

4.1 Firewall Lab Report



Jungo Software Technologies

OpenRG Software Platform v. 3.10

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.

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 vendor provided a US Robotics 8200, running on a single Intel IXP425 processor and including 64 MB SDRAM. The product also had four switched 10/100BaseTX Local Area Network (LAN) ports, one switched 10/100BaseTX Wide Area Network (WAN) port and one 9-pin serial port. In addition the product included a USB port that was not used during testing.

Software

The product came pre-installed with and successfully completed testing with firmware image OpenRG v. 3.10.

In order for OpenRG customers to retrieve the latest software version they can visit their technical support web site at http://www.jungo.com/support/support_main.html for this and all other product update information.

Documentation

To satisfy documentation requirements, Jungo provided the Network Security Lab team with the following electronic (.pdf) document in order to assist in the installation, configuration, and administration of OpenRG:

- *User Manual - OpenRG version 3.10, DOC-UM-3107-09-03*

Documentation defining log event dispositions was found in:

- *User Manual - OpenRG version 3.10, page 88*

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](#)
- [Required Services Security Policy – Corporate Category module](#)

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 Jungo OpenRG was an integrated software platform. OpenRG was designed and installed on a router-based appliance that performed stateful packet inspection. By default, the USR 8200 was configured for Many-to-1 NAT outbound. The product was configured in port forwarded mode for inbound and NAT mode for outbound services. The Network Security Lab team was unable to host DNS on the product and therefore, like all other Required Service Security Policy services, a DNS server was made available and properly configured for address and name resolution on the private LAN. The Jungo OpenRG also had a DHCP server available to the private LAN, which was on by default but disabled for testing.

Default Install Posture

Section Introduction

The following section documents the Candidate Firewall Products 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

The OpenRG was configured following the instructions found in the OpenRG User Guide. IP addresses were defined for the public and private interfaces. The default DHCP server for the private network was disabled.

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 OpenRG 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 traffic was denied from passing inbound through the OpenRG. Outbound traffic was allowed for the RSSP services by default. In addition, the OpenRG did not respond to ICMP echo request sent directly to its public interface. All traffic sent to the public interface was denied.

The table below contains a description of the services determined to be listening on the OpenRG itself immediately upon completing installation. The “Available To” column describes to which set of users (with respect to the firewall) the service in question is available.

Protocol Port/MsgType	Service Name	Administration Related?	Available To
UDP 137	NetBIOS NS	No	Private
UDP 138	NetBIOS DGM	No	Private
TCP 139	NetBIOS SSN	No	Private
TCP 445	Microsoft DS	No	Private
TCP 992	Telnets	Yes	Private
TCP 8443	Web-based administrative interface	Yes	Private
TCP 80	Web-based administrative interface	Yes	Private
ICMP/8	Echo Request	No	Private

Since by default all non-administrative traffic sent to the public interface was dropped, and since no traffic was passed inbound through the product, the product initially met the default installation criteria requirements.

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 “Security” -> “General” selected: “Block IP Fragments”.
- Under “Security” -> “Advanced Filtering” -> “LAN Ethernet Rules” added an anti spoofing rule to allow 205.160.98.1 through 205.160.98.254 outbound. Added one additional rule to deny all other traffic.
- Under “Security” -> “Advanced Filtering” -> “Input Rules” -> “Final Rules” added rules to allow outbound RSSP traffic and deny all other traffic.
- Under “Security” -> “Advanced Filtering” -> “Output Rules” -> “Final Rules” added rules to allow inbound RSSP traffic and to deny all other traffic.
- Under “Advanced” -> “Remote Administration” enabled HTTPS and disable HTTP.

The Network Security Lab team performed port scans followed by additional scans and other tests to ensure that the OpenRG 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 OpenRG 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

While the OpenRG product did log events locally, all locally logged data would be lost upon reboot or loss of power. Therefore, in order to meet the criteria, the products were configured to send all log data to a private syslog server.

To configure the OpenRG to use syslog the Network Security Lab Team selected “Advanced” -> “System Settings” -> “Security Logging” and “Advanced” -> “System” -> “Settings” -> “System

Logging". Both "System Logging" and "Security Logging" were set to "Information" and the IP address of a private syslog server was added. Under "Security" -> "Security Log" -> "Settings" all the options listed were enabled.

The following logged events were taken from the syslog server. The first logged event was a permitted outbound HTTP session. The second logged event was a denied outbound UDP connection attempt. The third logged event was a rule configuration change.

```
Jun  2 12:54:16 gw 2005 openrg RGFW-OUT: ACCEPT LAN-OUTBOUND [39] Maximum security enabled service (TCP 205.160.98.66:50166->205.160.90.66:80 on ixp0)
```

```
Jun  2 12:54:53 gw 2005 openrg RGFW-OUT: BLOCK [44] Rule: Advance filter, fw/policy/0/chain/1200/rule/1 (UDP 205.160.98.66:32772->205.160.90.66:113 on ixp0)
```

```
Jun  2 12:47:54 gw 2005 openrg RGFW-CONF: [1] Firewall internal (Firewall configuration succeeded)
```

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 default method of administration was via a web browser from any host on the private network through TCP port 443. The web administrative interface used SSL for encryption of the traffic. The product also supported remote access from hosts on the private network via a telnet client to TCP port 23, but this was not used during testing. The administrative interface used during testing required a simple username and password to identify and authenticate an administrator to the OpenRG. The OpenRG also provided a standard serial console interface for local, non-networked administration.

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 OpenRG had no problem continuing to enforce the security policy when power was restored following a forced power loss. Additionally, the product continued to maintain time, date, and authentication 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 OpenRG 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 OpenRG. 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

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

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 tested was an implementation of an engineering reference. Other products based on the Jungo Software Technologies design may have modifications which conflict with ICSA Labs Firewall Certification requirements.

During default install testing TCP port 113 responded with reset packets when connection attempts were made. All other ports did not respond when connection attempts were made.

Conclusion

The Candidate Firewall Product met all the criteria elements in the Baseline and Corporate and therefore has attained 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 OpenRG, 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 OpenRG to have its ICSA Labs Firewall Certification revoked:

1. Jungo Software Technologies withdraws from the ICSA Labs Firewall Certification Program.
2. The product fails a periodic spot-check and Jungo Software Technologies 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.

Copyright © 2005 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.