

---

# **CHENGDU HUAWEI STORAGE & NETWORK SECURITY CO., LTD.**

**Quidway Eudemon Firewall Product Group**  
**Quidway Eudemon 500 & 1000**  
**VRP 3.30-0358(10)**

## **Introduction**

Not every product can achieve ICSA Labs Firewall Certification. Only those products that meet the criteria after undergoing rigorous testing by firewall experts at ICSA Labs earn this distinction.

Products which have achieved ICSA Labs Firewall Certification remain continuously deployed within the ICSA Labs Network Security Lab where they are available for continued testing for the length of the testing contract. Products are subjected to supplemental spot-check testing when new attack techniques emerge and vulnerabilities become known. Spot-check tests are also performed on a periodic basis to verify that updated product versions continue to meet the ICSA Labs Firewall Certification criteria.

In the event that a product fails spot-check tests, the vendor is required to provide adequate fixes within a prescribed length of time. Once these fixes have been verified by the Network Security Lab, a report is written which documents the product shortcomings found and provides information about the nature of the fixes including any changes to the configuration of the product as well as any patches or updates to components submitted by the vendor. Failure to provide adequate fixes will cause the product's ICSA Labs Firewall Certification to be revoked.

Successful spot-check testing ends with the writing of a report which documents any product shortcomings found and provides information about any required fixes including any changes to the configuration of the product as well as any patches or updates to components submitted by the vendor.

## **Background**

### **Section Introduction**

Products subjected to spot-check testing have been previously tested and have an existing ICSA Labs Firewall Certification. This section of the report provides information about previous testing and the circumstances leading to the product being selected for spot-check testing.

### **Previous Testing**

The Quidway Eudemon Firewall Product Group consisted of two Firewall Product Families. One family was the Quidway Eudemon 200 (E200) by itself and the other consisted of the Quidway Eudemon 500 (E500) and the Quidway Eudemon 1000 (E1000). The E200 was the first product of the Quidway Eudemon Firewall Product Group to be tested.

The Quidway Eudemon 200 (E200) was successfully tested against the following modules from version 4.1 of *The Modular Firewall Certification Criteria*:

- *Baseline module*,  
<http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/baseline.pdf>
- *Logging Update – version 4.1a*,  
[http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/4.1a\\_logging.pdf](http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/4.1a_logging.pdf)
- *Required Services Security Policy – Corporate Category module*,  
<http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/corporate.pdf>

The most recent full test cycle was performed with VRP version 3.30-0358(11). The 4.1a Firewall Lab Report dated October 10, 2007 documenting this testing can be found at:

- <http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/huawei.pdf>

### **Circumstances of Spot-Check**

To complete testing of the Quidway Eudemon Firewall Product Group, the E500 and E1000 were subjected to spot-check testing to ensure that they, like the E200, met ICSA Labs Firewall Certification Criteria requirements.

## **Candidate Firewall Product Components**

### **Section Introduction**

The set of hardware, software, and documentation components delivered to ICSA Labs for testing are collectively called the “Candidate Firewall Product” or “CFP.” Updated CFP components may have been submitted prior to spot-check testing. In the event of a product failing spot-check tests, updated hardware, software, or documentation will be required in order to successfully maintain its ICSA Labs Firewall Certification. This section of the report describes any updates made to the CFP components submitted prior to or during the course of spot-check testing.

### **Hardware**

Like the E200, the E500 and E1000 were 3U rack-mountable firewall appliances with IBM PowerPC 750 processors, 256 MB memory, and 32 MB flash storage. They all also had two built-in 10/100 Ethernet network interfaces and two serial ports.

Unlike the E200, which had two unpopulated module slots, the E500 and E1000 each had four module slots. The E500 and E1000 each contained an 8 port 10/100 Ethernet network interface module.

The dedicated logging server used for the E200 testing continued to be used for the E500 & E1000 and remained the same as previously tested.

### **Software**

The E1000 was initially configured using VRP version 3.30-0357(08) and in conjunction with testing of the E200, was upgraded to version 3.30-0358(09) and later successfully completed spot-check testing with version 3.30-0358(10).

The E500 was initially configured using VRP version 3.30-0358(10), which successfully completed spot-check testing without any fixes needed.

Customers of Huawei Technologies can obtain updates at <http://support.huawei.com>.

The software on the dedicated logging server used for the E200 testing continued to be used for the E500 & E1000 and remained the same as previously tested.

## Documentation

To satisfy documentation requirements, Chengdu Huawei Storage & Network Security Co., Ltd. provided the Network Security Lab team with the following electronic documents in order to assist in the installation, configuration, and administration of the E500 & E1000:

- *Qidway Eudemon Series Quick Start, Issue 01 (2006-08-25)*
- *Qidway Eudemon 500/1000 Firewall Installation Manual, T2-080460-20050916-C-1.02*
- *Qidway Eudemon 500/1000 Firewall Operations Manual, T2-081697-20051015-C-1.01*
- *Qidway Eudemon 500/1000 Firewall Command Reference, T2-081997-20051015-C-1.01*

Documentation defining log event dispositions was found in:

- *Log Event Dispositions of Eudemon V1.1, VRP Version 3.30*

## Configuration

The tested configuration of the E500 & E1000 was substantially the same as that tested on the E200, with the following differences:

- The E200 was configured to use the two built-in 10/100 Ethernet network interface ports. The E500 & E1000 were instead configured to use ports on their 8 port 10/100 Ethernet network interface modules and the built-in ports were not used.
- Due to a difference in logging configuration options, the E500 & E1000 logging configuration for “firewall interzone trust untrust” specified separately the inbound acl and outbound acl to be logged. On the E200, enabling logging for the “firewall interzone trust untrust” without specifying an acl automatically enabled logging for both inbound and outbound acls defined for that “interzone.”
- A “firewall defend ip-options” feature not available on the E200 was configured on the E500 & E1000.

## Criteria Violations and Resolutions

### Section Introduction

In the event that the Network Security Lab team discovers or confirms criteria violations while performing spot-check tests of the Candidate Firewall Product, the vendor must make repairs before spot-check testing can be completed and certification retained. The section that follows documents any and all criteria violations discovered or confirmed during testing. Additionally any steps that must be taken by an administrator to ensure that the product meets the criteria are documented below.

### Results

In addition to criteria violations found and fixed during testing of the E200, an additional problem unique to the E1000 was found:

- The firewall rules could be bypassed by packets with certain extra data included.

This was found to be corrected in VRP version 3.30-0358(10). As the E500 was tested only with 3.30-0358(10) after the E1000 successfully completed testing, this problem was not seen on the E500 although it may have existed in previous VRP versions.

## Miscellaneous Notes

### Section Introduction

Observations, general notes, and/or specific comments collected during testing by the Network Security Lab team that did not fall neatly into one of the preceding sections are included below. Note that all observations and comments that follow may be subjective and may have had no bearing on the product passing or failing to meet the criteria.

### Network Security Lab Comments

The E200 had a criteria violation regarding a Denial-of-Service attack when it was configured to block all fragmented packets, which was fixed in VRP version 3.30-0358(11). This problem did not exist on the E500 & E1000, and therefore they were able to successfully pass testing with VRP version 3.30-0358(10).

Another criteria violation found on the E200 related to FTP extended responses was also not found to exist on the E500 & E1000.

## Conclusion

Successful spot-check testing of the Quidway Eudemon 500 & 1000 indicated that the products met all the criteria elements in the Baseline and Required Services Security Policy – Corporate Category modules and therefore have joined the Quidway Eudemon 200 in obtaining ICSA Labs Firewall Certification.

## Testing Information

### Lab Report Date

January 11, 2008

### Test Location

ICSA Labs  
1000 Bent Creek Blvd., Suite 200  
Mechanicsburg, PA 17050  
USA

### Product Headquarters

Chengdu Huawei Storage & Network Security Co., Ltd.  
Harbour Networks P&D Center. Building 17  
ZhongGuanCun Software Park  
No.8, Dongbeiwang West Road  
Hai-Dian District Beijing P.R.China  
100094

### Copyright

Copyright © 2008 Cybertrust, Inc. All Rights Reserved. No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express permission in writing from ICSA Labs. ICSA Labs is a division of Cybertrust, Inc and is a registered mark of Cybertrust, Inc.