

4.1 Firewall Lab Report



D-Link Corporation

NetDefend DFL-2500

Version 2.11.07

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 an appliance based NetDefend DFL-2500. The DFL-2500 was an Intel Pentium 4 based system with a 2.93 GHz processor, 512MB RAM, eight 10/100/1000 ethernet ports and a serial console port.

The DFL-2500 was administered using a web interface. Therefore, no additional hardware was required or submitted for testing.

Software

The DFL-2500 was initially shipped with version 2.10.1. Criteria Violations discovered during testing required patches that brought the DFL-2500 to version 2.11.07, as explained later in the section "Criteria Violations and Resolutions".

In order for D-Link Corporation customers to retrieve the latest version they can access the D-Link Technical Support site at <http://support.dlink.com/>

No separate underlying operating system was installed on the firewall hardware since the DFL-2500 was an all-in-one appliance.

Documentation

To satisfy documentation requirements, D-Link Corporation provided the Network Security Lab team with the following electronic (.pdf) documents in order to assist in the installation, configuration, and administration of DFL-2500:

- *DFL-2500_A2_QIG_v1.02.pdf (DFL-2500 Quick Start Guide)*
- *NetDefendOS_210_CLI_Guide.pdf Published 2006-10-24*
- *NetDefendOS_210_Firewall_UserManual.pdf Published 2006-10-23*

Documentation defining log event dispositions was found in:

- *NetDefendOS_210_Log_Reference_Guide Published 2006-10-24*

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>

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 DFL-2500 was a router-based appliance utilizing a custom packet filtering configuration, Intrusion Prevention system, and Network Address Translation. The product was configured in NAT mode for inbound and outbound services. DNS could not be hosted 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.

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

The DFL-2500 was installed according to the instructions in DFL-2500_A2_QIG_v1.02.pdf (DFL-2500 Quick Start Guide). This involved connecting the DFL-2500 to the private network, configuring the host computer’s IP address to match the suggested range in the DFL-2500 Quick Start Guide, opening a web browser on a host computer on the private network, entering the suggested IP address into the web browser and connecting using the default username and password. Once connected, and only if this is the first time the product is configured, you are given a “Setup Wizard” to follow. During this time, the Firewall Lab team configured the “WAN” link to “Static” and set the “IP Address” field to the appropriate IP Address, changed the “LAN” ip address, created the initial administrative user, set the “Date and Time”, disabled the DFL-2500 “DHCP service” and “Activated” the configuration.

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 DFL-2500 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 from public sources was denied from passing inbound through the DFL-2500 to private hosts. In addition, the product did not respond to ICMP echo requests sent directly to its external interface. The DFL-2500 did permit outbound traffic for the RSSP services by default, but no other TCP, UDP, ICMP or IP protocol traffic was permitted.

The table below contains a description of the services determined to be listening on the DFL-2500 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
TCP 443	Web-based administrative interface	Yes	Private

The DFL-2500 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 “Objects” -> “Services”, created one custom service group that combined all the required RSSP services for inbound traffic which includes FTP, DNS, HTTP, HTTPS, SMTP, IMAP and POP3.
- Under “Rules” -> “IP Rules” and using the default RSSP service group provided for outbound traffic which included FTP, Telnet, DNS, HTTP, HTTPS, IMAP, SMTP and POP3, a rule was created that allowed RSSP service group outbound from the private network.
- Under “Rules” -> “IP Rules and choosing the “NAT” tab for the above rule, the radio button was chosen for “Use Interface Address”
- Under “Rules” -> “IP Rules” and using the previously mentioned custom services group, a rule was created for inbound RSSP traffic from the public network and under the “SAT” tab, the radio button for “Destination Address” was selected and a host IP address was given in the “To” field.
- To satisfy the additional Corporate category requirements to enforce a different security policy, the outbound rules were modified to allow outbound Secure Shell (SSH) connections.

The Network Security Lab team performed port scans followed by additional scans and other tests to ensure that the DFL-2500 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 DFL-2500 in either direction, as expected.

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 DFL-2500 had the ability to store logs on both the product itself and a private syslog host. To meet specific persistence requirements, the DFL-2500 was configured to send the log messages to a private host via syslog. This was accomplished under “System” -> “Log” -> “Event Receivers”.

The following logged events were taken from the syslog server. The first logged event was a successful administrative connection from a host on the private network to the DFL-2500’s private interface, the second logged event was a valid outbound HTTP connection, and the third logged event was an unsuccessful inbound SSH attempt from the public network.

```
May 21 13:42:06 205.160.72.254 [2007-05-21 15:28:17] FW: SESMGR:  
prio=2 id=04900001 rev=1 event=sesmgr_session_created action=none  
user=admin database=AdminUsers ip=205.160.72.66 type=HTTPS
```

```
May 21 13:42:50 205.160.72.254 [2007-05-21 15:29:02] FW: CONN:  
prio=1 id=00600001 rev=1 event=conn_open rule=outbound-rssp  
conn=open connipproto=TCP connrecvif=lan1 connsrcip=205.160.72.66  
connsrcport=36835 conndestif=wan1 conndestip=205.160.70.66  
conndestport=80
```

```
May 21 13:44:18 205.160.72.254 [2007-05-21 15:30:29] FW: RULE:  
prio=3 id=06000051 rev=1 event=ruleset_drop_packet action=drop  
rule=Default_Rule recvif=wan1 srcip=205.160.70.66  
destip=205.160.70.2 ipproto=TCP ipdatalen=40 srcport=39143  
destport=22 tcphdrhlen=40 syn=1
```

The DFL-2500 did not initially meet all the logging requirements, resulting in updated images and updated documentation. Refer to the “Criteria Violations and Resolutions” section for more information.

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 primary means for administration was via a web browser from any host on the private network using HTTPS on port 443 by default. Full administrative access was also available via a serial console port and SSH.

Attempts to bypass the authentication mechanism for all means of administration were unsuccessful and the DFL-2500 initially met all administration requirements.

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 DFL-2500 had no problem continuing to enforce the security policy or maintaining authentication data when power was restored following a forced power loss. Additionally, the product was able to maintain time across reboots and power losses.

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

Since the product did not initially meet all the functional and security testing requirements, refer to the “Criteria Violations and Resolutions” section for more detailed information concerning the issues found during functional and security testing.

After D-Link Corporation addressed the issues reported by the Network Security Lab team the DFL-2500 was re-tested. The product properly permitted the minimum set of common services inbound and outbound per the Corporate module of the criteria. Furthermore, the DFL-2500 was no longer susceptible to attacks launched inbound and outbound to and through the product, including fragmentation and trivial Denial-Of-Service 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 following Documentation criteria violations were found by the Network Security Lab team during testing and corrected by D-Link Corporation.

- The supplied documentation incorrectly listed the type of connection needed when using a web browser.
- The supplied documentation incorrectly stated that the command line interface (CLI) was not able to configure the firewall portion of the DFL-2500 when in fact that it could be used.

The following Functional and Security criteria violations were found by the Network Security Lab team during testing and corrected by D-Link Corporation.

- Once a valid TCP reset packet was captured, it could be replayed numerous times through the product.
- The product allowed spoofed/invalid RST packets.

The following Logging criteria violations were found by the Network Security Lab team during testing and corrected by D-Link Corporation..

- The product did not log every unique DNS request.
- The product incorrectly logged administrative connections as “type=HTTP” when the connection used was actually HTTPS.

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 has a unique feature when using the web based administrative interface. Once a change is made, it must be manually saved and once the save is done, another web page opens that requires the administrator that made the change to acknowledge within a certain timeframe that the changes are to be approved. If the changes are not approved in the timeframe given, the product will revert to the configuration it was using before any changes were made. This can be particularly useful if the administrator is not local to the product at the time a change is made and is inadvertently locked out of the system.

Conclusion

The Candidate Firewall Product met all the criteria elements in the Baseline and the Corporate criteria module 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 DFL-2500, 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 DFL-2500 to have its ICSA Labs Firewall Certification revoked:

1. D-Link Corporation withdraws from the ICSA Labs Firewall Certification Program.
2. The product fails a periodic spot-check and D-Link 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 5, 2007

Test Location

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

Product Headquarters

D-Link Corporation
No. 289, Sinhu 3rd Rd.,
Neihu District, Taipei City 114,
Taiwan, R.O.C.

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.