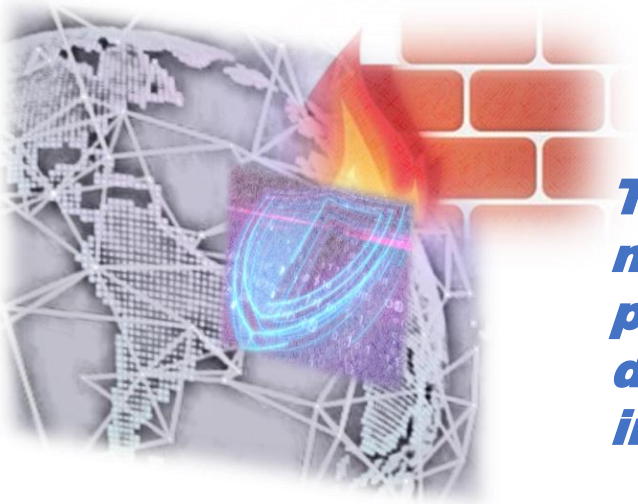
Cabling & Wireless DIGITAL NEWS

Febbraio 2022



Tecniche per il miglioramento delle prestazioni di filtraggio del traffico in reti industriali multi-firewall

[a] *Luca Durante, Marcello Maggiora, Lucia Seno, Adriano Valenzano*

Gli attacchi alle reti telematiche condotti attraverso il cyberspazio rappresentano un problema di estrema attualità che causa continua preoccupazione nella comunità degli esperti di sicurezza e attira costantemente l'attenzione dell'opinione pubblica e dei media. In uno scenario globale altamente interconnesso, quale quello che caratterizza la società moderna, l'esposizione a cyber-minacce riguarda ormai tutti i tipi di infrastrutture di rete [1] e, inevitabilmente, anche quelle a carattere "industriale" utilizzate in diversi settori applicativi come il manufacturing e la produzione, i sistemi di controllo distribuiti, le reti e le infrastrutture critiche per la mobilità, il trasporto e la distribuzione dell'energia, dell'acqua potabile etc.

In tali contesti, in particolare, la convergenza e la condivisione di tecnologie tra settori fino a qualche tempo fa rigidamente distinti all'interno delle aziende (si pensi ad esempio all'*operation technology* - **OT** e all'*information technology* - **IT**) stanno sicuramente producendo benefici di tipo tecnico, funzionale ed economico, ma rischiano anche di spalancare le porte ad hacker e cyber-criminali ampliando in modo significativo il numero di "bersagli" a loro appetibili oltre a permettere una migliore e più comoda accessibilità ai sistemi target anche da postazioni remote.

Come noto le tecniche di difesa in queste situazioni si basano su strategie e meccanismi concepiti in modo da limitare i danni, quando non si è in grado di prevenirli completamente, e fanno leva su tecnologie hardware (h/w) e software (s/w) di ormai ampia diffusione anche in ambienti operativi diversi da quelli per cui essi sono stati originariamente concepiti.

I firewall (fw), tra le varie contromisure disponibili, sono forse gli strumenti più utilizzati anche in ambito industriale per proteggere zone e/o sotto-reti, filtrando opportunamente i flussi di traffico che li attraversano tramite decisioni del tipo "permesso/proibito".

E' infatti opportuno tener presente che i paradigmi Industry 4.0 e Industrial Internet of Things (IIoT), che si stanno rapidamente affermando nel mondo produttivo, esasperano i concetti di connettività e disponibilità delle risorse [2] imponendo di fatto un'evoluzione delle architetture di rete in senso globale, anche in situazioni dove l'isolamento e l'uso massiccio di tecnologie proprietarie garantivano tempo fa un alto livello di *security* e *safety*.

Reti industriali che utilizzano firewall multipli per separare zone logicamente distinte (ad es. secondo lo standard IEC 62443 [3]) non sono più una rarità e spesso un messaggio proveniente dal mondo esterno deve attraversare più livelli di firewall (e quindi di filtraggio) prima di raggiungere la destinazione a cui è diretto.

In queste condizioni, tuttavia, il firewall stesso può diventare un vero e proprio collo di bottiglia sia quando viene sollecitato con traffico elevato, ad esempio per il verificarsi di "picchi" di comunicazione o nel caso di attacchi *Denial of Service* (DoS), sia quando è preso di mira come bersaglio principale degli attacchi cyber.

Il degrado delle prestazioni di un firewall sovraccarico è un problema a cui si cercato di porre rimedio già da tempo e per il quale è possibile trovare nella letteratura specializzata svariate proposte/soluzioni con relativi vantaggi e svantaggi.

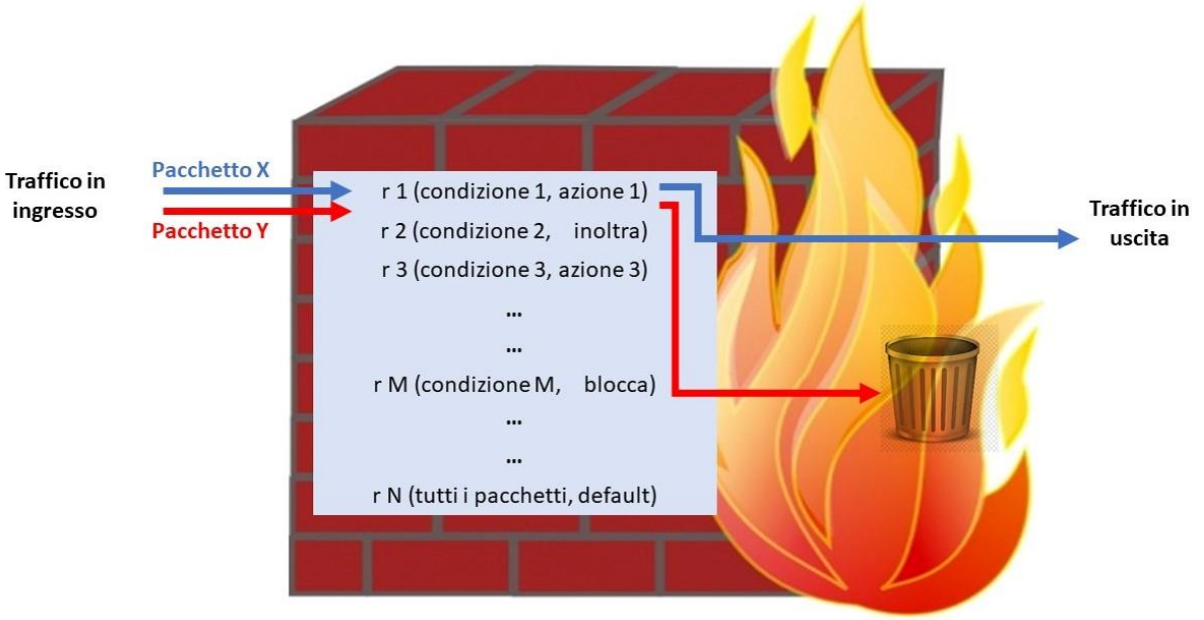


Fig. 1 – Il traffico che attraversa un firewall viene analizzato e trattato sulla base di una gerarchia di regole che stabiliscono quali pacchetti devono essere bloccati e quali continuare il loro percorso.

Da un punto di vista piuttosto generale la più semplice attività di filtraggio del traffico da parte del firewall può essere modellata come schematizzato in **Fig. 1.**

In pratica i pacchetti che fluiscono in una determinata direzione (ingresso o uscita) sono sottoposti a verifica tramite un insieme di regole **r** del tipo <condizione, azione>. La condizione solitamente è costituita da specifici valori/intervalli di valori di alcuni campi presenti nel pacchetto: ad esempio per il filtraggio a livello IP tali campi sono source e *destination IP address*, *source* e *destination port* e *protocol type*. Se i campi presenti nel pacchetto soddisfano la condizione della regola, ovvero appartengono agli intervalli in essa specificati, viene eseguita l'azione corrispondente, altrimenti l'analisi del pacchetto prosegue tramite la regola successiva.

In estrema sintesi le azioni prese in considerazione in questo articolo sono quelle che stabiliscono se inoltrare (trasmettere) o scartare (bloccare) il pacchetto esaminato. L'analisi delle regole da parte del firewall avviene in sequenza fino a che o si incontra una **r** la cui condizione verificata o si raggiunge l'ultima **r** della sequenza che specifica l'azione di default (inoltro/scarto) valida per tutti i pacchetti. Con questo tipo di organizzazione il tempo di analisi di un pacchetto da parte di un fw dipende evidentemente dal numero di regole **r** utilizzate e in molti casi cresce linearmente con esso.

Poiché non è raro trovare nella realtà configurazioni di firewall che includano da centinaia a migliaia di regole organizzate anche in modo complesso, si comprende come tale aspetto possa risultare particolarmente critico in condizioni di traffico intenso.

Un altro elemento che influisce sulle prestazioni del firewall è il profilo del traffico che viene sottoposto ad analisi: il comportamento di fw è tanto migliore quanto prima si è in grado di decidere se inoltrare o scartare il pacchetto in esame, ovvero quanto prima si incontra nella sequenza delle regole una r la cui condizione è soddisfatta dai campi del pacchetto. Tenendo presente questi aspetti, le principali tecniche volte a migliorare le prestazioni dei firewall possono essere grossolanamente classificate in soluzioni per singolo fw e soluzioni per fw multipli. Alla prima categoria appartengono approcci di analisi, compressione e riordino delle regole. L'analisi consente di individuare inconsistenze ed errori eliminando regole inutili o ridondanti, mentre la compressione permette di determinare configurazioni di fw tra loro equivalenti dal punto di vista del filtraggio ma con numero di r minimi o quasi. Tipicamente analisi e compressione sono azioni che vengono effettuate offline. Il riordino dinamico, invece, riorganizza le r in base alla probabilità decrescente che le loro condizioni siano soddisfatte.

Per fare ciò è necessario avvalersi di informazioni sul traffico in ingresso al fw che vengono collezionate in tempo reale.

Tra le tecniche volte a migliorare le condizioni di lavoro di fw multipli che si trovano in situazioni di sovraccarico la soluzione proposta in [4] e basata sulla migrazione di regole appare piuttosto promettente anche per l'adozione in contesti industriali. L'architettura di riferimento, in questo caso, è una rete in cui sono presenti due o più livelli di firewall a guardia di sotto-reti diverse come schematizzato in **Fig. 2**.

Quando un fw (il firewall perimetrale nella figura) diviene sovraccarico a causa di un incremento del traffico, dovuto ad esempio ad un attacco DoS, si procede a trasferire le regole di filtraggio per i pacchetti diretti esclusivamente ad una o più delle sotto-reti a valle (che sono a loro volta protette da altri fw) in modo da alleggerire il lavoro di filtraggio del dispositivo in sofferenza. In pratica il traffico diretto a sotto-reti ulteriormente protette non viene più analizzato dal firewall perimetrale ma dirottato a valle di esso tramite l'introduzione di opportune regole di bypass.

Chiaramente il miglioramento delle condizioni operative del primo fw è ottenuto a spese di un incremento del carico di lavoro per gli altri fw nel sistema, che devono disporre delle risorse di elaborazione aggiuntive necessarie a farvi fronte.

L'idea, in apparenza semplice, presenta tuttavia una serie di aspetti delicati che vanno tenuti in debita considerazione.

Le regole, infatti, non sono in genere totalmente indipendenti e non possono essere trasferite in qualunque caso.

Il trasferimento, inoltre, deve preservare l'integrità di sicurezza della rete ovvero i pacchetti ammessi e scartati devono essere assolutamente gli stessi, senza eccezioni, prima e dopo la trasformazione.

Questo ed altri requisiti hanno quindi determinato la necessità di sviluppare un opportuno algoritmo di migrazione descritto in dettaglio in [4] dove viene anche fornita una prova formale di correttezza.

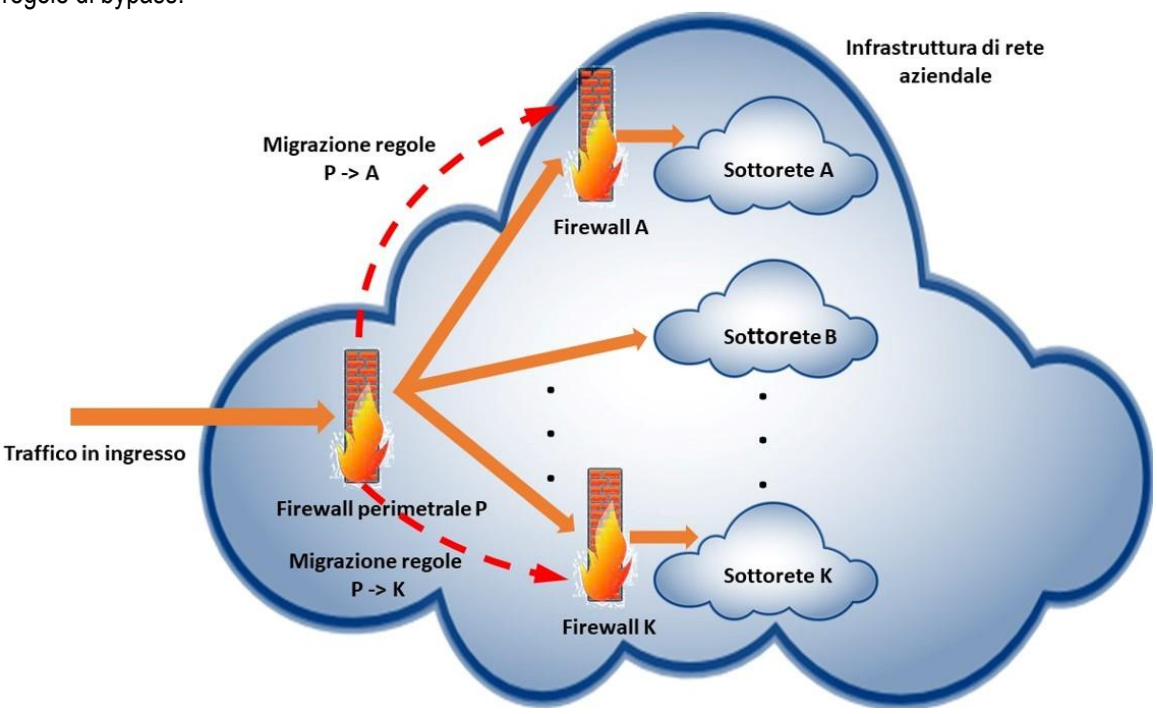


Fig. 2 – Il sistema prevede una gerarchia di firewall costituita dal firewall di bordo e da una serie di firewall a presidio di sottoreti interne. Quando il traffico in ingresso supera un certo limite (ad esempio in caso di attacco DOS) tale da mettere in crisi il trattamento del pacchetto di una parte del traffico viene delegato ad uno o più firewall secondari in base alla destinazione, trasferendo opportunamente le regole necessarie, alleggerendo così il carico del firewall perimetrale.

Il modello di trasformazione proposto è del tutto generale e concepito ad un livello di astrazione sufficientemente elevato da potersi così adattare a gran parte delle implementazioni di fw reali.
Al fine di verificare la bontà della tecnica di migrazione e valutare il guadagno in termini prestazionali in ambienti non simulati sono infine in corso ulteriori studi e sperimentazioni su test-bed di laboratorio che includono firewall reali ad ampia diffusione quali Linux IPtables [5].
Obiettivo di tali lavori è riuscire a disporre di una caratterizzazione del guadagno prestazionale ottenibile in situazioni reali/realistiche, anche in vista di un successivo impiego della metodologia di migrazione in applicazioni pilota. ✓

Riferimenti bibliografici:

[1]. M. Cheminod, L. Durante, and A. Valenzano, "*Review of security issues in industrial networks*", IEEE, Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277–293, Feb. 2013.

[2]. C. Zunino, A. Valenzano, R. Obermaisser, and S. Petersen, "*Factory communications at the dawn of the fourth industrial revolution*", Computer Standards & Interfaces, vol. 71, Aug. 2020, Art. no. 103433.

[3]. International Electrotechnical Commission, "*IEC 62443 Security for Industrial Automation and Control Systems*".

[4]. Luca Durante, Lucia Seno, and Adriano Valenzano. "*A formal model and technique to redistribute the packet filtering load in multiple firewall networks*", IEEE Transactions on Information Forensics and Security, Vol. 16, pp. 2637–2651, Jan. 2021.

[5]. L. Seno, M. Cheminod, I. Cibrario Bertolotti, L. Durante, A. Valenzano "*Improving performance and cyber-attack resilience in multi-firewall industrial networks*", CNR-IEIIT Tech. Report, Jan. 2022.

[a] CNR-IEIIT, Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni
c.so Duca degli Abruzzi 24, 10129 Torino
Email:
{ luca.durante, marcello.maggiora, lucia.seno, adriano.valenzano }@ieiit.cnr.it