ICSA Labs
Network Firewall Certification Testing Report
Enterprise (IPv6) - 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-2011-0228-03

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 IPv6 lab report is to document the steps taken to ensure the Candidate Firewall Product met all of the IPv6 certification criteria requirements. All IPv6 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 IPv6 requirements will be documented within this section. It is worth noting that the IPv6 services such as EDSN0, FTP and others were tested and reported in the Enterprise Lab Report referenced above. This section will outline any additional steps taken to configure the Candidate Firewall Product for IPv6.

Finally, the Candidate Firewall Product was configured in a dual stack (IPv4/IPv6) mode.

Candidate Firewall Product Configuration

The Network Security Lab team performed the following procedures during the configuration of IPv6:

- Configure Network Interfaces for IPv6 under “Network” -> ”Interfaces”, and select “View IP Version – IPv6”.
- Configure service groups for RSSP-IN and RSSP-OUT from “Firewall” -> ”Services” -> ”Add Group”.
- Configure Access Rules from “Firewall” -> ”Access Rules”.

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 IPv6 specific events.

Results

The following logged events were taken from the syslog server on the private network. The first logged event was a valid HTTP connection. The second and third logged event was an invalid TCP connection attempt. The fourth logged event was a failed administrative login attempt.

Nov 18 15:19:41 172.26.34.102 id=firewall sn=0017C51C6454 time="2010-11-18 15:17:49" fw=205.160.100.2 pri=6 c=262144 m=98 msg="Connection Opened" n=0 src=2cce:205:160:102::100:49424:X0 dst=2cce:205:160:100::100:80:X1 proto=tcp/http

Nov 18 15:21:45 172.26.34.102 id=firewall sn=0017C51C6454 time="2010-11-18 15:19:52" fw=205.160.100.2 pri=6 c=262144 m=98 msg="Connection Opened" n=0 src=2cce:205:160:102::100:37500:X0 dst=2cce:205:160:100::100:67:X1 proto=tcp/67

Nov 18 15:21:45 172.26.34.102 id=firewall sn=0017C51C6454 time="2010-11-18 15:19:52" fw=205.160.100.2 pri=5 c=64 m=36 msg="TCP connection dropped" n=0 src=2cce:205:160:102::100:37500:X0 dst=2cce:205:160:100::100:67:X1 proto=tcp/67

Nov 18 15:23:13 172.26.34.102 id=firewall sn=0017C51C6454 time="2010-11-18 15:21:21" fw=205.160.100.2 pri=1 c=32 m=30 msg="Administrator login denied due to bad credentials" n=0 usr="admin" src=172.26.33.126:0:X2 dst=172.26.34.102:443:X2 proto=tcp/https

The E-Class NSA Series did not initially meet all logging requirements. Please 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 handles the blocking of Remote Administrative access via IPv6

Results

The E-Class NSA Series can block remote administrative access via IPv6 by deselecting "HTTP" and "HTTPS" from "Network"->"Interfaces"->"Edit Interface".

The E-Class NSA Series did not initially meet all administrative requirements. Please refer to the "Criteria Violations and Resolutions" section for more information.

Security Testing

Introduction

Once configured to handle IPv6 traffic the Candidate Firewall Product should handle fragmented datagrams correctly, be able to block packets with Routing Header type 0 and be able to selectively block packets as outlined in the certification criteria.

Results

The E-Class NSA Series 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 SonicWALL E-Class NSA Series was re-tested. The product properly handled IPv6 traffic as per the IPv6 criteria.

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 Functional and Security criteria violation was found by the Network Security Lab team during testing and corrected by SonicWALL:

- The E-Class NSA Series would crash when certain UDP packets were sent to or through the device.

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

- The E-Class NSA Series did not properly log allowed traffic.
- The E-Class NSA Series did not properly log disallowed traffic.
- The E-Class NSA Series did not properly log all ICMPv6 packets.
- The E-Class NSA Series did not properly log RAW IPv6 packets.

The following Administration violation was found by the Network Security Lab team during testing and corrected by SonicWALL:

- The E-Class NSA Series did not allow disabling network access for web administration via IPv6.

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.