ICSA Labs
Network Firewall Certification Testing Report
Enterprise (High Availability) - Version 4.1x

SonicWALL, Inc.

E-Class Network Security Appliance (NSA) Series

February 28, 2011

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

FWXX– SONICWALLI-2011-0228-02

SonicWALL Network Firewall Certification Testing Report
Enterprise (High Availability) - Version 4.1x

Table of Contents

Executive Summary

This lab report is a companion report to the Enterprise certification lab report, which can be found at:

https://www.icsalabs.com/sites/default/files/SW_Enterprise.pdf

The goal of the Enterprise High Availability (HA) lab report is to document the steps taken to ensure the Candidate Firewall Product met all of the HA certification criteria requirements. All HA specific configuration steps and any issues found are documented within this lab report.

All other areas usually covered within an ICSA Labs Firewall Certification Lab Report can be found in the Enterprise Lab Report referenced above.

Candidate Firewall Product Configuration Tested

Introduction

Any changes made to the Candidate Firewall Product (CFP) to meet the HA requirements will be documented within this section. Additionally, if HA does not work in any specific configuration mode supported by the CFP this will be noted.

Candidate Firewall Product Configuration

The SonicWALL, Inc. (SonicWALL) E-Class Network Security Appliance (NSA) Series was previously configured to use NAT for inbound and outbound services. This configuration was maintained for HA testing except for the addition of a NAT policy and associated firewall rules to provide access to the servers used in testing HA capabilities.

The Network Security Lab team performed the following procedures during the configuration of HA:

- Under the Web interface, the “Wizards” button was used to access the “Public Server Wizard”.
- The server type “Web Server” and “HTTP (TCP 80)” service was selected.
- The private side IP address of the web cluster used for HA testing was entered.
- A “Server Public IP Address” was entered to allow access to HA servers while not affecting access to the previously configured Required Services Security Policy (RSSP).
- Under “High Availability” -> “Settings” the Serial Number of the backup product was entered and “Enable High Availability” was checked.
- The “Send Syslog messages from both HA units with unique serial numbers” setting on the “Diag” page was checked.
- Under “Firewall” -> ”Advanced”, “Disable Application Firewall, Anti-Spyware, Gateway AV and IPS Engine (increases maximum SPI connections)” was checked.

Logging

Introduction

Version 4.1x of *The Modular Firewall Certification Criteria* requires that the Candidate Firewall Product provide an extensive logging capability.

The Network Security Lab team has detailed in the Enterprise Lab Report, referenced above, that the logging functionality provided by the Candidate Firewall Product meets all of the certification criteria requirements. This section details how the CFP logs HA state changes..

Results

While the E-Class NSA Series did log events locally, which could be viewed via the web-based administrative interface, all locally logged data would be lost upon reboot or loss of power. Therefore, in order to meet the persistence criteria, all log data was delivered to a remote syslog server.

The following logged events were taken from the syslog server on the private network. The first logged event shows when the “Passive” unit enters the “Other” state:

Mar 29 15:34:58 gw id=firewall sn=0017C51C6454 time="2010-03-29 15:34:57" fw=205.160.50.1 pri=6 c=1 m=1129 msg="Peer firewall has reduced link status. In event of failover, it will operate with limited capability." n=0

This logged event shows when the “Passive” unit became “Active”:

Jun 30 15:03:57 gw id=firewall sn=0017C514B928 time="2010-06-30 15:08:38" fw=205.160.50.1 pri=1 c=1 m=145 msg="Backup firewall has transitioned to Active" n=0

The product initially did not meet one or more logging requirements. Refer to the “Criteria Violations and Resolutions” section for more information.

Administration

Introduction

The administration requirements are generally covered and documented in the aforementioned Enterprise Lab Report. This section will document how the Candidate Firewall Product addresses HA specific administration requirements.

Results

The E-Class NSA Series utilizes the web interface to determine and control which product is currently active. In order to manually switch which device was currently active in an HA cluster, the user is required to reboot the active product though the Web interface or otherwise cause a failover event (i.e. unplug a cable) to force failover to the backup device.

Functional and Security Testing

Introduction

Once configured to operate in one of the permitted in High Availability (HA) modes 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 SonicWALL addressed the issues reported by the Network Security Lab team the E-Class NSA Series was re-tested. The product properly handled HA functionality and state changes as specified in the HA criteria. During re-testing of the E-Class NSA Series, it was not susceptible to attacks launched inbound or outbound to or through the product, including fragmentation and trivial Denial-Of-Service attacks.

Reaction Time and Number of Simultaneous Connections

Introduction

Prior to the commencement of testing vendors are required to provide ICSA Labs with the number of simultaneous connections the Candidate Firewall Product (CFP) should be able to sustain when being tested against the High Availability (HA) criteria. ICSA Labs expects the CFP to be able to sustain a minimum of 66.6% of that number.

The CFPs ability in this area is reported below. Additionally the CFP's ability to react to failover events within the prescribed time is documented.

Results

The NSA E7500 specifications listed its ability to handle 1,000,000 simultaneous connections. The required number of simultaneous connections was 666,936. The NSA E5500 specifications listed its ability to handle 750,000 simultaneous connections; therefore the tested number of simultaneous connections was 499,968.

The NSA E7500 reacted to a failure of an active network interface in an average of 35 milliseconds (ms), When the "Active" device experienced a power failure the reaction time to failover was an average of 4.5 seconds (4500 ms). The NSA E5500 responded to a failure of an active network interface in an average of 35 ms with an average reaction time of 7 seconds (7000 ms) for a power failure of the "Active" device.

Criteria Violations and Resolutions

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 criteria violations were found by the Network Security Lab team during testing and corrected by SonicWALL:

- The E-Class NSA Series did not fail over established TCP sessions until data was transmitted.
- The E-Class NSA Series did not properly log a failure of either the public or private interface of the unit currently in “Passive” mode.

Testing Information

This report is issued by the authority of the Managing Director, ICSA Labs.

Testing was conducted under normal operation conditions.

Lab Report Date

February 28, 2011

Please visit www.icsalabs.com for the most current information about this and other products.

Test Location

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

Product Developer's Headquarters

SonicWALL, Inc.
2001 Logic Drive,
San Jose, CA 95124
USA

The certification test methods used to produce this report are accredited and meet the requirements of ISO/IEC 17025 as verified by the ANSI-ASQ National Accreditation Board/ACLASS. Refer to certificate and scope of accreditation number AT – 1423.