

3 Security Policy

The following security policies are enforced by the TOE:

- **Security Audit:** TOE generates audit records of user's actions that occur on the TOE. The user actions include management actions, and attempts to login into the TOE. The TOE includes a limited storage buffer, but the records can be stored on a syslog server in the IT environment.
- **Information Flow:** The TOE uses ACLs to control forwarding of network data at specified ports on network equipment to the network and access to the management functions. 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. The ACLs can be used to limit the hosts that can access the TOE and the networks, denying access to all other hosts.
- **Identification and Authentication:** The TOE requires that all users are identified and authenticated before any access to the management functions is permitted. The TOE provides Authentication Method lists, which are used to specify the order in which the authentication mechanisms are employed whenever there are one or more authentication mechanisms available. Authentication mechanisms are the local authentication and external authentication using RADIUS and TACACS/TACACS+ which is provided by an external server in the IT environment.
- **Security Management:** The TOE includes a number of command-line functions to manage its security policies. These functions can be accessed using the Command

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

Line Interface (CLI) (via a directly connected terminal or a remote SSH session). The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

- **TSF protection:** The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

4 Assumptions

The following assumptions are identified in the Security Target:

- | | |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.EAUTH | External authentication services will be available via RADIUS or TACACS/TACACS+. |
| A.FLOW | The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE. |
| A.GOODADM | An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation. |
| A.INSTALL | The TOE has 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.PHYSICAL | The TOE will be appropriately located within facilities providing controlled access to prevent unauthorized physical access and to ensure that the TOE controls the applicable information flows. |

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 augmented with ALC_FLR.1 in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM); seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
- This evaluation does not verify all claims made in the product’s end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5.1 and 6 respectively).
- The following features must be disabled or restricted in the evaluated configuration:
 - SNMP is assumed to be **disabled** in the evaluated configuration.
 - Web Management Access is assumed to be **disabled** in the evaluated configuration.
 - Telnet access is assumed to be used only for local, wired connections (i.e., it is assumed to be **disabled** for remote/network access to the TOE).
 - *Strict Password Enforcement* is assumed to be **enabled** in the evaluated configuration.
- The following features were not evaluated but can be used in the evaluated configuration:
 - 802.1x Authentication, which is an authentication protocol which allows users to be granted or refused access to a local area network based on a set of credentials. In most cases, 802.1x is used with a central RADIUS server.
 - MAC authentication, which grants user access to a local area network based on the PC’s MAC address.
 - BGP Guard, which is a security mechanism associated with the BGP routing protocol. BGP Guard protects your BGP routing topology by restricting the number of router hops the BGP session can traverse.

5 Architectural Information

The TOE consists of the following product families of switches and routers:

- FastIron (Layer 2-3 Switches)
- NetIron (IPv4/IPv6 and Multiprotocol Label Switching (MPLS)Routers)
- BigIron (Layer 3 Switches)

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

The basic operation of the switches and routers is as follows:

3. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
4. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.

Each Ironshield Switch or Router from one of the Ironshield product families (BigIron, NetIron, and FastIron) is a hardware appliance that runs a version of Foundry Networks' IronWare Operating System (IOS) and the software-based IronShield Security Module.

In addition, each IronShield Switch or Router has physical network connections to its environment to facilitate routing and switching of network traffic and can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to a syslog server in the environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can also be configured to use an external authentication service such as a RADIUS or TACACS/TACACS+ using an external server in the environment.

The following are models are the TOE:

BigIron:

- RX family with IronWare OS version 2.5.00b
 - BI-RX-4-AC (4 slot device)
 - BI-RX-8-AC (8 slot device)

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

- BI-RX-16-AC (16 slot device)
- BI-RX-32-AC (32 slot device)

NetIron

- XMR family with IronWare OS version 3.8.00a
 - NI-XMR-4-AC (4 slot device)
 - NI-XMR-8-AC (8 slot device)
 - NI-XMR-16-AC (16 slot device)
 - NI-XMR-32-AC (32 slot device)

- MLX family with IronWare OS version 3.8.00a
 - NI-MLX-4-AC (4 slot device)
 - NI-MLX-8-AC (8 slot device)
 - NI-MLX-16-AC (16 slot device)
 - NI-MLX-32-AC (32 slot device)

FastIron

- SuperX series with IronWare OS version 4.1.00
 - FI-SX1-AC – (8 slot device with single management)
 - FI-SX800-AC – (8 slot device with redundant management)
 - FI-SX1600-AC – (16 slot device with redundant management)

- GS/LS Family with IronWare OS version 4.2.00a
 - FLS624 (24 port stackable)
 - FLS648 (48 port stackable)
 - FGS624P (24 port stackable)
 - FGS624P-POE (24 port stackable with Power over Ethernet)
 - FGS624XGP (24 port stackable with integrated 10 Gig Interface)
 - FGS624XGP-POE (24 port stackable with integrated 10 Gig Interface with Power over Ethernet)
 - FGS648P (48 port stackable)
 - FGS648P-POE (48 port stackable with Power over Ethernet)

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

- Edge X family with IronWare OS version 4.1.00
 - FESX424 (24 port stackable)
 - FESX424-PREM (24 port stackable with full L3 support)
 - FESX424+1XG (24 port stackable with one port 10 Gig Interface)
 - FESX424+1XG-PREM (24 port stackable with one port 10 Gig Interface with full L3 support)
 - FESX424+2XG (24 port stackable with two port 10 Gig Interface)
 - FESX424+2XG-PREM (24 port stackable with two port 10 Gig Interface with full L3 support)
 - FESX448 (48 port stackable)
 - FESX448-PREM (48 port stackable with full L3 support)
 - FESX448+1XG (48 port stackable with one port 10 Gig Interface)
 - FESX448+1XG-PREM (48 port stackable with one port 10 Gig Interface with full L3 support)
 - FESX448+2XG (48 port stackable with two port 10 Gig Interface)
 - FESX448+2XG-PREM (48 port stackable with two port 10 Gig Interface with full L3 support)
 - FESX424HF (24 port stackable (100FX/1000X))
 - FESX424HF-PREM (24 port stackable (100FX/1000X) with full L3 support)
 - FESX424HF+1XG (24 port stackable (100FX/1000X) with one 10 Gig Interface)
 - FESX424HF+1XG-PREM (24 port stackable (100FX/1000X) with one 10 Gig Interface with full L3 support)
 - FESX424HF+2XG (24 port stackable (100FX/1000X) with two 10 Gig Interface)
 - FESX424HF+2XG-PREM (24 port stackable (100FX/1000X) with two 10 Gig Interface with full L3 support)
 - FESX424-POE (24 port stackable with Power over Ethernet)
 - FESX424-POE+1XG (24 port stackable with one port 10 Gig Interface and Power over Ethernet)
 - FESX424-POE+2XG (24 port stackable with two port 10 Gig Interface and Power over Ethernet)
 - FESX624 (24 port stackable with hardware based IPv6 support)
 - FESX624-PREM (24 port stackable with hardware based IPv6 support and full L3 support)
 - FESX624+2XG (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces)

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

- FESX624+2XG-PREM (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
- FESX648 (48 port stackable with hardware based IPv6 support)
- FESX648-PREM (48 port stackable with hardware based IPv6 support and full L3 support)
- FESX648+2XG (48 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces)
- FESX648+2XG-PREM (48 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
- FESX624HF (24 port stackable with hardware based IPv6 support (100FX/1000X))
- FESX624HF-PREM (24 port stackable with hardware based IPv6 support and full L3 support (100FX/1000X))
- FESX624HF+2XG (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces (100FX/1000X))
- FESX624HF+2XG-PREM (24 port stackable with hardware based IPv6 support and 2 10 Gig Interfaces and full L3 support)
- Edge Switch family with IronWare OS version 4.0.00a
 - FES2402 (24 port stackable)
 - FES2402-PREM (24 port stackable with full L3 support)
 - FES4802 (48 port stackable)
 - FES4802-PREM (48 port stackable with full L3 support)
 - FES9604 (96 port stackable)
 - FES9604-PREM (96 port stackable with full L3 support)
 - FES12GCF (12 port stackable)
 - FES12GCF-PREM (12 port stackable with full L3 support)
 - FES2402-POE (24 port stackable with Power over Ethernet)
 - FES2402-POE-PREM (24 port stackable with full L3 support and Power over Ethernet)
 - FES4802-POE (48 port stackable with Power over Ethernet)
 - FES4802-POE-PREM (48 port stackable with full L3 support and Power over Ethernet)

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

6 Documentation

Following is a list of useful documents supplied by the developer when download from the Foundry Networks website or shipped with the product.

Evaluated:

- Foundry Switch and Router Command Line Interface Reference, December 2007
- Foundry Security Guide, December 2007

BigIron:

- Foundry BigIron RX Series Installation Guide, March 2008
- Foundry BigIron RX Series Configuration Guide, June 2008
- Foundry Switch and Router Installation and Basic Configuration Guide, December 2007

FastIron

- Foundry FastIron Compact Switch Hardware Installation Guide, December 2007
- Foundry FastIron Configuration Guide, June 25 2008
- Foundry FastIron GS Compact Layer 2 Switch POE and POE-Upgradeable Hardware Installation Guide, December 2007
- Foundry FastIron LS Layer 2 Compact Switch Hardware Installation Guide, December 2007
- Foundry FastIron X Series Chassis Hardware Installation Guide, November 2007
- Foundry FastIron Compact Switch Hardware Installation Guide, December 2007

NetIron:

- Foundry NetIron MLX Series Installation and Basic Configuration Guide, December 2007
- Foundry NetIron XMR Series Installation and Basic Configuration Guide, December 2007
- Foundry NetIron XMR/MLX Configuration Guide, April 2008

Not evaluated:

- Foundry Management Information Base Reference
- Release notes
- Patch Release Notes
- ReadMe
- MD5_Checksums

The security target used is:

- Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Target, version 0.92, July 10, 2008

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

7 IT Product Testing

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The following tasks were performed by the evaluation team:

- The developer test suite was examined and found to provide adequate coverage of the security functions.
- A selection of the developer tests were run and the results found to be consistent with the results generated by the developer.
- No vulnerabilities in the TOE were found during a search of vulnerability databases.
- Tests devised from postulated vulnerabilities in the I&A mechanism revealed no problems.

The following models were actually tested;

NetIron XMR Family (modular)

- NI-XMR-4-AC (4 slot device)
Code Release – IronWare OS version 3.8.00a

NetIron MLX Family (modular) – TOE-MLX

- NI-MLX-4-AC (4 slot device)
Code Release – IronWare OS version 3.8.00a

BigIron RX Family (modular) - hostname: TOE-RX

- BI-RX-4-AC (4 slot device)
Code Release – IronWare OS version 2.5.00b

FastIron EdgeX Family (stackable -10/100/1000)

- FESX424HF-PREM (24 port stackable (100FX/1000X) with full L3 support)
Code Release - IronWare OS version 4.1.00

FastIron EdgeSwitch Family (stackable-10/100)

- FES2402-PREM (24 port stackable with full L3 support)
Code Release - IronWare OS version 4.0.00a

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

FastIron SuperX Series (modular) – hostname: TOE-SX

- FI-SX1-AC (8 slot device with single management)

Code Release – IronWare OS version 4.1.00

FastIron GS/LS Family (stackable-10/100/1000)*

- FGS624P (24 port stackable)
- FLS648 (48 port stackable)

Code Release – IronWare OS version 4.2.00a

The chosen models are a sample set of the models that are considered the TOE. The set is deemed adequate because the only differences between the models with a given family is the number of interface slots available with the chassis and media type. The chassis sizes range from 4, 8, 16, and 32 slots. Stackable devices provide either 24 or 48 ports and are either copper or fiber based.

8 Results of the Evaluation

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

9 Validator Comments/Recommendations

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. Some limitations and clarifications of the evaluated product are summarized in Section 4.1 of this document. In addition the following problem was identified by the CCTL during evaluation.

Error with the command used to change a user's password.

Existing usernames and passwords configured on a Foundry Device with specific privilege levels (super-user, read-only, port-config) can be escalated to the super-user privilege level if the users' password is changed without including the user's privilege level option in the syntax. The issue is documented in the NIAP-CCEVS Certification Appendix A to the Foundry Security Guide and in the Configuration Guides.

10 Annexes

Not applicable.

VALIDATION REPORT

Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches and Routers

11 Security Target

The security target for this product's evaluation is **Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Target, version 0.92, July 10, 2008**

12 Glossary

There were no definitions used other than those used in the CC or CEM.

VALIDATION REPORT
Foundry Networks IronShield (BigIron, NetIron, FastIron, and FastIron Edge) Switches
and Routers

Bibliography

The Validation Team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.
- [2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.
- [3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.
- [4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.
- [5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.
- [6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.
- [7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
- [8] Evaluation Technical Report for Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Part II, version 1.0 July 10, 2008
- [9] Foundry Networks IronShield (BigIron, NetIron, and FastIron) Switches and Routers Security Target, version 0.92, July 10, 2008.
- [10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001