ICSA Labs
Network Firewall Certification Testing Report
Enterprise - 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-2011-0228-01

Table of Contents

Executive Summary

Introduction

The goal of ICSA Labs is to significantly increase end user, small and medium businesses, corporations, and large enterprises trust in information security products and solutions. For more than 18 years, ICSA Labs, an independent division of Verizon Business, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Businesses worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs manages and facilitates technology consortia that focus on emerging, well-defined technologies. The consortia provide for information exchanges among industry leading developers, and for the development of product testing and certification programs and standards. For more information about ICSA Labs, please visit www.icsalabs.com.

Product Overview

The SonicWALL® E-Class Network Security Appliance (NSA) Series uses patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology in combination with multi-core specialized security microprocessors to deliver high speed gateway anti-virus, anti-spyware, intrusion prevention and Application Intelligence. With a broad range of scalable solutions for enterprise deployments in distributed environments, campus networks and data centers, the E-Class NSA Series offers high performance protection.

Scope of Assessment

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 4.1x of *The Modular Firewall Certification Criteria.* The criteria requirements are documented in Baseline and Enterprise modules. Both of of which can be found on the ICSA Labs website.

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.

Summary of Findings

The Candidate Firewall Product met all the criteria elements in the Baseline and Enterprise modules 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.

In addition to this lab report testing for the IPv6, Voice over IP (VoIP) and High Availability (HA) requirements can be found in their associated lab reports. These reports can be found at:

https://www.icsalabs.com/sites/default/files/SW_Enterprise_HA.pdf
https://www.icsalabs.com/sites/default/files/SW_Enterprise_VoIP.pdf
https://www.icsalabs.com/sites/default/files/SW_Enterprise_IPv6.pdf

Certification Maintenance

The E-Class Network Security Appliance (NSA) Series, 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 E-Class NSA Series to have its ICSA Labs Firewall Certification revoked:

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

Candidate Firewall Product Components

Introduction

The set of hardware, software, and documentation components delivered to ICSA Labs for testing are collectively called the "Candidate Firewall Product" or "CFP." Updated CFP components may have been submitted prior to spot-check testing. In the event of a product failing spot-check tests, updated hardware, software, or documentation will be required in order to successfully maintain its ICSA Labs Firewall Certification. This section of the report describes any updates made to the CFP components submitted prior to or during the course of spot-check testing.

Hardware

SonicWALL, Inc. (SonicWALL) provided an NSA E7500 (E7500) which had a 16 core 600Mhz Octeon CPU from Cavium Networks with 2GB RAM and 512MB Flash. The E7500 had four 10/100/1000Base-T ports, four mini-GBIC ports, one RJ-45 Serial port, 2 USB ports, and a dedicated HA link port. Additionally, SonicWALL provided an NSA E5500 (E5500) which had an 8 core 550Mhz Octeon CPU from Cavium Networks with 1GB RAM and 512MB Flash. The E5500 had four 10/100/1000Base-T ports, four mini-GBIC ports, one RJ-45 Serial port, 2 USB ports, and a dedicated HA link port.

Software

Prior to testing, the E7500 and E5500 were upgraded to SonicOS Enhanced version 5.5.0.0-36o--IPv6-d_15o. During the course of testing, SonicWALL submitted updated firmware to resolve criteria violations discovered by the Network Security Lab team. Testing successfully completed with SonicOS Enhanced version 5.5.1.0-5o--IPv6-15o.

Firewall Product Family Description

This section lists the members of the Candidate Firewall Product Family. A representative set of models was submitted for testing and listed in the Hardware section above. In order to submit a family of products for certification, the vendor must attest that:

- The vendor designs and maintains control over the entire set of hardware, firmware, and software for each member of the product family;
- The vendor software, including but not limited to the functional software and the operating system software, is uniform across the product family;
- The management interface(s) for the members of the product family are uniform and completely consistent;
- Each member in the product family has an equivalent set of functionality; and
- The functional, integration, and regression testing conducted by the vendor is uniform and consistent across the product family.

Family Members

- NSA E5500
- NSA E6500
- NSA E7500
- NSA E8500

Documentation

To satisfy documentation requirements, SonicWALL provided the Network Security Lab team with the following electronic (.pdf) documents in order to assist in the installation, configuration, and administration of E-Class NSA Series:

- *SonicOS Enhanced 5.5 Administrator's Guide, Oct 2009*
- *SonicOS Enhanced 5.5.1.0 Release Notes, Rev C, Jan 17, 2011*
- *SonicOS 5.5 IPv6 Feature Module, Jan 18, 2011*
- *NSA E7500 Getting Started Guide, August 5, 2010*

Documentation defining log event dispositions was found in:

- *SonicOS Enhanced 5.5 Administrator's Guide, Oct 2009, Part 16, Chapter 69*

Documentation describing how fixes and upgrades are handled was found in:

- *SonicOS Enhanced 5.5 Administrator's Guide, Oct 2009, Chapter 11*

Candidate Firewall Product Configuration Tested

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 E-Class NSA Series appliances were router based operating as a stateful packet-filtering firewall. The E-Class NSA Series supports both straight-through and NAT modes. NAT mode was configured for use for all inbound and outbound services. DNS could not be hosted on the E-Class NSA Series and therefore, like all other services, a DNS server was made available and properly configured for address and name resolution on the private LAN.

Default Install Posture

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 E7500 was installed according to the instructions in the *NSA E7500 Getting Started Guide*. This involved configuring a PC with an IP address in the E7500's default private network range in order to access the Setup Wizard via a web browser. Following the steps in the Setup Wizard, a password was set, the time zone was selected, and the public (WAN) and private (LAN) network settings were entered. Afterwards, the E7500 was restarted and the PC was reconfigured to use the new private network settings.

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 E7500 public interface neither accepted, nor passed inbound through the product, any non-administration-related TCP, UDP, ICMP, or other IP protocol traffic.

By default no traffic was allowed through the product.

The table below contains a description of the services determined to be listening on the E7500 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 80	Web-based administrative interface	Yes	Private
TCP 443	Web-based administrative interface	Yes	Private
TCP 2601	Debugging interface	Yes	Private
TCP 2602	Debugging interface	Yes	Private
TCP 2604	Debugging interface	Yes	Private
ICMP 8	PING	No	Private

The product initially failed to meet the Default Install criteria. Refer to the "Criteria Violations and Resolutions" section for more information.

Required Services Security Policy Transition

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. It is worth noting that some of these services are IPv4 specific. Services specific to VoIP requirements will be enumerated within the VoIP lab report. Additionally, products tested 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:

- Services groups were added under "Firewall" -> "Services" -> "Add Group". Two groups were created, one for the inbound services which was named "RSSP-In" and one named "RSSP-Out" for the outbound services with each group using the appropriate RSSP services.

- Under “Network” -> “Address Objects”, objects were created for the host on the private network as well as an address object for the private network IP address range.

- Using the “Wizards” option, a “public server” was created using the “RSSP-In” services group previously created.

- Under “Network” -> “Interfaces”, chose “X0” and unchecked everything except ‘HTTPS”.

- Under “Network” -> “Interfaces”, chose “X1” and unchecked everything.

- Under “Network” -> NAT Policies”, verified the inbound NAT policies were correctly set for the RSSP-Inbound services directed to the “Address Object” created earlier.

- Under “Firewall” -> “Access Rules”, a rule was created using the “Add” button and setting the “Action” to “Allow”, the “Source” to the “Address Object” previously created for the private network, the “Destination” to “Any” and the “Service” set to “RSSP-Out”.

- Under “Firewall” -> “Access Rules”, clicked the “Configure” button for each rule displayed and unchecked “Allow IP Fragments”.

- Under “Firewall” -> “Advanced”, enabled the following checkboxes, “Enable Stealth Mode”, Randomize IP ID”, “Drop Source Routed Packets”, “Disable Application Firewall”, “Anti-Spyware”, “Gateway AV”, “IPS Engine”, “Enable IP Header Checksum Enforcement”, and finally “Enable UDP Checksum Enforcement”. Everything else was unchecked.

- Under “Firewall” -> “TCP Settings”, enabled all of the following checkboxes, “Enforce Strict TCP Compliance with RFC 793 and RFC 1122”, “Enable TCP Handshake Enforcement”, and “Enable TCP Checksum Enforcement”. “SYN Flood Protection Mode” was then set to “Always Proxy WAN Connections”.

- Under the following headings, made sure everything is turned off: “PC Card”, “SonicPoint”, “VoIP”, “Application Firewall”, “VPN”, “High Availability” and “Security Services”.

- Corporate category products are required to allow configurations beyond the normal RSSP. This was performed under “Firewall” -> “Access Rules”, where a rule was created using the “Add” button and setting the “Action” to “Allow”, the “Source” to the “Address Object” previously created for the private network, the “Destination” to “Any” and the “Service” set to “SSH”.

The Network Security Lab team performed port scans followed by additional scans and other tests to ensure that the E7500 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. In addition to RSSP, the same ports listed above remained open.

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, EDNS0, IMAP, POP3, and SSH 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, EDNSO, IMAP, POP3 and SSH 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 E7500 in either direction, as expected.

The product did not initially meet one or more requirements. Refer to the "Criteria Violations and Resolutions" section for detailed information concerning the problems found during RSSP testing.

Logging

Introduction

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

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

While the E7500 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 private syslog server.

This was accomplished by defining a remote syslog server under "Log" > "Syslog", setting the "Syslog Event Redundancy Filter" to 0 seconds to ensure that all log event were successfully captured, checking "syslog" for all categories under "Log" > "Categories", and ensuring that "Enable Logging" was selected for all rules under "Firewall" > "Access Rules".

The following logged events were taken from the syslog server on the private network. The first logged event was an allowed RSSP connection:

> Jun 29 10:13:16 gw id=firewall sn=0017C514B934 time="2010-06-29 13:23:46" fw=205.160.50.1 pri=6 c=262144 m=98 msg="Connection Opened" n=0 src=103.198.105.115:19092:X1 dst=205.160.51.66:110:X0 proto=tcp/pop3

The second logged event was a denied raw IP protocol packet:

> Oct 23 11:08:21 205.160.51.254 id=firewall sn=0017C51C6454 time="2009-10-23 11:03:03" fw=205.160.50.1 pri=1 c=512 m=522 msg="Malformed or unhandled IP packet dropped" n=0 src=205.160.50.66:88:X1 dst=205.160.51.254:88:X0 proto=103

The final logged event was an allowed administrative login:

> Jun 30 10:42:26 gw id=firewall sn=0017C514B934 time="2010-06-30 13:52:55" fw=205.160.50.1 pri=6 c=16 m=29 msg="Administrator login allowed" n=0 usr="admin" src=172.26.35.125:0:X2 dst=172.26.34.51:443:X2 proto=tcp/https

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

Administration

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 method of administration was via a web browser from any host on the private network via HTTP over TCP port 80 or HTTPS over TCP port 443. The product was also configured to allow SSL 128-bit encrypted remote administration from hosts on the public network via HTTPS on port 443. Limited administrative access was also available via a serial console port.

Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

Persistence

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, 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 E-Class NSA Series had no problems continuing to enforce the security policy or maintaining authentication data when power was restored following a forced power loss.

Time and Date Acquisition

Introduction

The Candidate Firewall Product must meet either the NTP or SNTP criteria requirements. These requirements have been structured to ensure that the Candidate Firewall Product will always be able to acquire the correct time and date from a reliable source in a secure manner.

Results

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

After SonicWALL addressed the issues reported by the Network Security Lab team, the E7500 was re-tested. The product met the SNTP testing requirements per the Enterprise module criteria.

Functional and Security Testing

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 SonicWALL addressed the issues reported by the Network Security Lab team, the E-Class NSA Series was re-tested. The product properly permitted the minimum set of common services inbound and outbound per the Enterprise module criteria. It was not susceptible to attacks launched inbound or outbound to or 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 Logging criteria violations were found by the Network Security Lab team during testing and corrected by SonicWALL:

- The CFP did not log TCP packets with a source port of 0 sent to or through either interfaces.
- The CFP did not log the destination port of a TCP or UDP packet sent to or through either interface when the destination port was set to 0.
- The CFP did not log certain raw IPv4 packets with a data payload sent to or through its interfaces.
- The CFP incorrectly logged certain denied IPv4 packets as allowed.

The following Time and Date Acquisition criteria violations were found by the Network Security Lab team during testing and corrected by SonicWALL.

- The CFP did not log any changes made to the system clock where the response from the SNTP server caused the system clock to be updated.
- The CFP did not log any failed attempts to reach the SNTP server.

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

- The CFP responded to certain TCP ports on the private interface from the private network with a debugging command line with no authentication mechanism.
- The CFP responded to ping requests on the private interface from the private network with pings disabled via the web interface.
- The CFP responded to HTTPS requests on the private interface from the private network when HTTP and HTTPS redirect were disabled via the web interface.

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.