
TippingPoint, a division of 3Com

TippingPoint X505

Version 2.2.4.6517

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 X505 appliance. The X505 had an Intel Pentium Processor running at 2.4 GHz, 1 GB of main memory, four 10/100 Ethernet adapters, a 1 GB hard drive and a serial console port.

The X505 used a remote web-based administrative interface. Therefore, no additional hardware was required or submitted for testing.

Software

The X505 arrived with version 2.2.1_6506 which is integrated with a base OS of vxWorks 5.2.4. During testing, TippingPoint submitted new firmware images to resolve criteria violations discovered by the Network Security Lab team. Testing successfully completed with version 2.2.4.6517.

The X505 did not require a license key to be installed into the product.

The latest version of the firmware can be obtained by current TippingPoint customers that have a valid support contract by contacting TippingPoint's technical support at tacmail@tippingpoint.com and requesting build 2.2.4.6517.

Documentation

To satisfy documentation requirements, TippingPoint provided the Network Security Lab team with the following electronic (.pdf) documents in order to assist in the installation, configuration, and administration of X505:

- *X-Series Deployment Guide, Part Number: TECHD-0000000075, Version 2.2*
- *Quick Start TippingPoint X505, Part Number:TECHD-0000000077, Version 2.2*
- *X-Series Local Security Manager (LSM) Users Guide, Part Number: TECHD-0000000067, Version 2.2*
- *X-Series Concept Guide, Part Number: TECHD-0000000074, Version 2.2*
- *ICSA Firewall Configuration Notes for X505 Firewall, Release 2.2.4.6517, Part Number: TECHD-00000000133*

Documentation defining log event dispositions was found in:

- *Local Security Manager (LSM) Users Guide, pp 15, 201 - 238*

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

Candidate Firewall Product Configuration The X505 was a router-based appliance utilizing a custom packet filtering configuration, Intrusion Prevention system, and Network Address Translation. While the X505 does support an IP only bridging mode called Transparent Mode, 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 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 X505 was installed according to the instructions in *Quick Start TippingPoint X505*. This involved connecting a laptop to the serial console. Following the steps in the “Setup Wizard”, username and password levels were assigned, and then both the actual username and password were configured. “LAN” and “WAN” interfaces were assigned to separate “Security Zones” followed by the default firewall rule set being accepted. The X505 was then automatically rebooted by the “Setup Wizard”.

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 X505 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 X505 to private hosts. In addition, the product did not respond to ICMP echo requests sent directly to its external interface. The X505 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 X505 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 22	SSH	Yes	Private
TCP 443	HTTPS	Yes	Private

The X505 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 "Network" -> Interfaces" -> "Internal", clicked the "Enable NAT" checkbox.
- Under "Network" -> IP Address Group", created a setting for the "RSSP host" on the private network.
- Under "Network" -> IP Address Group", created a setting for the private network.
- Under "Firewall" -> "Service Groups", created both inbound and outbound groups for the required RSSP services.
- Under "Firewall" -> "Firewall Rules", created rules using the previously created "Service Groups" and "IP Address Groups" for outbound connections using the "Source Zone" as LAN(private) and "Destination Zone" as "WAN".
- Under "Firewall" -> "Firewall Rules" created rules using the previously created "Service Groups" and "IP address Groups" for inbound connections using the "Source Zone" as "WAN" and "Destination Zone" as "LAN(RSSP host)".
- 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 X505 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 X505 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 X505 had the ability to store logs on both the product itself or a private syslog host. To meet specific persistence requirements, the X505 was configured to send the log messages to a private host via syslog. Following the procedures outlined in the *ICSA Firewall Configuration Notes for X505 Firewall, Release 2.2.4.6517*, the Network Security Lab team enabled remote syslog using the command line interface to configure an IP address for the private syslog host and also to configure the default "System", "Audit", "Block" and "Traffic" logs to be sent to the private syslog host.

The following logged events were taken from the syslog server. The first logged event was a successful HTTP inbound connection, the second logged event was a failed outbound NTP connection, and the third logged event was an unsuccessful administrative login attempt from the private network to the private interface.

```
Jun          20          02:21:29          gw          205.160.78.254
2006,src=205.160.70.66,TCP:34471,WAN,dst=205.160.70.8,TCP:80,LAN,
start="Jun 20 02:21:29 2006",msg="Regular Session Start"
```

```
Jun          21          10:16:42          gw          205.160.78.254
2006,src=205.160.78.66,TCP:55931,LAN,dst=205.160.70.66,UDP:123,WA
N,rule="Rule 41",cat="Security",msg="Blocked by the policy rule
41"
```

```
JUN 20 02:46:31 gw 2006 fw.tp.prop [audit] user=[administrator]
src=205.160.78.253 iface=1 access=0 Invalid password for
administrator
```

The X505 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 X505 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 X505 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 TippingPoint addressed the issues reported by the Network Security Lab team, the X505 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 X505 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

All criteria violations were addressed by TippingPoint in firmware version 2.2.4.6517.

The following Functional and Security criteria violations were found by the Network Security Lab team during testing.

- The product allowed FTP port commands with an IP address different from the FTP client's address. This would allow FTP bounce attacks to occur if the attempted data connection did not flow through the product. However, FTP bounce attacks with data connections flowing through the product were not allowed.
- Once a valid ICMP port unreachable or ICMP Time Exceed packet was captured, it could be replayed numerous times through the product.
- The product allowed TCP packets inbound and outbound without a properly established TCP session for RSSP services.
- The product was susceptible to certain trivial Denial-of-Service attacks.
- The product allowed fragmented packets outbound without proper reassembly of the packets.
- Remote syslog did not function correctly.

The following Logging criteria violations were found by the Network Security Lab team during testing.

- The product did not log the IP Protocol in all logged events.
- The product did not log all ICMP type packets going to or through the product from both the public and private networks.
- The product did not log any raw IP Protocol packets sent to or through the product when no data was present.
- The product did not log spoofed TCP RST packets coming from the public network.
- The product did not have a year stamp in remote syslog messages.
- The product did not log an event when an administrative user made a manual time change to the system clock.
- The product did not log a system startup message to remote syslog.
- The product did not log any access requests to the administrative interface from the private network to remote syslog.
- The product did not log firewall rule or policy changes to remote syslog.
- The product did not log the username, the source IP address and a statement of denied or successful authentication to the HTTPS or SSH administrative interfaces.

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 X505 did have the ability to limit inbound or outbound access using various methods including, but not limited to, authentication and time of day on a per rule basis.

Failed administrative logins produced two separate log messages. The first message showed the login as failed while the second message gave the reason for the failure.

When using the web browser based administrative interface, Internet Explorer version 6 or higher must be used along with 128-bit encryption and support for Java Script and cookies.

Conclusion

The Candidate Firewall Product met all the criteria elements in the Baseline and Corporate 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 X505, 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 X505 to have its ICSA Labs Firewall Certification revoked:

1. TippingPoint withdraws from the ICSA Labs Firewall Certification Program.
2. The product fails a periodic spot-check and TippingPoint 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 20, 2006

Test Location

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

Product Headquarters

TippingPoint, a division of 3Com
7501 North Capital of Texas Highway
Building B
Austin, Texas 78731 USA

Copyright

Copyright © 2006 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.