# Table of Contents

## Introduction ................................................................................................................................................................ 1

## Documentation .......................................................................................................................................................... 1
  - Installation Documentation ......................................................................................................................... 1
  - Administration Documentation ..................................................................................................................... 1
  - Log Interpretation ......................................................................................................................................... 1
  - Accurate Documentation .............................................................................................................................. 1

## Functional Testing .............................................................................................................................................. 1
  - Security Policy Enforcement ....................................................................................................................... 2
  - Proper Services Operation ............................................................................................................................ 2
  - Data Integrity ................................................................................................................................................ 2
  - Data Confidentiality ..................................................................................................................................... 2
  - User Authentication .................................................................................................................................... 2
  - User Authorization ...................................................................................................................................... 2

## Web Application Firewall Specific Functionality .................................................................................................. 2
  - Web Attack Protection and Prevention ......................................................................................................... 2
  - Enforcement Method ...................................................................................................................................... 2
  - Hiding Internal Application Structure ......................................................................................................... 3
  - Accommodating Application Changes .......................................................................................................... 3
  - SSL Support .................................................................................................................................................. 3
  - Client Authentication .................................................................................................................................... 3
  - Transparent Service ...................................................................................................................................... 3
  - Protocol Configurability ............................................................................................................................... 3

## Vulnerability Testing ............................................................................................................................................. 3
  - Administrative Access Testing ..................................................................................................................... 3
  - Exploit Testing .............................................................................................................................................. 4
  - Denial of Service .......................................................................................................................................... 4
  - No Vulnerabilities Introduced ....................................................................................................................... 4

## Logging .................................................................................................................................................................. 4
  - Required Log Events ...................................................................................................................................... 4
  - Required Log Data ........................................................................................................................................ 5
  - Accuracy of Log Data ................................................................................................................................... 5
  - Precision of Date and Time ........................................................................................................................... 5
  - Log Data Presentation ................................................................................................................................... 5
  - Standard Log Format ..................................................................................................................................... 6
  - Linking Multiple Log Files for a Single Event ............................................................................................... 6
  - User Privacy Compliance ............................................................................................................................. 6
  - Application-Level Forensics Functionality .................................................................................................... 6

## Administration ..................................................................................................................................................... 6
  - Administrative Interface ............................................................................................................................... 6
  - Administrative Functions ............................................................................................................................... 6
  - Administrative Functions Testing .................................................................................................................. 6
  - Administrative Interface Authentication ....................................................................................................... 6
  - Security Policy Confidentiality ..................................................................................................................... 6
  - Remote Administration ................................................................................................................................. 7
  - Concurrent Administrative Sessions (Conditional) ......................................................................................... 7

## Persistence ............................................................................................................................................................ 7
  - Administrative Configuration Persistence .................................................................................................... 7
  - Security Policy Persistence ............................................................................................................................ 7
  - Log Data Persistence ..................................................................................................................................... 7
  - Date and Time Persistence ............................................................................................................................. 7
  - Remote Administration Configuration Persistence .......................................................................................... 7

## Glossary .................................................................................................................................................................. 8
Introduction

This Web Application Firewall Certification Criteria document describes test criteria for products that implement security policy enforcement for the protection of HTTP and HTTPS web-based applications.

With the exception of the Documentation requirements, and unless otherwise noted, the Candidate Web Application Firewall Product must only meet the requirements that appear in this document after having been installed and configured according to the Installation Documentation. The Documentation requirements must be met at all times before and after installation.

Refer to the Glossary for a definition of terms used in this document.

Documentation

SUMMARY: Verify that the vendor supplies adequate documentation to enable an administrator to properly and securely install and administer the Candidate Web Application Firewall Product.

Installation Documentation

DO1 – The Candidate Web Application Firewall Product must include written and/or electronic documentation containing the following information:

A. Instructions to properly and securely install the Candidate Web Application Firewall Product;
B. Minimum system requirements for all components of the Candidate Web Application Firewall Product;
C. Default settings (e.g., usernames, passwords, IP addresses, etc.);
D. The base version of all software and firmware components comprising the Candidate Web Application Firewall Product;
E. Whether or not customer support is available;
F. (Conditional) Where and how customers access customer support, in the event that customer support is available;
G. (Conditional) Where to obtain patches and how to apply them in the event that patches are required for any component of the Candidate Web Application Firewall Product.

Administration Documentation

DO2 – The Candidate Web Application Firewall Product must include written and/or electronic documentation applicable for administering and maintaining the Candidate Web Application Firewall Product.

Log Interpretation

DO3 – The Candidate Web Application Firewall Product must include written and/or electronic documentation indicating how to properly interpret required log data.

Accurate Documentation

DO4 – The written and/or electronic documentation used for the purposes of testing must be accurate.

Functional Testing

SUMMARY: Verify that the services provided by the Candidate Web Application Firewall Product operate securely and as a reasonable user would expect. Any claims made by the vendor will be tested and verified to be true and accurate.
Security Policy Enforcement
FS1 – The Candidate Web Application Firewall Product must demonstrate through testing that its security policy cannot be circumvented.

Proper Services Operation
FS2 – The Candidate Web Application Firewall Product, while enforcing a security policy, must allow permitted services in that security policy to function as designed.

Data Integrity
FS3 – The Candidate Web Application Firewall Product must demonstrate through testing that all data permitted by the security policy must maintain its integrity. NOTE: The Candidate Web Application Firewall Product may modify or remove content as defined in the security policy.

Data Confidentiality
FS4 – The Candidate Web Application Firewall Product must demonstrate through testing that it is capable of being configured to preserve the pre-existing confidentiality of all data permitted by the security policy.

User Authentication
FS5 – (Conditional) In the event that the Candidate Web Application Firewall Product supports supplemental user authentication, it must demonstrate through testing that it can properly use supported authentication mechanisms to authenticate any user attempting to access protected network resources.

User Authorization
FS6 – (Conditional) In the event that the Candidate Web Application Firewall Product supports supplemental user authentication, it must demonstrate through testing that authenticated users only have access to resources for which they are authorized.

Web Application Firewall Specific Functionality

Web Attack Protection and Prevention
HF1 – Candidate Web Application Firewall Product must be capable of being configured to block a representative set of the most common application vulnerability categories without negatively affecting intended functionality of the protected web application including but not limited to the following classifications/vulnerabilities:

- Buffer overflow / code injection
- Cross Site Scripting
- Cross Site Request Forgery
- Improper Input Validation
- Denial of Service
- Session Mismanagement
- Insufficient Protection of Application Resources / Information Leakage
- Faulty Access Control / Authentication Coding

Enforcement Method
HF2 – The Candidate Web Application Firewall Product must effectively employ a combination of the following enforcement methods to effectively prevent web system attack.
• Negative Security Model – The Candidate Web Application Firewall Product must be capable of creating and enforcing a security policy based upon the negative security model including attack-signature and/or rule-based detection and prevention.

• Positive Security Model – The Candidate Web Application Firewall Product must be capable of creating and enforcing a security policy based upon positive Web application behavior; including unknown or potential attacks without negatively affecting intended functionality of the protected web application.

• URL Rewriting/Normalization – The Candidate Web Application Firewall Product must be capable of utilizing URL normalization and rewriting to prevent malicious attacks.

• Active Learning – The Candidate Web Application Firewall Product must be capable of augmenting web application protection with an active learning mechanism without negatively affecting intended functionality of the protected web application.

Hiding Internal Application Structure
HF3 – The Candidate Web Application Firewall Product must be able to mask the internal Web application architecture, structure, and naming.

Accommodating Application Changes
HF4 – The Candidate Web Application Firewall Product must be able to implement reversible incremental changes to the security policy for protected Web applications without rendering the site inoperable or insecure, with sufficient policy configuration granularity to perform changes such as policy editing, tuning, rollback, relaxing of specific rules, while fully operational in production.

SSL Support
HF5 – The Candidate Web Application Firewall Product must support encryption of the Web transaction data using SSL either by passively decrypting SSL sessions or by terminating SSL, decrypting and re-creating the session. This is not applicable if the Candidate Web Application Firewall Product is embedded in the web-server outside of the SSL session security perimeter. The encryption mechanism must be an industry standard product providing secure and anomaly free functionality.

Client Authentication
HF6 – The Candidate Web Application Firewall Product must be capable of providing support for standard client authentication methods including basic, Digest, Windows, and client-side certificates.

Transparent Service
HF7 – The Candidate Web Application Firewall Product must support the capability to bypass the enforcement of security policy rules for specified Web applications.

Protocol Configurability
HF8 – The Candidate Web Application Firewall Product must have sufficient configurability to provide sufficient control over traffic flows at the protocol level including HTTP support, encoding methods/types, protocol validation, and configuration of protocol parameters such as request, response and header lengths.

Vulnerability Testing

Administrative Access Testing
VT1 – The Candidate Web Application Firewall Product must demonstrate through testing that no unauthorized control of its administrative functions can be obtained.
Exploit Testing
VT2 – The Candidate Web Application Firewall Product must demonstrate through testing that it is not vulnerable to any publicly known exploits or vulnerabilities.

NOTE to VT2: In the event that the Candidate Web Application Firewall Product incorporates a 3rd party operating system (e.g. Microsoft © Windows ™, *NIX), then the Candidate Web Application Firewall Product must provide reasonable and appropriate measures to protect the host operating system from any publicly known vulnerabilities. As such, the Candidate Web Application Firewall Product may include operating system hardening guidelines to meet this requirement.

Denial of Service
VT3 – The Candidate Web Application Firewall Product must demonstrate through testing that the device is not rendered inoperable by any trivial Denial of Service attack.

NOTE to VT3: It is assumed that the Candidate Web Application Firewall Product resides behind an ICSA Labs Certified Firewall (network firewall). Therefore, the scope of this requirement is limited to valid network traffic destined for the Web Application Firewall or the servers it is protecting, for example, services such as HTTP, HTTPS, and Remote Administration.

No Vulnerabilities Introduced
VT4 – The Candidate Web Application Firewall Product must demonstrate through testing that it does not introduce any publicly known vulnerabilities to protected network hosts or permit the enumeration of any potentially sensitive network or host information.

Logging

SUMMARY: Verify that the Candidate Web Application Firewall Product is able to provide an administrator the means necessary to properly audit security-related events. The captured log data should be able to provide an administrator enough information to monitor events that may impact the security or integrity of the Candidate Web Application Firewall Product itself or the resources it was designed to protect.

Required Log Events
LO1 – The Candidate Web Application Firewall Product must have the capability to log all of the following event types. NOTE: It is not required that logging is enabled at all times or that it is enabled by default:

A. All successful and unsuccessful attempts to access resources protected by the configured security policy;
B. All successful and unsuccessful attempts to authenticate to an administrative interface;
C. All successful and unsuccessful authentication attempts required to access resources protected by the security policy;
D. All changes to the configured security policy;
E. Each system startup;
F. All manually entered changes to the system clock.

NOTE to LO1-A: An attempt, whether successful or unsuccessful, is defined as the initiation or denial of the HTTP transaction.

NOTE to LO1-C: Criteria element LO1-C refers to when the Candidate Web Application Firewall Product is performing the authentication to access resources protected by the security policy.
Required Log Data
LO2 – For each event that the Candidate Web Application Firewall Product logs, the following log data elements, at a minimum and when applicable, must be captured in the log:

A. Date and time:
   1. The date recorded by the Candidate Web Application Firewall Product for each event in the log must consist of the four-digit year, the month and the day.
   2. The time recorded by the Candidate Web Application Firewall Product for each event in the log must consist of the hour, the minute and the second.
B. Source IP address or hostname;
C. Destination IP address or hostname;
D. Source port;
E. Destination port;
F. Service Name or Protocol (HTTP, HTTPS);
G. URL (Path, Parameters);
H. HTTP Method (GET, POST);
I. Session Identification (according to Candidate Web Application Firewall Product);
J. Disposition of the event (e.g., permitted, denied, etc.);
K. Reason for failure, if access denied;
L. User identification, where applicable;
M. Description of security policy alterations, additions, or deletions;
N. Statement of success or failure to authenticate at an Administrative Interface;
   1. Failed authentication attempts must include the reason for the failure.

NOTE to LO2-A: In accordance with the LO1-F requirement to log system clock change events, the date and time both before and after the change must be recorded using the data elements required by LO2-A.

NOTE to LO2-C: In the event that multiple web sites are hosted on a single IP address, the Candidate Web Application Firewall Product must include the hostname requested in the HTTP header.

Accuracy of Log Data
LO3 – All log data captured by the Candidate Web Application Firewall Product must be accurate.

Precision of Date and Time
LO4 – The date and time recorded by the Candidate Web Application Firewall Product for all log events must reflect the exact date and time to the precise second that the event occurred.

Log Data Presentation
LO5 – All required log data for all required log events must be available for review upon demand and presented in a human readable format while preserving the relative sequence of events.

NOTE to LO5: Review upon demand is defined as the ability to retrieve current log events when desired. For instance, if the log events are being queued and sent to a log viewer (whether local to the Candidate Web Application Firewall Product or being sent to a remote logging mechanism) periodically, then a mechanism to either to view the queued log events directly or release them would meet this requirement.
Standard Log Format
LO6 – The Candidate Web Application Firewall Product must be capable of producing at least one industry standard log format (e.g., W3C, syslog, etc.) for exporting to external applications (application-level forensics tools, application vulnerability scanners, etc.)

Linking Multiple Log Files for a Single Event
LO7 – (Conditional) In the event that the Candidate Web Application Firewall Product uses multiple log messages to record a single log event, each log message must include a clear, accurate link between the corresponding log messages.

User Privacy Compliance
LO8 – The Candidate Web Application Firewall Product must be able to identify and mask sensitive, confidential, or private fields in logs, as defined by an administrator.

Application-Level Forensics Functionality
LO9 – The Candidate Web Application Firewall Product must be able to provide functionality for Application-Level Forensics, including event investigation, navigation, and correlation.

Administration

Administrative Interface
AD1 – The Candidate Web Application Firewall Product must include a secure administrative interface from which all administrative functions are accessible to an administrator. In the event that an available interface is found to be insecure, it must be possible to disable that interface and still access all required administrative functions.

Administrative Functions
AD2 – Administrative functions must exist as part of the Candidate Web Application Firewall Product to:

A. Configure and change the security policy;
B. Configure and change administrative user authentication information;
C. Configure and change remote administration settings, if applicable;
D. Configure and change or acquire date and time;
E. Enable logging of required log events;
F. Review required log data;
G. Ability to activate a previous system configuration and security policy on-demand.

Administrative Functions Testing
AD3 – The Candidate Web Application Firewall Product must demonstrate through testing that all available administrative functions work properly.

Administrative Interface Authentication
AD4 – The Candidate Web Application Firewall Product must be capable of requiring authentication using a valid username and password combination or some stronger form of authentication before permitting access to any administrative functions.

Security Policy Confidentiality
AD5 – The Candidate Web Application Firewall Product must demonstrate through testing that it incorporates reasonable measures to protect the confidentiality and integrity of data contained within its security policy.
Remote Administration

AD6 – The Candidate Web Application Firewall Product must demonstrate through testing that it can be configured to make a remotely accessible administrative interface available and that, at a minimum, supports the following requirements:
   A. Encryption using industry standard and accepted cryptography and key lengths;
   B. Inactivity timeouts;
   C. The ability to logoff the current administrative session on demand.

Concurrent Administrative Sessions (Conditional)

AD7 – In the event the Candidate Web Application Firewall Product allows concurrent administrative sessions, then the Candidate Web Application Firewall Product must take adequate measures to protect the integrity of the configured security policy during alteration.

Persistence

Administrative Configuration Persistence

PE1 – In the event that the Candidate Web Application Firewall Product is restarted or electrical power is lost or removed, all administrative configuration information must persist and remain unchanged.

Security Policy Persistence

PE2 – When electrical power is reapplied after being lost or removed from the Candidate Web Application Firewall Product, the Candidate Web Application Firewall Product must do one of the following:
   A. Enforce the same security policy that was being enforced prior to the loss or removal of power; or
   B. Enforce a deny-all security policy, while including an Administrative Function(s) capable of restoring the Candidate Web Application Firewall Product to the same security policy that was being enforced prior to the loss or removal of power.

Log Data Persistence

PE3 – In the event that the Candidate Web Application Firewall Product is restarted or electrical power is lost or removed, all log data not in transit must persist and remain unchanged. NOTE: The Candidate Web Application Firewall Product may use a separate logging server to meet this requirement.

   NOTE to PE3: If log events are queued and sent in batches to the log viewer (whether local to the Candidate Web Application Firewall Product or to a remote logging mechanism) these messages must also be persistent and not lost when power is lost or removed.

Date and Time Persistence

PE4 – In the event that the Candidate Web Application Firewall Product is restarted or electrical power is lost or removed, the date and time must persist and remain unchanged. NOTE: The Candidate Web Application Firewall Product may use NTP in symmetric active mode as defined in RFC 1305 to meet this requirement.

Remote Administration Configuration Persistence

PE5 – In the event that electrical power is lost or removed from the Candidate Web Application Firewall Product, Remote Administration settings must remain configured the same when electrical power is reapplied.

NOTE1 TO PERSISTENCE REQUIREMENTS – The PERSISTENCE requirements are not intended to cover situations where electrical power is lost or removed while exercising any of the Administrative Functions.
NOTE2 TO PERSISTENCE REQUIREMENTS – With the exception of PE1, the PERSISTENCE requirements are not intended to cover situations where the Candidate Web Application Firewall Product hardware becomes faulty as a result of a loss or removal of power.

Glossary

Administrative Functions – The operations or actions that an administrator can perform on the Candidate Web Application Firewall Product. They are only available through an Administrative Interface defined above.

Administrative Interface – Any interface which enables an administrator to configure or manage the Candidate Web Application Firewall Product. Administrative interfaces may include a Graphical User Interface (GUI) or a Command Line Interface (CLI). Administrative interfaces may be accessed locally or remotely via any number of methods, including but not limited to KVM, serial console, or via network access. Each administrative interface will be listed and examined separately.

Administrator – Any individual responsible for configuring, managing, or maintaining the Candidate Web Application Firewall Product. Any individual granted full or partial read/write access to an administrative interface is considered an administrator.

Application Buffer Overflow – Exceeding the quantities expected by the application within a given field.

Application Error Handling Problems – Application error messages that reveal detailed application implementation details or potential flaws that could assist an attacker with potential application exploitation.

Application Misconfigurations – Web server and application server system misconfigurations that could potentially result in the total compromise of a website and/or backend systems.

Backdoors and Debugging Commands – Exploitation of application features aimed for the development environment only.

Candidate Web Application Firewall Product – The complete system submitted to ICSA Labs to be evaluated against the criteria during certification testing. This includes any and all documentation, hardware, firmware, software, host operating systems, management stations, etc. used to meet the criteria requirements. Common services such as Syslog and NTP are provided by ICSA Labs and are not considered part of the Candidate Web Application Firewall Product.

Command Injection – Execution of unchecked “system commands” or scripts on web servers, database servers, and other systems supporting the application.

Configured Security Policy – A persistent set of explicit or implicit rules that help define how, when, and what resources are accessed and by whom. This only applies to static rules that are defined by an administrator.

Cookie – A text file stored on a user’s computer used to identify the user when visiting a web site.

Cookie Poisoning – Modification of a cookie to gain unauthorized information about a user for purposes such as identity theft.

Cross Site Request Forgery – Also known as CSRF, XSRF, or Cross Site Reference Forgery. This attack works by exploiting the trust websites and users. This is accomplished by a user accessing a website that has a hidden, imbedded link containing a URL path to a protected page on a vulnerable website that...
the user accesses. The user’s browser attempts to load this link, unbeknownst to the user, and thus allows the attacking website to access something secure on the user’s account on the vulnerable website. Cross Site Scripting, also known as XSS, is the insertion of malicious code into a web site or web-based application, typically in the form of JavaScript, which executes client-side when viewed by another user’s web browser or application.

Directory Traversal – The disclosure or reading of data or application files outside the intended accessible directory tree.

Documentation – Any documents made available to customers in hard copy or electronic form used to learn how to properly use or operate a product distributed by the vendor. Documentation may be included with the purchase price or sold as a separate component. Hard copy documentation must be delivered in a bound and organized format. Electronic documentation can be made available on-line via the web or FTP, or it can be delivered on CD in PDF, HTML, or other industry accepted formats. Documentation delivered only through email or other private communication may not be used to meet documentation requirements. Context-sensitive help, though useful, is also not considered a permissible way to meet requirements.

Dynamic Security Policy – A non-persistent set of rules that define how, when, and what resources are accessed and by whom. This only applies to the components of a policy that are dynamically extracted from other rules or created during runtime.

Encryption – The translation of data into a secret format. Encrypted messages are designed to be reversible and restored to their original format.

Forceful Browsing – Attempts at bypassing the application flow.

Group – A categorization of multiple users with similar access rights. Groups are used to control access to resources when multiple users share the same privileges.

Harden – Configure a host to be resistant to attack by removing or disabling any unnecessary features, services, or applications.

Hash – Also known as “Message Digest”. When used as a noun, it is a fixed-length key representing a variable-length message. When used as a verb, it is the act of converting a variable-length message into a fixed-length key. Hashing algorithms are designed to operate one-way and the resulting hash values cannot be restored to their original format.

Hidden Manipulation – Tampering with hidden field values.

Known Vulnerabilities – Vulnerabilities that use known, published bugs to exploit holes in an operating system, service, or application.

Local Administration – Administration performed while directly connected to a device, usually through a direct serial connection or with the use of a keyboard, mouse, and monitor.

Log – When used as a noun, it is defined as a record of an action or event stored in a persistent format. When used as a verb, it is the act of capturing an action or event and writing it to a file.

Log Event – A log message or collection of log messages used to identify and report a single system or network event.

Log Message – A single message recorded in a log file. Multiple log messages may be used to record a single log event.
Malicious User – Any individual who attempts to access resources he is not authorized to access. A malicious user may also attempt to deny other users access to resources for which they are permitted access.

META Characters – Changing the behavior of an application with the aid of meta characters inserted as user input.

Parameter Tampering – Manipulation of the HTTP request structure being sent between the client (web browser) and the application with parameter values that fall outside preconfigured or expected ranges.

Remote Administration – Administration performed through a network connection. This includes connections from public, private, and dedicated management networks. Remote administration may be performed using a web browser, custom application, or common service such as SSH. Remote administration may be the normal and preferred means for administering a Candidate Web Application Firewall Product.