

4.1a Firewall Spot-Check Lab Report



Microsoft Corporation Internet Security and Acceleration Server 2006 Version 5.0.5721.240

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 Internet Security and Acceleration (ISA) Server 2006 was successfully tested against the following modules from version 4.1a 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

- *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 ISA Server 2004 version 4.0.3443.594. The 4.1a Firewall Lab Report dated June 1, 2007 documenting this testing can be found at:

- <http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/ISA2004.pdf>

Circumstances of Spot-Check

The ISA Server 2006 was selected for spot-check testing when Microsoft Corporation released Internet Security and Acceleration Server 2006 version 5.0.5721.240.

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

The ISA Server 2006 hardware components tested remained the same as previously tested with ISA Server 2004.

Software

Prior to spot-check testing, the ISA Server 2004 version 4.0.3443.594 was upgraded to ISA Server 2006 version 5.0.5721.240.

Documentation

Updated documentation regarding installation and configuration options can be found at:

- <http://www.microsoft.com/isaserver/techinfo/guides-articles.msp>

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

As no criteria violations were discovered while testing ISA Server 2006, the vendor was not required to supply any fixes. No additional steps or configurations were necessary in order for testing to be completed.

Conclusion

Successful spot-check testing of the ISA 2006 indicated that the product continued to meet all the criteria elements in the Baseline and Corporate modules and therefore has retained ICSC Labs Firewall Certification.

Testing Information

Lab Report Date

February 14, 2008

Test Location

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

Product Headquarters

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
USA

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.