CyberSecurity: Attivazione servizio WAF

Firenze, 16 Ottobre 2018

TIX
Tuscany Internet Exchange

Attivazione servizio Web Applicatio Firewall (WAF)

Il servizio WAF consente la protezione delle applicazioni e dei servizi WEB per mezzo di regole di sicurezza (Security Checks).

L'attivazione del servizio WAF deve essere richiesta via ticket dal referente RT dell'applicazione.

L'attivazione del WAF, in mancanza di richieste specifiche, viene eseguita in due fasi:

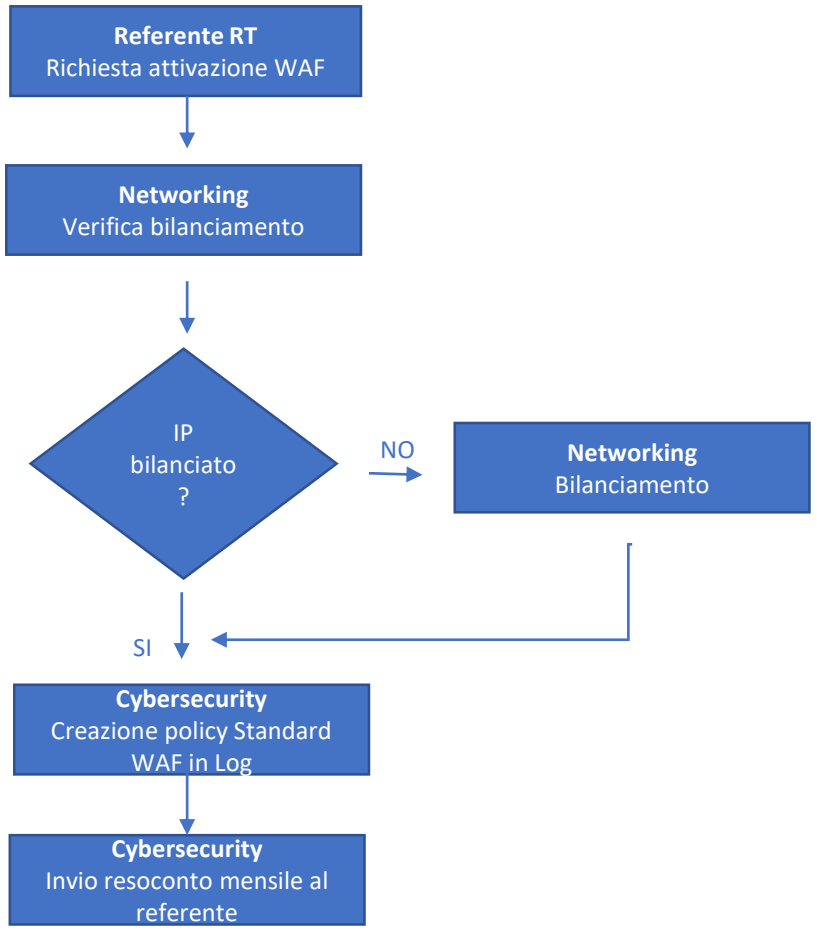
- la prima prevede il monitoraggio degli eventi su un set ristretto di security checks (Policy Standard);
- la seconda, esplicitamente richiesta dal referente RT, prevede il passaggio alla modalità blocco degli eventi ritenuti malevoli.

L'attivazione di controlli ulteriori verrà eseguita su esplicita richiesta del referente RT.

Poiché ogni applicazione ha le sue caratteristiche e livelli di sicurezza già esistenti, è consigliato attivare i security checks in base all'applicazione sotto esame in collaborazione con il team di sviluppo dell'applicazione.

Fase 1 - Attivazione WAF e policy iniziale

La policy iniziale con la quale viene attivato il WAF, in mancanza di richieste specifiche, sarà la Policy Standard in modalità solo log.
Un resoconto sugli eventi loggati sarà inviato al referente RT dell'applicazione web.



Fase 2 – modifica Policy Standard in modalità blocco

La fase 2 di attivazione del WAF prevede l'attivazione della modalità blocco sulla Policy Standard consentendo un grado di protezione di base, un minimo coinvolgimento degli sviluppatori e una bassa probabilità di blocchi indesiderati.

Un resoconto mensile sugli eventi bloccati sarà inviato al referente RT dell'applicazione web.

Livello di protezione di base

- Protezione valida per la maggior parte di contenuti WEB
- Coinvolgimento sviluppatori-> MINIMA
- Falsi positivi o blocchi indesiderati-> RARI

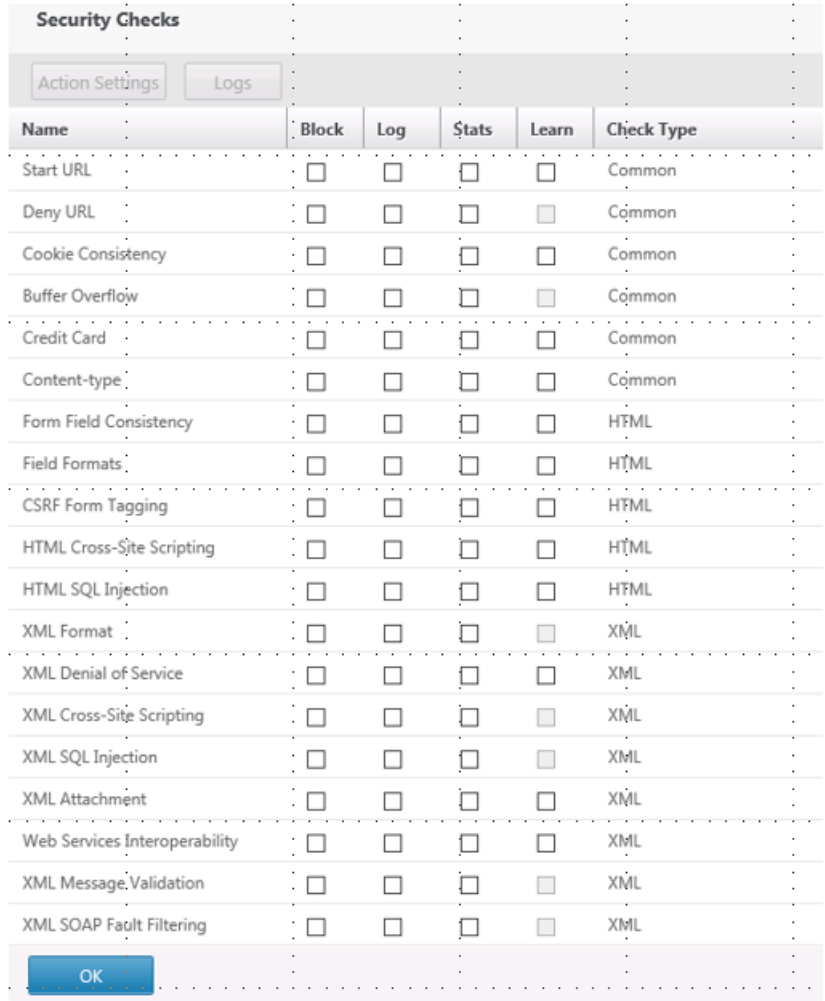
Security Checks

L’immagine visualizza la lista completa dei Security Checks disponibili, raggruppati per tipologia

Common security Checks

HTML security Checks

XML security Checks



WAF – Controlli aggiuntivi, IP Reputation e Advanced mode

Controlli aggiunvivi attivabili sui Security Checks non compresi nella policy standard ed ulteriori affinamenti della policy standard possono essere messi in opera a fronte di richieste specifiche con un'analisi basata su un processo di «learn» in cui la tipologia di traffico (richieste e azioni utente) verso l'applicazione proveniente da indirizzi ip «fidati» viene inserito in una whitelist, tutto il resto del traffico non conforme alle tipologie «learned» verrà bloccato.

E' possibile attivare un'ulteriore controllo di sicurezza basato sull'IP Reputation, in pratica l'ip sorgente delle richieste verso il server protetto da WAF viene controllato per verificare che non appartenga a range di ip malevoli.

Il WAF prevede un Basic Mode ed un Advanced Mode.
Rispetto al Basic, che è quello di default, il modo Advanced prevede che il WAF effettui l'ispezione delle risposte, memorizzi le sessioni utente e valuti se il client abbia inviato al server un form compilato in ogni suo campo, non alterato, con dati conformi in termini di tipo (integer, character, ecc.) e dimensioni (max length). In pratica l'advanced mode prevede la Sessionization del traffico.

Controlli aggiuntivi - Processo di Learn - Obiettivi e fasi

Obiettivo

Il processo di Learn, basandosi sull'utilizzo dell'applicazione WEB da parte di un utente «fidato», ha l'obiettivo di fornire in modo rapido e automatico delle regole WAF generali per la messa in sicurezza dell'applicazione.

Fasi

Fase 1: Learn su navigazione utente fidato e creazione Policy-Baseline in modalità LOG

a. Revisione per consolidamento, con supporto sviluppatori, delle regole generali create dal Learn

Fase 2 : Validazione Policy-Baseline e creazione Policy-Definitiva

a. Verifica LOG con supporto sviluppatori in caso di presenza anomalie
b. Decisione sull'attivazione della Policy baseline e decisione su quali regole abilitare in modalità BLOCCO

Fase 3(*): Learn su navigazione utente internet

a. Verifica LOG con supporto sviluppatori
b. Creazione Policy definitiva e decisione su quali regole abilitare in modalità BLOCCO

(*): Fase 3 necessaria solo se la Fase 2 è non è esaustiva o la complessità dell'applicazione non permette di vagliare tutte le casistiche

Esempio di Processo di Learn e attivazione WAF

Step 1 - Fasi attivazione WAF in ambiente di COLLAUDO			
Fase	**Obiettivo**	**Periodo (*)**	**Personale necessario**
Learn	Acquisizione navigazione lecita	omissis	omissis
Verifica e Deploy	Creazione regole WAF	omissis	omissis
Log	Monitoraggio falsi positivi	omissis	omissis
Blocco e Log	Attivazione blocco	omissis	omissis

Le regole create nello Step 1 per l'ambiente di Collaudo sono utilizzate per costruire la policy iniziale del corrispondente ambiente di Esercizio

Step 2 - Fasi attivazione WAF in ambiente di ESERCIZIO			
Fase	**Obiettivo**	**Periodo (*)**	**Personale necessario**
Log	Monitoraggio falsi positivi	omissis	omissis
Blocco e Log	Attivazione blocco	omissis	omissis

Nel caso non fosse disponibile l'ambiente di Collaudo, si procederà solo con le fasi descritte nello Step1 applicate all'ambiente di Esercizio

(*) valori minimi e massimi definiti in base ai casi d'uso comuni, la variazione dipende dalla complessità dell' applicazione e dal grado di protezione richiesto.