ICSA Labs
Network Firewall Certification Testing Report
Enterprise (VoIP) - 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-2011-0228-04

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 Voice over IP (VoIP) lab report is to document the steps taken to ensure the Candidate Firewall Product met all of the VoIP certification criteria requirements. All VoIP 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 VoIP requirements will be documented within this section. Additionally, if VoIP 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 NSA Series was previously configured to use NAT for inbound and outbound services. This configuration was maintained for VoIP testing except for the following procedures:

- Under “SIP” -> “Settings” enabled the checkbox for “Enable Consistent NAT”.
- Under “SIP” -> “Settings” enabled the checkbox for “Enable SIP Transformations”.
- Under “SIP” -> “Settings” -> “Enable SIP Transformations”, changed both settings for “SIP Signaling Activity inactivity time out” and “SIP Media inactivity time out”.

VoIP Required Services Security Policy

Introduction

The VoIP Required Services Security Policy (RSSP) articulates the services expected to allow VoIP to be handled by the Candidate Firewall Product in a secure and functional manner.

Results

The Network Security Lab team performed the following actions, utilizing the WebUI, during configuration of the VoIP RSSP:

- Under “Network” -> “Address Objects”, added a custom object pointing to the SIP server on the private network.
- Under “Firewall” -> “Services”, added a custom service group that included a custom “SIP” service that allowed only UDP/5060.
- Under “Firewall” -> “Access Rules”, created a rule set that allowed inbound access for the RSSP inbound custom service group that pointed to the server residing on the private network.
- Under “Firewall” -> “Access Rules”, created a rule set that allowed inbound access for the SIP custom service group that pointed to the PBX residing on the private network.

The Network Security Lab team performed port scans followed by additional scans and other tests to ensure that the E-Class NSA Series was indeed configured according to the VOIP RSSP and that 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 inbound and outbound SIP, RTP and TFTP service requests. Finally the Network Security

Lab team confirmed that no other traffic was permitted to traverse the SonicWALL E-Class NSA Series in either direction, as expected.

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 VoIP traffic.

Results

The SonicWALL E-Class NSA Series does have the ability to log locally, however, due to persistence requirements, logs were sent to a local syslog server.

The following logged events were taken from the syslog server. The first logged event was a valid SIP response to a SIP registration event. The second logged event was a valid VoIP call that had successfully connected and the third logged event was a failed administrative login.

> Apr 26 08:45:58 205.160.57.254 id=firewall sn=0017C514B928 time="2010-04-26 08:52:20" fw=205.160.50.7 pri=7 c=1048576 m=643 msg="SIP Request" n=0 src=205.160.57.20:5060:X0 dst=205.160.50.20:5060:X1 note="SIP REGISTER (asterisk1@205.160.50.20)"
>
> Apr 26 08:51:01 205.160.57.254 id=firewall sn=0017C514B928 time="2010-04-26 08:57:24" fw=205.160.50.7 pri=6 c=1048576 m=622 msg="VoIP Call Connected" n=0 src=205.160.50.20:5060:X1 dst=205.160.57.20:5060:X0 note="SIP (1001@205.160.50.7:29720 to 2001@205.160.50.20)"
>
> Apr 26 08:47:19 205.160.57.254 id=firewall sn=0017C514B928 time="2010-04-26 08:53:42" fw=205.160.50.7 pri=1 c=32 m=30 msg="Administrator login denied due to bad credentials" n=0 usr="admin" src=205.160.57.66:0:X0 dst=205.160.57.254:443:X0 proto=tcp/https

Administration

Introduction

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

Results

In order to view the dynamically opened RTP ports, open the WebUI and go to the following location, “VoIP” -> “Call Status”.

Functional and Security Testing

Introduction

Once configured to enforce the VoIP 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.

SonicWALL addressed the issues reported by the Network Security Lab team and the E-Class NSA Series was re-tested. The product properly permitted the minimum set of common services inbound and outbound per the VoIP criteria. Furthermore, during re-testing of the E-Class NSA Series, it was not susceptible to attacks launched inbound and outbound to and through the product, including fragmentation and trivial Denial-Of-Service attacks.

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

- An invalid packet was allowed that prematurely terminated a call.

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.