

---

# Microsoft Corporation

## Internet Security and Acceleration Server 2004 SP2

### v4.0.3443.594

#### 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.

The criteria against which vendor-submitted products are tested is an industry-accepted standard to which a consortium of firewall vendors, end users, and the ICSA Labs staff contributed. This standard has evolved over the years into its present iteration – version 4.1 of *The Modular Firewall Certification Criteria*.

The setting for testing is the Network Security Lab at ICSA Labs. During and following initial testing, products remain continuously deployed within this lab environment, which closely approximates the real Internet to ensure more realistic firewall testing. Products are available for and regularly subjected to supplemental testing as new attack techniques emerge and vulnerabilities become known. Only products that continue to meet the criteria under these circumstances retain certification.

Successful firewall product testing culminates in the writing of a report that documents the results of each phase of testing. It also documents the product components submitted by the vendor, the configuration of the product as tested, any patches or updates generated during testing, and the mandatory and optional criteria modules against which the product was tested.

#### Candidate Firewall Product Components

##### Section Introduction

To comply with the requirements stated in version 4.1 of *The Modular Firewall Certification Criteria*, vendors must submit all necessary product hardware, software, and documentation. Collectively, the set of components delivered to ICSA Labs for testing comprises the product under test, called the “Candidate Firewall Product” or “CFP”. This section of the report describes each component of the Candidate Firewall Product submitted for testing in the Network Security Lab at ICSA Labs.

##### Hardware

The Microsoft Internet Security and Acceleration (ISA) Server 2004 SP2 in the Network Security Lab was installed on a system with an Intel Pentium 4 2.6 GHz processor with 512 MB RAM. The system also had a 40 GB hard disk drive and two Ethernet 10/100 network interface cards.

## Software

The operating system the ISA Server 2004 was installed on was a Windows Server 2003 R2. The Network Security Lab Team applied Windows 2003 Service Pack 1 to the base operating system as well as allowing the operating system to run the critical updates from Microsoft's automated update site as per the vendor's written instructions. Service pack 1 was downloaded from <http://www.microsoft.com/> and the critical updates were installed using <http://windowsupdate.microsoft.com>.

The ISA Server 2004 version tested in the Network Security Lab was version 4.0.3443.594 SP2 for Standard Edition and Enterprise Edition. Microsoft provided a certificate key for the ISA Server 2004 software and Windows Server 2003 R2 operating system.

In order for Microsoft ISA Server 2004 customers to retrieve the latest version they may find the appropriate contact phone number for their technical support representatives and product update information at <http://www.microsoft.com/technet/downloads/isa/2004/servicepacks/default.mspx> or by using Microsoft automated update service at <http://windowsupdate.microsoft.com>.

## Documentation

To satisfy documentation requirements, Microsoft Corporation provided the Network Security Lab team with the following electronic (html/doc) documents in order to assist in the installation, configuration, and administration of ISA Server 2004 SP2:

- *Deployment Guidelines for ISA Server 2004 Enterprise Edition, April 5, 2005*  
<http://www.microsoft.com/technet/prodtechnol/isa/2004/deploy/dgisaserver.mspx>
- *Deployment Recommendations for ISA Server 2004 in a Workgroup or Domain, April 5, 2006,*  
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/domainworkgroup.mspx>
- *ISA Server 2004 Service Pack 2, January 30, 2006*  
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/sp2.mspx>
- *ISA Server 2004 Enterprise Edition Quick Start Guide, January 2005,*  
<http://download.microsoft.com/download/3/e/2/3e2ae4a2-67a0-4431-88aa-dda29e592e3c/isaequickstart.doc>
- *ISA Server 2004 Enterprise Edition Configuration Guide, January 2005,*  
[http://download.microsoft.com/download/6/9/0/690d2ee7-a4e0-4c0a-80d4-1e30ebcac1de/isa\\_2004\\_ee\\_configuration\\_guide.doc](http://download.microsoft.com/download/6/9/0/690d2ee7-a4e0-4c0a-80d4-1e30ebcac1de/isa_2004_ee_configuration_guide.doc)
- *Best Practices for Configuring Networks in ISA Server 2004, November 2, 2005,*  
[http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/bp\\_networks.mspx](http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/bp_networks.mspx)
- *Best Practices Firewall Policy for ISA Server 2004, May 3, 2005,*  
[http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/firewall\\_policy.mspx](http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/firewall_policy.mspx)

Documentation defining log event dispositions was found in:

- *Best Practices: Logging, December 9, 2005*  
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/logging-best-practices.mspx>

The minimum hardware requirements for the ISA Server 2004 SP2 components were defined at:

- *Getting Started Guide, October 20, 2004*  
[http://www.microsoft.com/technet/isa/2004/plan/gettingstarted\\_3.mspx](http://www.microsoft.com/technet/isa/2004/plan/gettingstarted_3.mspx)

## Firewall Certification Criteria

The Candidate Firewall Product was 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>
- *Required Service Security Policy – Corporate Category module*,  
<http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/corporate.pdf>

Additionally, as described further in the Criteria Violations and Resolutions section below, this product was tested against updated logging criteria:

- *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)

## Candidate Firewall Product Configuration Tested

### Section Introduction

Often, firewall products can be configured many different ways. Therefore the Network Security Lab team frequently confronts many configuration-related decisions before ever adding a single security policy rule on the Candidate Firewall Product. Since the Network Security Lab team attempts to exploit the Candidate Firewall Product, configuration decisions are made to facilitate exploitation. Decisions that the Network Security Lab team must make often include whether or not to use:

- Bridge versus router mode;
- Proxied versus filtered network services;
- NAT versus straight-thru (non-NAT) mode – for outbound services;
- Straight-thru, port forwarding, or 1-to-1 public-to-private IP mapping – for inbound services;
- DNS servers on the Candidate Firewall Product itself rather than at a separate host or ISP;
- Additional network interfaces for server protection and network segregation.

### Candidate Firewall Product Configuration

The ISA Server 2004 SP2 was configured as a stand alone product that must be installed on a supported operating system. During installation the Network Security Lab team selected to use “Firewall” mode with the ISA Server 2004 SP2. This enabled Network Address Translation for private clients accessing the public network. Port forwarding was used to provide Required Service Security Policy (RSSP) services to public clients. DNS could not be hosted on the product and therefore, like all other RSSP services, a DNS server was made available and properly configured for address and name resolution on the private LAN.

## Default Install Posture

### Section Introduction

The following section documents the Candidate Firewall Product's default stance. After being installed, Candidate Firewall Products must drop or deny all attempts to send non-administration-related traffic inbound to or through the product. To arrive at the default Candidate Firewall Product posture, the Network Security Lab team follows the installation documentation provided by the vendor. When choices are available during installation the Network Security Lab team chooses what will help the Candidate Firewall Product meet the default installation criteria requirements.

### Results

After installation of Windows Server 2003 R2 with SP1 and allowing the operating system to run all of the automated critical updates, the Network Security Lab team installed the ISA Server 2004 SP2 using the documents *ISA Server 2004 Enterprise Edition Quick Start Guide*, *Deployment Guidelines for ISA Server 2004 Enterprise Edition*, *Best Practices for Configuring Networks in ISA Server 2004* and finally the *Getting Started Guide*.

The Network Security Lab team performed port scans to determine the default install security posture. The port scans were followed by additional scans to ensure that the ISA server 2004 SP2 public interface neither accepted, nor passed inbound through the product, any non-administration-related TCP, UDP, ICMP, or other IP protocol traffic.

By default, all TCP, UDP, ICMP and other IP protocol traffic was denied from passing inbound or outbound through the ISA Server 2004. In addition, all traffic sent to the public interface was denied.

As no traffic was allowed inbound and no services on the product were available to the public network, the ISA Server 2004 SP2 met all default installation criteria requirements without requiring any additional configurations.

## Required Services Security Policy Transition

### Section Introduction

Each phase of Candidate Firewall Product testing is performed predominantly while enforcing a particular security policy. Firewall products must be configurable to minimally enforce the security policy spelled out in *The Modular Firewall Certification Criteria*, commonly referred to as the "Required Services Security Policy" or "RSSP". The RSSP permits a set of common Internet services inbound and outbound while dropping or denying all other network service traffic. Additionally, products tested against the Corporate category RSSP must be able to support additional, non-specified network services thereby enforcing a security policy different than the RSSP.

### Results

The Network Security Lab team performed the following actions during the transition from the default install security posture to the RSSP:

- Under "Arrays" -> "Network" -> "Internet Access" rule was added for NAT by using the right hand window pane and choosing "Create Network".
- Under "Arrays" -> "Firewall Policy" and by right clicking the "Firewall Policy" link in the left hand window pane and choosing "New" -> "Access Rule", a group was created that included individual rules for DNS, FTP, HTTP, HTTPS, IMAP, POP3, SMTP, and Telnet for the outbound direction.

- Under “Arrays” -> “Firewall Policy” and by right clicking “Firewall Policy” and choosing “New”-> “Server Publishing Rule”, separate rules were created by following the wizard and allowing the following inbound protocols using NAT: DNS, FTP, HTTP, HTTPS, IMAP, POP3, and SMTP.
- As per the Corporate Criteria module requirements, an inbound rule that allowed SSH was added under “Arrays” -> “Firewall Policy” and by right clicking “Firewall Policy” and choosing “New”-> “Server Publishing Rule”, and following the wizard.

The Network Security Lab team performed port scans followed by additional scans and other tests to ensure that the ISA Server 2004 SP2 was indeed configured according to the RSSP and that no other TCP, UDP, ICMP, or other IP protocol traffic was permitted to or through the product in either direction.

After performing the scans mentioned above, the Network Security Lab team then verified that the product properly handled outbound active and passive mode FTP, HTTP, HTTPS, SMTP, DNS, IMAP, and POP3 service requests. Additionally, the Network Security Lab team then verified that the product properly handled inbound active and passive mode FTP, HTTP, HTTPS, SMTP, DNS, IMAP, and POP3 service requests. And the Network Security Lab team verified that the product denied inbound Telnet traffic while properly permitting outbound Telnet traffic. Finally the Network Security Lab team confirmed that no other traffic was permitted to traverse the ISA Server 2004 SP2 in either direction, as expected.

## Logging

### Section Introduction

Version 4.1 of *The Modular Firewall Certification Criteria* requires that the Candidate Firewall Product provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default. However, the capability must exist on Candidate Firewall Products in the event that occasions calling for detailed logging usage arise.

The Network Security Lab team tests the logging functionality provided by the Candidate Firewall Product ensuring that all permitted and denied traffic can be logged for traffic sent both to and through the product. Among the other events that must be logged are security policy changes and administrative login attempts. The Network Security Lab team either configures the local logging mechanism or a remote logging mechanism such as syslog. For all logged events the Network Security Lab team verifies that all necessary log data is recorded.

### Results

The ISA Server 2004 SP2 stored its log files locally. The logs that were generated from the ISA Server 2004 SP2 were located in the “C:\Programs Files\Microsoft ISA Server\ISALogs\” directory in files named FWSEXTDyyyymmdd.log and IPSEXTDyyyymmdd.log, where yyyy was the Year, mm was the two digit Month, and dd was the two digit Day. Log files starting with “FW” were events logged by the firewall engine, and files starting with “IP” were events logged by the packet filter engine. Log events for authentication were accessed using the “Start -> Applications -> Administrative Tools -> Event Viewer” application.

The following logged events were taken from the local firewall logs. The first logged event was an allowed outbound FTP session, the second logged event was denied inbound telnet session and the third logged event was an allowed inbound SSH session.

```

5/30/2007 12:56:36 PM    0    0    0    0x0    0x0    0x0
5/30/2007 8:56:36 AM    205.160.68.66    205.160.60.66    33177
21    FTP    Initiated Connection    Outbound RSSP    Internal
External    FW    Firewall    TCP    205.160.68.66

```

```

5/30/2007 12:32:25 PM    0    0    0    0xc004000d
FWX_E_POLICY_RULES_DENIED    0x0    0x0    5/30/2007    8:32:25    AM
    205.160.60.66    205.160.60.8 51591 23    TelnetDenied
Connection [Enterprise] Default ruleExternal    Local Host    FW
    Firewall    TCP    205.160.60.66

5/30/2007 9:04:23 AM    205.160.60.66    205.160.68.66    51593
22    ssh server    Initiated Connection    Inbound SSH External
Internal    FW    Firewall    TCP    0.0.0.0

```

The ISA Server 2004 SP2 did not initially meet all of the logging requirements. Refer to the “Criteria Violations and Resolutions” section for information concerning the logging problems found during testing.

## Administration

### Section Introduction

Firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor-provided administration software, from a web browser-based interface, via some non-networked connection such as a serial port, or via some other means, authentication must be possible before access to administrative functions is gained. The Network Security Lab team tests not only that authentication mechanisms exist but also that they cannot be bypassed for all required administrative interfaces.

### Results

The ISA Server 2004 SP2 was primarily administered locally using the ISA Server administrative console. Remote administration could be used after configuring Terminal Services from a public host.

Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

## Persistence

### Section Introduction

Power outages, electrical storms, and inadvertent power losses should not cause the Candidate Firewall Product to lose valuable information such as the security policy being enforced, log data, and authentication data, and time. Further, the security policy being enforced following the restoration of power should be the same as the security policy being enforced prior to the loss of power. This section documents the findings of the Network Security Lab team while testing the Candidate Firewall Product against the persistence requirements.

### Results

The ISA Server 2004 SP2 had no problems continuing to enforce the security policy when power was restored following a forced power outage. Additionally, the product continued to maintain the time, date, authentication data and log data.

## Functional and Security Testing

### Section Introduction

Once configured to enforce a security policy the Candidate Firewall Product should “properly” permit the services allowed by that policy. In this case, “properly” means that the service functions correctly. The Candidate Firewall Product must be capable of preventing the well-known, potentially harmful behavior found in some network protocols while at the same time being compliant with their RFCs in all other ways. In the event of a conflict, the product must be configurable for the more secure option. During functional testing the Network Security Lab team checks to ensure proper protocol behavior on the permitted services.

During security testing the Network Security Lab team uses commercial, in-house-created, and freely-available testing tools to attack and probe the Candidate Firewall Product. The Network Security Lab team uses these tools to attempt to defeat or circumvent the security policy enforced on the Candidate Firewall Product. Additionally, using trivial Denial-of-Service and fragmentation attacks the Network Security Lab team attempts to overwhelm or bypass the Candidate Firewall Product.

Since there is overlap between functional and security testing, the results of both phases of testing are presented in the section below.

### Results

The Network Security Lab team confirmed that the ISA Server 2004 SP2 permitted the services in the Required Services Security Policy properly and that the configured services functioned correctly. Furthermore, the product was not circumvented by the attacks launched inbound and outbound to and through the ISA Server 2004 SP2. Finally, the product was not defeated by trivial Denial-Of-Service and fragmentation attacks.

## Criteria Violations and Resolutions

### Section Introduction

In the event that the Network Security Lab team uncovers criteria violations while testing the Candidate Firewall Product, the vendor must make repairs before testing can be completed and certification granted. The section that follows documents any and all criteria violations discovered during testing. Additionally any steps that must be taken by an administrator to ensure that the product meets the criteria are documented below.

### Results

The ISA Server 2004 SP2 does not log raw IP Protocols without data. As per *The Modular Firewall Certification Criteria, Logging Update – Version 4.1a*, this is acceptable provided that 1) the product cannot be configured to allow this traffic and 2) this is documented. Microsoft produced additional documentation to meet this requirement.

- *Knowledge Base article number 936905, May 9, 2007, <http://support.microsoft.com/kb/936905/en-us>*

## 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 product was managed primarily by using the local interface. The remote administrative interface was disabled by default.

When defining the "IP Packet Filters" rule to allow the Terminal Services client to connect for remote administration it was required that access was restricted to one IP address. This is required so that administrative log events can be correlated between log files.

## Conclusion

The Candidate Firewall Product met all the criteria elements in the Baseline and Corporate modules and therefore has retained ICSA Labs Firewall Certification. The Candidate Firewall Product will remain continuously deployed at ICSA Labs for the length of the testing contract and will be periodically checked as new attacks and vulnerabilities are discovered. In the event that the Candidate Firewall Product is found susceptible to new attacks or vulnerabilities during a check, the Network Security Lab team will work with the vendor to resolve the problems in order for the Candidate Firewall Product to maintain its ICSA Labs Firewall Certification.

## Certification Maintenance on Future Versions

The ISA Server 2004 SP2, like all products and product groups that are granted ICSA Labs Firewall Certification, will remain certified on this and future released versions of the product for the length of the testing contract. Future versions continue to be certified since the product is continuously deployed in the Network Security Lab and subjected to periodic spot-checks on the most current product version.

Three circumstances will cause the ISA Server 2004 SP2 to have its ICSA Labs Firewall Certification revoked:

1. Microsoft Corporation withdraws from the ICSA Labs Firewall Certification Program.
2. The product fails a periodic spot-check and Microsoft Corporation subsequently fails to provide an adequate fix within a prescribed length of time.
3. The product fails to meet the next full test cycle against the current version of the criteria.

## Testing Information

### Lab Report Date

June 1, 2007

### 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

### Copyright

Copyright © 2007 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.