1.0 High Availability (HA) Firewall Module Lab Report

An Independent Division of Verizon Business

Elitecore Technologies Ltd.

Cyberoam CR50i
Version 9.5.6 build 25

Introduction

The ICSA Labs High Availability (HA) Firewall Certification Criteria module is a component of *The Modular Firewall Certification Criteria*. It is intended to supplement the certification of a firewall product that has been initially tested and certified against the Baseline and one of the Required Services Security Policy (RSSP) modules.

This criteria against which vendor-submitted products are tested is an industry-accepted standard to which a consortium of network firewall vendors, end users, and the ICSA Labs Network Security Lab team contributed. For more details of what was tested please refer to version 1.0 of *The High Availability 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 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 testing against the HA Firewall Certification Criteria culminates in the writing of a report that documents the results of testing and directly references the report for the initial Baseline and RSSP certification testing. The Firewall certification report also documents the product components submitted by the vendor, the configuration of the product as tested and any patches or updates generated during testing.

Candidate Firewall Product Components

Section 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 HA testing. In the event of a product failing the HA tests, updated hardware, software, or documentation will be required in order to successfully meet the ICSA Labs HA Firewall Certification Criteria requirements. This section of the report describes any updates made to the CFP components submitted prior to or during the course of HA testing.

Hardware

Other than providing a second unit to support HA testing, the Elitecore Cyberoam CR50i hardware components tested remained the same as previously tested.

Software

HA testing of the Cyberoam CR50i started with version 9.5.3 build 20. During the course of HA testing, Elitecore submitted updated firmware to resolve criteria violations discovered by the Network Security Lab team. Testing successfully completed with version 9.5.6 build 25.

Documentation

To satisfy documentation requirements, Elitecore provided the Network Security Lab team with the following electronic (.pdf) documents in order to assist in the HA configuration and administration of the CR50i:

- *High Availability Configuration Guide, Version 9, Document version 95621-1.0-22/09/2008*
- *User Guide, Version 9, Document version 95621-1.1-22/09/2008*
- *Console Guide, Version 9, Document version 95621-1.0-22/09/2008*

HA Certification Criteria

The Candidate Firewall Product was tested against version 1.0 of *The High Availability Firewall Certification Criteria:*

- *http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/optional/ha.pdf*

Background

Section Introduction

Products subjected to HA testing have been previously tested and have an existing ICSA Labs Firewall Certification. This section of the report provides information about previous testing of the CFP.

Previous Testing

The Cyberoam CR50i was successfully tested against the following modules from version 4.1a of *The Modular Firewall Certification Criteria* before undergoing HA testing*:*

- *Baseline module,*
  http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/baseline.pdf
- *Logging Update – version 4.1a,*
  http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/4.1a_logging.pdf
- *Required Services Security Policy – Corporate Category module,*
  http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/4.1/corporate.pdf

Initial testing of the Cyberoam CR50i was documented in a 4.1 Firewall Lab report which can be found at:

- *http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/elitecore_family.pdf*

Additionally, spot-check testing of the Cyberoam CR25i, also a member of the Cyberoam Unified Threat Management Appliance Family, provided an update to the family's certification. The 4.1a Firewall Spot-Check Lab Report documenting this testing can be found at:

- *http://www.icsalabs.com/icsa/docs/html/communities/firewalls/pdf/cyberoam_spotcheck.pdf*

Candidate Firewall Product Configuration Tested

Section Introduction

When testing is performed against the HA module, it is the goal of the ICSA Labs Network Security Lab to test the Candidate Firewall Product(s) in the configuration used to pass prior certification testing. Occasionally, however, it may be necessary to configure the product differently to support the features being tested in the HA module.

In these circumstances any changes made will be documented in this section. Additionally, some of the tests conducted during prior certification testing will be run again to ensure these configuration changes do not introduce any new criteria violations.

Candidate Firewall Product Configuration Changes

The Cyberoam CR50i was previously configured to use NAT for inbound and outbound services. This configuration was maintained for HA testing except for the additional use of a “Virtual Host” to provide access to the servers used in testing HA.

The following steps were performed to reconfigure the product to use a “Virtual Host” for an inbound service:

- Under “Firewall” -> “Virtual Host” -> “Create”, a new “Virtual Host” was created to map HTTP Port 80 on an External IP address to HTTP Port 80 on a Mapped IP address on the private network.

- Under “Firewall” -> “Create Rule”, a rule was added to allow access to this “Virtual Host.”

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

- Under “System” -> “HA” -> “Configure HA”, the parameters to enable HA were entered, including:

  - “HA Configuration Mode” was set to “Active-Passive”,

  - “Dedicated HA Link Port” was set to use “Port-C”, which physically had a cross-over cable connecting the two units,

  - “Auxiliary HA link IP” was set to the IP address which had been manually configured on the second unit, and

  - Ports “Port-A” and “Port-B”, the private and public network interfaces, were selected to be “Monitored Ports.”

- HA was then enabled using the “Enable HA” button.

HA Testing , Criteria Violations, and Resolutions

Section Introduction

Once configured to meet *The HA Firewall Certification Criteria,* the Candidate Firewall Product should be able to perform stateful failover of established firewall sessions in various network and firewall outage scenarios within a defined time limit and without introducing security vulnerabilities. It must also be able to log events related to the failover as well as provide required administrative functions.

During HA testing, the Network Security Lab team uses an in-house-created testbed which provides the ability to create and monitor the required number of sessions during the various network and firewall outage scenarios. Testing for the 1.0 criteria utilizes connections to a website protected by the firewall to provide the required number of sessions to determine if the product meets the criteria requirements.

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.

Test Parameters

According to the HA criteria, products are to be tested at 66.6% of the product's documented number of simultaneous connections. Specifications for the CR50i listed its ability to handle 220,000 connections. The required percentage of connections combined with rounding due to the parallel nature of the testbed put the tested number of connections at 146,656.

While not specified by the criteria, the connection rate of sessions is a factor both in the overall ability for the product to support the tested number of connections and to ensure that tests can be completed before sessions begin to be timed-out. The CR50i specifications listed its ability to handle 3,000 connections per second. 2,700 connections per second (90% of the listed specifications) was selected as the target connection rate.

Results

The following HA criteria violations were found by the Network Security Lab team during testing and subsequently addressed by Elitecore in updated software:

- The product was not initially able to handle the required number of connections in conjunction with a connection rate sufficiently quick enough to allow tests to complete before the connections began to be timed-out.

- The product appeared to be incorrectly maintaining state on failed-over connections such that phantom connections would limit the number of connections the product could handle in subsequent tests as well as cause connections utilizing repeated TCP port numbers to be erroneously denied.

- Logs for HA-related events could only be accessed using a CLI command to list HA logs in a manner which was not persistent. Later software versions provided for the ability to log HA events using syslog.

- There was no log message for the startup of a non-active / auxiliary unit.

- There was not an administrative function to make a given unit Active on demand. Later software versions provided this ability with a "Put on StandBy" function which would then cause the non-Active unit to become Active.

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 documentation initially provided left a number of questions when it came to HA-related functionality. The documentation later provided, as listed previously in the Candidate Firewall Product Components section, was much improved.

- The CR50i can establish connections quicker than its specified rate. However, when this was allowed to happen, not all of those connections would failover during an outage event.

- Originally, manual clock changes on the primary unit did not affect the auxiliary unit and one was not allowed to change the time on the auxiliary unit while HA was enabled. Later software versions updated the time on the auxiliary unit when the clock was changed.

Conclusion

The Candidate Firewall Product met all the criteria elements in Version 1.0 of *The High Availability Firewall Certification Criteria* module and therefore has attained ICSA Labs HA Firewall Certification. The Candidate Firewall Product will remain continuously deployed at ICSA Labs for the length of the testing contract. In the event that the Candidate Firewall Product is found to no longer meet the criteria 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 HA Firewall Certification.

Certification Maintenance on Future Versions

The Cyberoam CR50i, like all products and product groups that are granted ICSA Labs HA 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.

Four circumstances will cause the CR50i to have its ICSA Labs HA Firewall Certification revoked:

1. Elitecore withdraws from the ICSA Labs HA Firewall Certification Program.

2. The product fails a periodic spot-check and Elitecore 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.

4. Elitecore fails to maintain the CR50i's ICSA Labs Firewall Certification.

Testing Information

Lab Report Date

February 9, 2009

Test Location

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

Product Headquarters

Elitecore Technologies Ltd.
904, Silicon Tower, Bh. Pariseema Building,
Ahmedabad-380006
Gujarat, India

Copyright