Arbor Networks® TMS

Analisi minacce avanzata, riduzione chirurgica e abilitazione servizio

Caratteristiche e Benefici Principali

Riduzione Chirurgica
Rimozione automatica del solo traffico dell'attacco senza interrompere il flusso del normale traffico aziendale.

Disponibilità e Controllo Illimitata di otto Tbps di Riduzione
Scalabilità delle difese da DDoS a un livello senza precedenti. Distribuzione di capacità di riduzione aggregata fino a otto terabit con gestione centralizzata per distribuzione.

Possibilità di offrire servizi gestiti
Possibilità di soddisfare la rapida crescita nella richiesta di servizi di protezione da DDoS. Utilizza TMS per fornire servizi di sicurezza DDoS cloud redditizi.

Una Lista Completa di Contromisure di Attacco
Proteggi la tua infrastruttura e/o i tuoi clienti dai più grandi e complessi attacchi DDoS voluminosi, in stato di esaustività tcp e a livello applicativo.

Distribuzione flessibile
Distribuzione di intelligence a livello applicativo, rilevamento delle minacce e mitigazione chirurgica in diverse zone della rete per la protezione dell'infrastruttura e generazione di maggior profitto dai servizi di protezione DDoS gestiti.

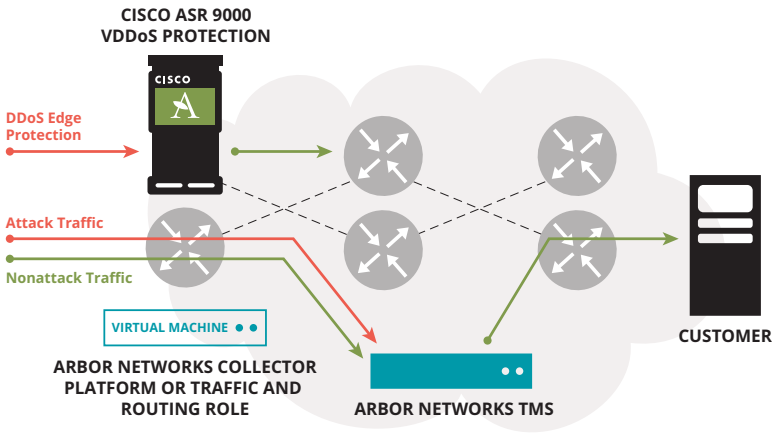
I fornitori di servizi Internet (ISP), i fornitori di servizi cloud e le aziende devono confrontarsi con un problema comune. Gli attacchi DDoS rappresentano un rischio elevato alla disponibilità dei servizi. La potenza, la complessità e la frequenza degli attacchi DDoS è in aumento. Gli operatori dei data center e i provider di rete richiedono una difesa che sia efficace, economicamente efficiente e semplice da gestire. Arbor Networks® TMS è la conoscenza leader nella protezione DDoS. Diversi fornitori di servizi, fornitori di servizi cloud e grosse imprese utilizzano TMS per la mitigation DDoS più di ogni altra soluzione.

La Soluzione Arbor Networks per la Protezione DDoS

La soluzione Arbor Networks integra l'intelligence su tutta la rete e il rilevamento di anomalie con una gestione delle minacce a livello di provider per semplificare l'identificazione e il blocco degli attacchi DDoS a livello di rete e applicativo.

Gli applicativi di rete TMS forniscono il componente vitale di filtraggio del traffico della soluzione Arbor Networks. TMS può essere distribuito in linea per una protezione sempre attiva. A differenza di altri prodotti, supporta anche un'architettura di mitigazione denominata "deviazione/reiniezione". In tal modo, solo il flusso di traffico che trasporta l'attacco DDoS è rediretto al TMS tramite aggiornamenti degli instradamenti emessi dalla soluzione Arbor Networks. TMS rimuove solo il traffico dannoso da tale flusso di pacchetti e inoltra il traffico lecito alla destinazione prevista.

Questo offre ai fornitori di sistemi, alle aziende di gradi dimensioni e ai fornitori di servizi di hosting/cloud di grandi dimensioni un enorme vantaggio. Abilita un singolo TMS centrale per proteggere più collegamenti e data center. Ne deriva un utilizzo più efficiente della mitigazione e una protezione completamente non intrusiva. I dispositivi inline devono ispezionare costantemente tutti i collegamenti monitorati. TMS richiede solo di ispezionare il traffico a esso redirezionato in risposta a un attacco a una determinata destinazione.



ARBOR NETWORKS
The Security Division of NETSCOUT

Diversi metodi di rilevamento e mitigazione delle minacce

Blocco di host dannosi noti utilizzando elenchi di inclusione ed esclusione. L'elenco di inclusione contiene gli host autorizzati, mentre quello di esclusione contiene zombie o host compromessi il cui traffico viene bloccato.

Blocco degli exploit a livello applicativo utilizzando filtri complessi. Il TMS fornisce visibilità e filtraggio del payload dei pacchetti per impedire che attacchi dissimulati impattino servizi essenziali.

Difesa da minacce basate su Web rilevando e mitigando gli attacchi mirati per HTTP. Questi meccanismi consentono inoltre di gestire gli scenari di flash crowd.

Protezione dei servizi DNS vitali da attacchi cache poisoning, a esaurimento delle risorse e di amplificazione. Maggiore visibilità nei servizi DNS.

Protezione dei servizi VoIP da script automatici o botnet che sfruttano i pacchetti per secondo e le propagazioni di richieste non corrette impiegando funzionalità specifiche per rilevare e mitigare gli attacchi a VoIP/SIP.

Ferma grossi attacchi di riflesso/amplificazione come NTP, DNS, SNMP, SSDP, SQL RS o Caricati dall'influenza fino a 80 Gbps di riduzione dell'attacco in un singolo chassis TMS.

Esponi e ferma attacchi nascosti nei pacchetti SSL tramite un Modulo di Sicurezza Hardware (HSM) TMS 2300 opzionale, con il quale decriptare pacchetti SSL, ispezionare e diminuire il traffico dell'attacco e re-criptare e diminuire il traffico del non attacco tornato nel cavo.

Feed di Intelligence® ATLAS

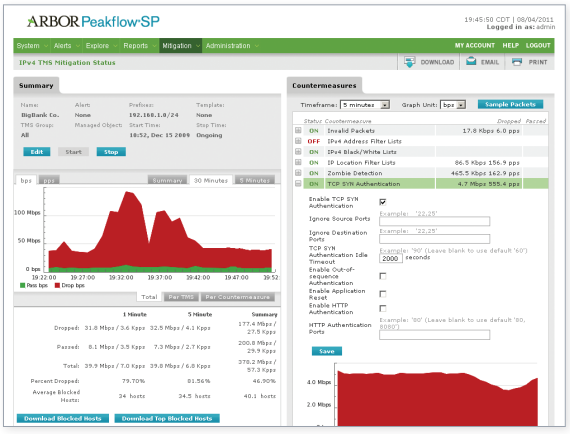
Grazie a una rete globale di monitoraggio del traffico e di sensori, i ricercatori di Arbor hanno sviluppato il Feed di Intelligence ATLAS, una libreria di difese mirate che forniscono la protezione automatica dalla maggior parte degli attacchi basati su botnet. Non appena i ricercatori di Arbor scoprono e neutralizzano minacce emergenti, il Feed di Intelligence ATLAS aggiorna automaticamente il TMS con nuove protezioni.

Rilevamento delle Minacce Completo

I data center e le reti pubbliche offrono più obiettivi agli attacchi DDoS. Questi obiettivi comprendono i dispositivi dell'infrastruttura (ad esempio, router, switch e bilanciatori di carico), sistemi DNS, capacità della larghezza di banda e applicazioni chiave quali Web, eCommerce, voce e video. Anche i dispositivi di protezione quali i firewall e i sistemi di prevenzione dalle intrusioni sono obiettivi degli attacchi. La soluzione Arbor Networks offre la suite più completa e adattiva del settore di funzionalità per il rilevamento di minacce, progettata per proteggere differenti risorse da attacchi complessi e combinati. Queste funzionalità comprendono il rilevamento statistico di anomalie, il rilevamento di anomalie del protocollo, la corrispondenza dei fingerprint e il rilevamento di anomalie profilate. La soluzione Arbor Networks apprende e si adatta costantemente in tempo reale, notificando gli operatori in caso di attacco o di cambiamenti inusuali nella richiesta e nei livelli dei servizi.

Riduzione Chirurgica in 4 Secondi

La chiave di un'efficace riduzione consiste nell'identificare e bloccare il traffico dell'attacco consentendo al traffico lecito di raggiungere la destinazione prevista. Gli attacchi DDoS su grande scala influiscono non soltanto sull'obiettivo previsto ma anche sugli sfortunati clienti che utilizzano il medesimo servizio di rete condiviso. Per ridurre la portata di questo danno collaterale, i fornitori di servizi e hosting spesso bloccano tutto il traffico destinato al sito preso di mira, completando in tal modo l'attacco DDoS. In alcuni casi, anche se si verifica un attacco dal flusso voluminoso creato per esaurire la capacità di banda o un attacco mirato a causare un'interruzione di un sito Web, TMS può isolare e rimuovere il traffico dell'attacco senza influire sugli altri utenti, in meno di 4 secondi. I metodi comprendono l'identificazione e l'esclusione di host dannosi, la riduzione basata sulla posizione geografica dell'IP, la rimozione di pacchetti non corretti e la limitazione della velocità (per gestire con calma i picchi di richieste non dannose). Le riduzioni possono essere automatiche o avviate da operatori e le diverse contromisure possono essere uniteper risolvere attacchi combinati.



Pannello di gestione per le notifiche e la mitigazione in tempo reale

Dashboard di mitigazione in tempo reale

La dashboard di mitigazione in tempo reale TMS è rappresentata da un'unica schermata che mostra agli operatori la causa esatta della notifica DDoS e l'effetto generato sull'attacco dalle contromisure. Consente di modificare le contromisure, di acquisire tutti i pacchetti e di decodificarli per ottenere una visione dettagliata dei flussi dei pacchetti normali e di attacco. Queste informazioni sono memorizzate per riferimento futuro e la generazione di rapporti di gestione, offrendo agli operatori e ai responsabili la piena visibilità e i rapporti sugli attacchi alle attività aziendali.

Rilevamento e Riduzione Attacco DDoS in Scala

SP Arbor Networks® scala le istanze fisiche e virtuali per fornire un rilevamento DDoS completo attraverso un'intera rete di fornitori di servizio, comprendente il cliente e il peering edge, il data center (o il cloud) edge, nonché il mobile e la dorsale centrale. Con questa visibilità senza pari, il flusso SP abilita una veloce ed efficace riduzione di qualsiasi attacco DDoS tramite qualsiasi Protezione TMS o Cisco ASR 9000 vDDoS. Le contromisure basate sulla riduzione bilanciano fino a 100 Gbps per TMS 5000 e fino a 4 Tbps in una distribuzione. La blacklist sblocca un altro livello di protezione superiore a qualsiasi altra contromisura di riduzione. La Protezione Cisco ASR 9000 vDDoS usa OpenFlow per inserire nella blacklist un grande quantitativo fino a decine di Tbps di protezione a ogni angolo della tua rete e inoltre salvaguarda la controcorrente critica e i link principali dagli attacchi.

Gestione e Report Completi

TMS semplifica e snellisce le operazioni offrendo la possibilità di visualizzare e gestire fino a otto terabit di capacità di mitigazione da un singolo punto di controllo. Questo consente di debellare più attacchi su grande scala e generare rapporti completi che riepilogano il processo di mitigazione per i clienti e/o la direzione.

Piattaforma per servizi DDoS gestiti

La soluzione Arbor Networks consente ai fornitori di servizi e ai fornitori di servizi di hosting/cloud di offrire servizi di protezione DDoS ai suoi clienti. L'accesso personalizzato al portale, le API e la gestione delegata offrono ai fornitori di servizi gestiti la flessibilità e il controllo per personalizzare i servizi secondo le necessità dei clienti. La soluzione Arbor Networks è il leader indiscusso nella protezione gestita da DDoS. ed è la soluzione preferita per la vasta maggioranza di servizi gestiti per DDoS.

Specifiche di Difesa DDoS TMS

Sessioni simultanee	Nessuna limitazione delle sessioni
Modalità di distribuzione	Inline attiva; monitoraggio inline, porta SPAN, diversione/rifiuto
Azioni di blocco	Blocco origine/sospensione origine, blocco per pacchetto, combinazione dell'origine, blocco basato su intestazione e percentuale
Protezione dagli attacchi	Attacchi al Flusso (TCP, UDP, ICMP, DNS, SSDP, NTP, SNMP, SQL RS, Amplificazione Caricata, Amplificazione DNS, Microsoft SQL Risoluzione Amplificazione Servizio, Amplificazione NTP, SNMP Amplification, Amplificazione SSDP) Attacchi alla Frammentazione (Teardrop, Targa3, Jolt2, Nestea), Pila di Attacchi TCP (SYN, FIN, RST, SYN ACK, URG-PSH, Bandiere TCP), Attacchi all'Applicazione (Flussi HTTP GET, Flussi di Invito SIP, tAttacchi DNS, attacchi di protocollo HTTPS), Posizionamento Cache DNS, Attacchi alla Vulnerabilità, Attacchi Esaurimento Scorte (Slowloris, Pyloris, LOIC, etc.). Protezione da flash crowd. IPv4 and IPv6 attacchi nascosti nei pacchetti criptati SSL
Contromisure DDoS	Elenco di esclusione/inclusione, generazione di rapporti e blocco in base alla posizione geografica dell'IP, blocco di zombie, filtraggio del contenuto dei pacchetti, filtraggio delle intestazioni dei pacchetti, rimozione delle botnet (feed AIF), rimozione dei pacchetti non corretti (TCP, UDP, DNS, DNSSEC, HTTP, HTTPS, SIP), diverse contromisure anti-spoofing, protezione da attacchi combinati, contromisure predisposte per CDN/ proxy, limitazione della velocità

Decimo *Worldwide Infrastructure Security Report*

Il decimo *Worldwide Infrastructure Security Report* di Arbor Network copre un periodo di 12 mesi, dal novembre 2013 all'ottobre 2014. Per il report, Arbor ha raccolto 287 interviste attraverso un mix di fornitori di servizio, hosting, mobile, imprese e altri tipi di operatori di rete in giro per il mondo di livello 1 e livello 2/3. Il rapporto è stato creato per raccogliere le esperienze, le osservazioni e le preoccupazioni della community responsabile per la protezione delle attività. Come negli anni precedenti, il sondaggio parlava di argomenti come le minacce contro i clienti e l'infrastruttura, tecniche impiegate per proteggere l'infrastruttura e i meccanismi per gestire, rilevare e rispondere agli incidenti della sicurezza.

Dieci anni di Report DDoS:

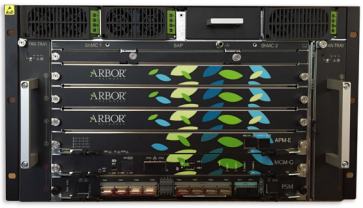
- Più che altro una seccatura e niente più di un evento indipendente un decennio fa, la mancanza di servizio distribuita (DDoS) è ora una vera e propria minaccia alla continuità dell'azienda e alla linea base. Gli attacchi DDoS oggi sono componenti di una campagna minacce complessa e avanzata spesso a lungo termine.

- Gli attacchi a livello applicativo si verificarono per il 90% nel 2014. 10 anni dopo, il 90% delle risposte "forzate" agli attacchi al flusso come la maggior parte dei vettori di attacco.

- L'elemento umano continua a essere un fattore nelle capacità di difesa—non solo oggi, ma anche negli ultimi dieci anni di report WISR. Solo nell'anno passato, il 54% degli intervistati ha riscontrato difficoltà nell'acquisire e conservare conoscenze personali nella sicurezza aziendale.

- Il più grande attacco DDoS nel 2014 era di 400 Gbps; dieci anni fa il più grande attacco era di 8 Gbps.

Per scaricare il rapporto più recente, accedere all'indirizzo: **www.arbornetworks.com/report**



TMS 5000
25 Gbps, 10 Mpps - 100 Gbps, 40 Mpps

TMS 2x00
2301: 1,5 Gbps, 3,5 Mpps
2302: 2,5 Gbps, 5 Mpps
2305: 5 Gbps, 7 Mpps
2310: 10 Gbps, 10 Mpps
2800: 10–40 Gbps, 30 Mpps

Espandi facilmente un applicativo TMS 2x00 al posto di un aggiornamento chiave della licenza software.

ARBOR NETWORKS
The Security Division of NETSCOUT

Sedi Centrali

Blanchard Road 76
Burlington, MA 01803 Stati Uniti

Numero Verde Stati Uniti
+1 866 212 7267
Tel. +1 781 362 4300

Vendite Nord America

Numero verde +1 855 773 9200

Europa

Tel. +44 207 127 8147

Asia Pacifica

Tel. +65 68096226

www.arbornetworks.com

DS/TMS/EN/0715-LETTER

Specifiche TMS 2300, 2800, 5000

	Serie TMS 2300	TMS 2800	TMS 5000
Throughput e Riduzione *Le serie 2300 & 2800 sono software con licenze aggiornabili*	**2301:** 1,5 Gbps, 3,5 Mpps **2302:** 2,5 Gbps, 5 Mpps **2305:** 5 Gbps, 7 Mpps **2310:** 10 Gbps, 10 Mpps	Licenze per 10 Mbps, 20 Gbps, 30 Gbps, 40 Gbps; tutte fino a 30 Mpps	**1 x APMe:** Fino a 25 Gbps, 10 Mpps **2 x APMe:** Fino a 50 Gbps, 20 Mpps **3 x APMe:** Fino a 75 Gbps, 30 Mpps **4 x APMe:** Fino a 100 Gbps, 40 Mpps
Requisiti di Alimentazione	Scorte Alimentatori Duali Ridondanti **AC:** 100-127V/200-240V, 50 a 60 Hz, 6/3A **DC:** da -48 a -72 V, 13 A max	Scorte Alimentatori Ridondanti **AC:** 100-127 VAC, 200-240 VAC, 12A @ 100 VAC, 6A @ 200 VAC, 50/ 60 Hz **DC:** da -48 a -72Vdc, 30A @ -48Vdc	Scorte Energia Quadrupla Ridondante **AC:** 100-240V, da 50 a 60Hz **DC:** da 40,5 a 72 VDC
Dimensioni	**Chassis:** 2U rack altezza **Peso:** 39 lbs (17,7 kg) **Altezza:** 3,45 in (8,76 cm) **Larghezza:** 17,14 in (43,53 cm) **Profondità:** 20 in (50,8 cm)	**Chassis:** 2U rack altezza **Peso:** 39 lbs (17,7 kg) **Altezza:** 3,45 in (8,76 cm) **Larghezza:** 17,14 in (43,53 cm) **Profondità:** 20 in (50,8 cm)	**Chassis:** 6U rack altezza **Peso:** Con AC: 77,15 lb (34,99 kg), Con DC: 58,52 lb (26,54 kg); Aggiungi 6 lb (2,72 kg) per APM-E lama **Altezza:** 10,463 in (265,76 mm) **Larghezza:** 19,00 in (482,6 mm) **Profondità:** 18,19 in (462,00 mm) with manici
Interfaccia di rete	12 x 1 GigE (SFP per rame, GigE SX, o GigE LX) or 6 x 10 GigE (SFP+ for SR o LR)	8 x 10 GigE (SFP+ per SR o LR or fibra mista)	32 x 10 GigE (QSFP+ con cavi di fuga, SR4 o 4LR) *Pianificato per il 2016:* 8 x 40 GigE (QSFP+ SR4 o LR4) 4 x 100 GigE (QSFP28 SR4 o LR4)
Magazzino	Disco Duale RAID 1 SSD	Disco Duale RAID 1, 240 GB	Hard Disk Duale RAID 1
Ambientale	**Temperatura operativa:** da 41° a 104°F (da 5° a 40°C) **Umidità relativa:** (operativo) da 5 a 85%, (non operativo) 95% a 73° a 104°F (da 23° a 40°C)	**Temperatura operativa:** da 41° a 131°F (da 5° a 55°C) **Umidità relativa:** (in servizio): da 5 a 85%, (non operativa) 95% a 73° a 140F C (da 23° a 40°C)	**Temperatura operativa:** da 23° F a 104° F (da -5° C a 40° C) **Umidità relativa:** (in servizio): dal 5% al 85%, senza condensa
Normative	RoHS 2002/95/EC, IEC/EN/UL 60950-1 2nd ed., E2006/95/EC, 2001/95/EC, FCC Parte 15 Sottoparte B Classe A, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, IC ICES-003 Classe A, ETSI EN 300 386, ETS 300-019-2-1, ETS 300-019-2-2, ETS 300-019-2-3, ETS 753, CISPR 22 Classe A, CISPR 24, Gost, BSMI, VCCI Classe A, KCC Classe A, UL Mark, CE Mark, ETSI, NEBS-3 (DC), NEBS-1 (AC)	UL 60950-1 2nd edizione/ CSA C22,2 No. 60950-1-07 2nd Edizione, Direttiva Basso Voltaggio 2006/95/EC, Direttiva di Sicurezza 2001/95/EC, CB Report e Certificato a IEC60950-1, 2a edizione e tutte le deviazioni interne, FCC 47CFR Parti 15, limite Classe A Verificato, Limite ICES-003 Class A, Direttiva EMC, 2004/108/EC, EN55022, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11,EN61000-3-2, EN61000-3-3, VCCI Classe A ITE(CISPR 22, Limite Class A), Approvazione BSMI, CNS 13438, Classe A e Sicurezza CNS13436, Approvazione KCC, Approvazione Gost, Limite CISPR 22 Classe A, Immunità CISPR 24, RoHS (recast) Direttiva 2011/65/EU	RoHS 6/6, IEC/EN/UL 60950-1, FCC Parte 15 Sottoparte B Classe A, ETSI EN 300 386, UL Mark, CE Mark
Deviazione hardware	Esterna		
Opzioni Descrizione/ Re-criptaggio SSL *Tramite Modulo di Sicurezza Hardware opzionale (HSM)*	**2301 & 2302:** 750 Mbps **2305 & 2310:** 5 Gbps **Connessioni HTTPS:** Fino a 45.000 **Sessioni Simultanee:** Fino a 150.000	**Throughput Ispezionato:** Fino a 5 Gbps **Connessioni HTTPS:** Fino a 45.000 **Sessioni Simultanee:** Fino a 150.000	Non Supportato
	SSL Supportato: SSL 3,0,TLS 1,0,TLS 1,1, TLS 1,2 **Suite codice FIPS supportato:** RSA_WITH_AES_128_SHA, RSA_WITH_AES_256_SHA, RSA_WITH_AES_256_SHA256, SSL3_CK_RSA_DES_192_CBC3_SHA **Suite codice non-FIPS supportato:** SSL3_CK_RSA_RC4_128_SHA, SSL3_CK_RSA_RC4_128_MD5, SSL3_CK_RSA_DES_64_CBC_SHA		