NOTA TECNICA · PRESTAZIONI

Quanto costa una blocklist OneFirewall al vostro firewall?

L'abbiamo misurato. Verificare un indirizzo in una blocklist di 300.000 voci ha richiesto al massimo 53,0 ns (miliardesimi di secondo), una volta per ogni nuova connessione. Tenere aggiornata la lista richiede pochi kilobit al secondo.

53,0 ns	0,00037%	3,8 kbit/s
lookup più lento su una lista di 300.000 voci	di un round trip di rete di 14,3 ms in Europa	download medio per una lista di 10.000 voci aggiornata ogni 5 minuti

IN SCALA

Lookup: 53,0 ns

Un round trip di rete in Europa: 14,3 ms

La barra è lunga 170 mm. Nella stessa scala il lookup sarebbe largo 0,63 millesimi di millimetro, troppo sottile per essere stampato. In altre parole: se il round trip durasse un giorno intero, il lookup durerebbe 0,32 s. Se fosse una passeggiata di un chilometro, il lookup sarebbero gli ultimi 3,7 mm.

QUANTO COSTA

Per ogni nuova connessione
al massimo 53,0 ns

Per un milione di nuove connessioni
53 ms di tempo di processore

Traffico di download
3,8 kbit/s (10.000 voci, ogni 5 minuti)

Percorso del traffico
invariato; nulla passa da OneFirewall

COSA HA FERMATO SUL CAMPO

35.000 attacchi al giorno
eliminati per una piattaforma SaaS entro 24 ore. La sua latenza è scesa del 28%. [11]

Il 92,6% degli IP attaccanti
nell'ondata di sfruttamento PHP2Shell era già noto a OneFirewall. Quegli IP hanno inviato il 99,96% dei 32.252 tentativi. [12]

8.934 eventi critici e alti
intercettati in 19 giorni su un'applicazione web, dove il 12% del traffico consentito dal firewall era malevolo. [13]

I dati sul campo provengono dai nostri casi di studio pubblicati, non da questo test.

> Lo scambio è sbilanciato. Il firewall spende qualche decina di nanosecondi per ogni nuova connessione e, in cambio, le connessioni da attaccanti noti vengono scartate al primo pacchetto.

1. Come l'abbiamo misurato

L'unico lavoro per connessione che un feed OneFirewall aggiunge è un lookup: questo indirizzo sorgente è nella lista? Il firewall esegue già un controllo di policy per ogni nuova connessione, quindi il feed rende solo più lunga la lista di indirizzi che controlla. Abbiamo cronometrato proprio quel lookup.

Abbiamo scritto un piccolo benchmark in C e lo abbiamo eseguito su un Apple M3 con 16 GB di RAM (macOS 26.7.1; Apple clang version 21.0.0 (clang-2100.1.1.101); -O2). Crea liste di indirizzi IPv4 pubblici casuali, da 1.000 fino a 1.000.000 di voci, nelle due forme che i firewall usano più spesso. Una tabella hash trova un singolo indirizzo in circa un passo. Una tabella di range ordinata si cerca dimezzando, richiede circa 20 passi con un milione di voci ed è la più lenta delle due.

Ogni configurazione ha eseguito 16.777.216 lookup per sette volte, e abbiamo tenuto la mediana. Ogni lookup attendeva il risultato del precedente, quindi il processore non poteva sovrapporli; i tempi qui sotto sono il costo completo di un singolo lookup, compresi 0,3 ns di overhead del ciclo. Abbiamo ripetuto l'intera prova tre volte e riportiamo la più lenta delle tre.

Tempo di un lookup (il più lento di tre prove)

Voci	Hash, indirizzo non in lista	Hash, indirizzo in lista	Range, non in lista	Range, in lista	Memoria (hash / range)
1.000	10,4 ns	4,7 ns	23,3 ns	10,2 ns	8 KB / 8 KB
10.000	5,8 ns	2,9 ns	20,4 ns	28,0 ns	131 KB / 80 KB
100.000	8,3 ns	4,0 ns	37,9 ns	47,5 ns	1,0 MB / 800 KB
300.000	6,0 ns	3,2 ns	39,0 ns	53,0 ns	4,2 MB / 2,4 MB
1.000.000	15,0 ns	5,3 ns	79,0 ns	63,1 ns	8,4 MB / 8,0 MB

“Non in lista” è il traffico ordinario, il caso più comune; “in lista” è il traffico da un attaccante presente nella lista. I tempi della tabella hash seguono quanto è piena la tabella (29–49% qui), non il numero di voci: per questo 1.000 voci sono risultate più lente di 10.000. 1 ns è un miliardesimo di secondo; 1 μs sono 1.000 ns; 1 ms sono 1.000.000 ns.

2. Tenere aggiornata la lista

Il dispositivo scarica la lista in testo semplice, un indirizzo per riga. Abbiamo generato liste di indirizzi pubblici casuali e le abbiamo misurate: 14,2 byte per voce. La colonna gzip è solo indicativa: gli indirizzi casuali si comprimono peggio di quelli reali, e l'uso della compressione dipende da server e dispositivo. La tabella del traffico usa la dimensione non compressa.

Dimensione della lista

Voci	Testo semplice	gzip	Byte per voce
10.000	142 KB	52 KB	14,2
100.000	1,4 MB	467 KB	14,2
300.000	4,3 MB	1,3 MB	14,2

Traffico di download al giorno, con la velocità media tra parentesi

Voci	Ogni 5 min	Ogni 30 min	Ogni ora	Una volta al giorno
10.000	41,0 MB (3,8 kbit/s)	6,8 MB (0,63 kbit/s)	3,4 MB (0,32 kbit/s)	142 KB (0,01 kbit/s)
100.000	410 MB (38 kbit/s)	68,3 MB (6,3 kbit/s)	34,2 MB (3,2 kbit/s)	1,4 MB (0,13 kbit/s)
300.000	1,2 GB (114 kbit/s)	205 MB (19 kbit/s)	102 MB (9,5 kbit/s)	4,3 MB (0,40 kbit/s)

Il cliente sceglie l'intervallo di aggiornamento, da 60 secondi a 24 ore. Cambia quanto è recente la lista e nient'altro.

3. Perché il lookup si paga una volta per connessione

I firewall che tracciano le sessioni controllano la policy sul primo pacchetto di una connessione e gestiscono il resto dalla tabella delle sessioni. Su FortiGate le sessioni accettate vengono delegate al processore NP e i pacchetti successivi non ripassano più dalla policy [3]. I valori qui sopra si aggiungono quindi una volta per connessione, non per ogni pacchetto.

Lookup più lento come quota di un round trip di rete

Round trip (Verizon, ottobre 2026) [10]	300.000 voci (53,0 ns)	1.000.000 di voci (79,0 ns)
In Europa, 14,3 ms	0,00037%	0,00055%
In Nord America, 33,4 ms	0,00016%	0,00024%
Da Londra a New York, 70,4 ms	0,000075%	0,00011%

Per confronto, Fortinet dichiara per un passaggio completo nel firewall di un FortiGate 100F 4,97 μs con pacchetti UDP da 64 byte [4], circa 94 volte il nostro lookup più lento.

4. Limiti di ciascuna piattaforma

Ogni piattaforma ha una propria dimensione massima della lista e proprie opzioni di aggiornamento. OneFirewall limita ogni feed al massimo della piattaforma, quindi una lista non supera mai ciò che il vendor ha previsto per il dispositivo.

Piattaforma	Opzioni di aggiornamento	Dimensione massima della lista	Altri limiti
FortiGate	Da 1 a 43.200 min, predefinito 5 [1]	300.000 IP per dispositivo, FortiOS 7.4.4 e successivi [2]	Le voci oltre il limite non vengono caricate [2]
Palo Alto Networks	5 min (predefinito), ogni ora, giorno, settimana, mese [7]	50.000 IP in totale; 150.000 su PA-3200, PA-5200, PA-7000 [8]	Fino a 30 liste [8]
AWS WAF (CloudFront, ALB)	Qualsiasi; lo decide la pianificazione della sincronizzazione	10.000 per IP set [5]	Una regola IP set costa 1 WCU a qualsiasi dimensione [5]; una chiamata di aggiornamento al secondo per account e Region [6]
Check Point	Un intervallo per tutti i feed, in secondi; 30 min predefiniti su Quantum Spark R82 [9]	Non pubblicata	

5. Cosa questo test non dice

L'abbiamo eseguito su un processore di uso generale, non su hardware firewall, e non abbiamo misurato alcun modello di firewall. I firewall usano strutture dati proprie e molti usano chip dedicati, quindi i loro valori assoluti saranno diversi dai nostri. Abbiamo cronometrato solo il lookup, non l'intero percorso di un pacchetto nel firewall. I nostri indirizzi erano casuali, mentre liste e traffico reali hanno schemi che questo test non

modella. I round trip sono misure pubblicate da Verizon, non nostre. OneDevice in Serie e WAP stanno sul percorso del traffico per progettazione e sono fuori dall'ambito di questa nota.

Il benchmark è di circa 250 righe tra C e Python. Si esegue con un solo comando e scrive ogni risultato in un file JSON; lo condividiamo volentieri su richiesta.

Fonti

1. Fortinet, FortiOS 7.4.0 Administration Guide: Configuring a threat feed (refresh rate 1-43,200 min, default 5) · https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/379433/configuring-a-threat-feed
2. Fortinet, FortiOS 7.4.4 Administration Guide: Threat feeds (device-wide entry and file-size limits) · https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/9463/threat-feeds
3. Fortinet, FortiOS 7.4.4 Hardware Acceleration Guide (NP fast path: policy match on the first packet, session offloaded) · https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6613da86-0277-11ef-8c42-fa163e15d75b/fortios-hardware-acceleration-744.pdf
4. Fortinet, FortiGate 100F Series data sheet (firewall latency 4.97 µs, 64-byte UDP; firewall throughput 20 Gbps)
5. AWS WAF Developer Guide: IP set match rule statement (up to 10,000 addresses, 1 WCU) · https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html
6. AWS WAF Developer Guide: AWS WAF quotas (5,000 WCU per web ACL, 1 Create/Put/Update call per second) · https://docs.aws.amazon.com/waf/latest/developerguide/limits.html
7. Palo Alto Networks, PAN-OS 11.1: Objects > External Dynamic Lists (refresh: five minutes by default, hourly, daily, weekly, monthly) · https://docs.paloaltonetworks.com/ngfw/help/11-1/objects/objects-external-dynamic-lists
8. Palo Alto Networks, PAN-OS 11.1 Admin Guide: External Dynamic List (IP capacity per model, 30 EDLs) · https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list
9. Check Point, Quantum Spark R82.00.X Admin Guide: IoC Feeds (fetched every 30 minutes by default); sk132193 Custom Intelligence Feeds · https://sc1.checkpoint.com/documents/Appliances/Quantum_Spark_R82.00.X/AdminGuides_Locally_Managed/EN/Content/Topics/IoC_Feeds.htm
10. Verizon, Monthly IP Latency Data (October 2026: Europe 14.263 ms, North America 33.354 ms, Trans-Atlantic 70.440 ms) · https://www.verizon.com/business/terms/latency/
11. OneFirewall Alliance, SaaS platform case study · https://onefirewall.com/it/case-study
12. OneFirewall Alliance, PHP2Shell threat briefing · https://onefirewall.com/it/php2shell-threat-briefing
13. OneFirewall Alliance, Web application case study · https://onefirewall.com/it/case-study-web-application

---

Redatto da OneFirewall Engineering, Londra · support@onefirewall.com · https://onefirewall.com/it/performance-impact