Protezione dei Dispositivi Stateful

Gli attacchi DDoS stanno crescendo a dismisura tanto che, per la prima volta nella storia, è stata superata la soglia dei 10 milioni di attacchi DDoS in un anno. Nello specifico, l'ATLAS Security Engineering and Response Team (ASERT) di NETSCOUT ha registrato 10.089.687 attacchi nell'ultimo anno. Inoltre, il lockdown imposto dalla pandemia ha prodotto i suoi effetti durante la scorsa primavera quando, solo nel mese di maggio, i cyber criminali hanno lanciato 929.000 attacchi DDoS, il più alto numero di attacchi mensili registrato finora. Gli attacchi avevano come obiettivo l'infrastruttura stateful utilizzata per lavorare e studiare da casa, con particolare riferimento ai firewall e ai concentratori di Virtual Private Network (VPN).

Sfida

Gli aggressori non stanno aumentando solo la frequenza, ma anche la complessità dei loro attacchi. Dall'ultimo Rapporto Annuale sulla Sicurezza delle Infrastrutture Mondiali (WISR) è emerso che il 58% delle aziende coinvolte sta registrando un aumento degli attacchi multivettoriali pari al 38% rispetto allo scorso anno. Nella seconda metà del 2020 è stato registrato un attacco con 26 vettori di attacco. Un numero record. Questi attacchi complessi sono un mix dinamico di attacchi di frammentazione, volumetrici e applicativi. Un aggressore lancia vari tipi di attacchi contemporaneamente o alternativamente, rendendo più complesse le operazioni di difesa.

L'incremento delle alternative di accesso alle reti da parte di utenti e altri dispositivi in concomitanza con la diffusione del lavoro da casa imposto dalla pandemia è da considerarsi un fattore determinante nell'interruzione della continuità operativa. I cyber criminali sanno che le società sono maggiormente esposte quando i loro dipendenti lavorano da remoto ed è proprio questo che li spinge a lanciare attacchi mirati con l'intento di mandare in crash i server e sovraccaricare i sistemi di qualsiasi dimensione. Tra i bersagli più comuni di questi criminali ci sono i dispositivi stateful come i firewall e i dispositivi VPN. Non a caso, secondo il Rapporto Annuale sulla Sicurezza delle Infrastrutture Mondiali (WISR), l'83% delle aziende coinvolte, il 21% in più rispetto al 2019, ha registrato degli attacchi DDoS nei quali i firewall e/o i dispositivi VPN sovraccaricati hanno contribuito a un'interruzione.

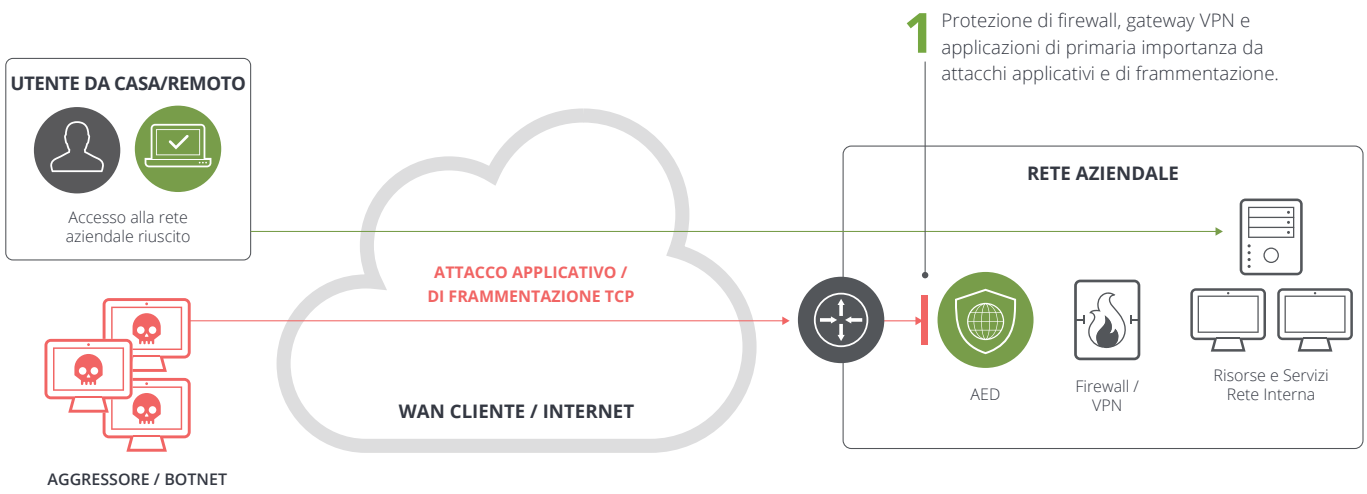
Minaccia

I firewall, i VPN e gli altri prodotti per la sicurezza sono elementi essenziali di una strategia difensiva basata su livelli, ma sono progettati per risolvere problemi di sicurezza fondamentalmente diversi rispetto ai prodotti specifici per la rilevazione e la mitigazione degli attacchi DDoS. Il problema sta nel fatto che i firewall e i VPN sono dispositivi stateful. Essere stateful significa usare tabelle per raccogliere i dettagli relativi alla connessione come gli indirizzi IP, le porte e le marche temporali. La memoria di queste tabelle è limitata e perfino i dispositivi ad alte prestazioni in grado di gestire milioni di connessioni sono vulnerabili di fronte ad attacchi di tipo flood progettati per sovraccaricare questi sistemi. In altre parole, sono vulnerabili agli attacchi DDoS e spesso diventano essi stessi i bersagli. Dal momento che gli stessi dispositivi stateful sono bersagli o bersagli parziali di attacchi a più livelli, anch'essi necessitano di protezione. Perfino un attacco a basso volume può esaurire le risorse dei concentratori di VPN e dei firewall. Anche attacchi con un volume di pochi Mbps possono portare i firewall di rete a un punto tale da non riuscire a gestire nuove connessioni.

Per una protezione adeguata contro gli attacchi DDoS, è necessaria una soluzione in grado di proteggere i dispositivi stateful da qualsiasi tipo di attacco.

Rischio

La disponibilità dei servizi di primaria importanza per l'azienda è essenziale. E non solo per evitare la perdita di entrate. La disponibilità dei servizi, infatti, rafforza anche la reputazione della società in un mercato e contribuisce al successo aziendale sostenibile. La cyber resilienza fa riferimento alla capacità di un'entità di raggiungere costantemente gli obiettivi prefissati indipendentemente dai cyber eventi avversi. I cyber eventi avversi sono quegli eventi che influenzano negativamente la disponibilità dei sistemi IT in rete, ma anche delle informazioni e dei servizi associati.



VPN

In passato, i VPN non venivano usati regolarmente, ma durante la pandemia di COVID-19 sono diventati la colonna portante del business. Ciò significa che le aziende stanno andando ben oltre le capacità standard e mettono a dura prova l'accesso alle loro applicazioni e risorse critiche. Ora più che mai, un attacco DDoS di entità relativamente ridotta potrebbe far crollare un gateway VPN impedendo agli utenti che lavorano in remoto da casa di svolgere regolarmente le loro attività. Man mano che i lockdown imposti dalla pandemia vengono revocati e la società torna alla normalità, molte organizzazioni continueranno a offrire almeno un ambiente ibrido e di lavoro da casa, con conseguente necessità di proteggere il gateway VPN.

Firewall

I firewall applicano quanto previsto dalla policy impedendo l'accesso non autorizzato ai dati. Questi prodotti di sicurezza si occupano di «integrità e confidenzialità della rete» tralasciando un aspetto altrettanto importante degli attacchi DDoS, cioè la «disponibilità della rete». Il firewall di prossima generazione (NGFW) è una soluzione di cyber security utile per proteggere la rete con funzionalità aggiuntive rispetto ai firewall tradizionali. Mentre i firewall tradizionali rilevano un traffico sospetto e bloccano l'accesso alla rete sulla base di una blacklist predefinita, i firewall NGFW sono dotati di funzionalità aggiuntive come la prevenzione anti-intrusione e l'ispezione approfondita dei pacchetti. Detto questo, perfino i firewall NGFW non garantiscono una protezione completa e anch'essi sono oggetto di attacchi.

Mitigazione

L'Arbor Edge Defense® (AED) è una soluzione di mitigazione on premise, sempre attiva, stateless e specifica per DDoS. AED è in grado di identificare e mitigare gli attacchi fino a 40 Gbps e grazie alla sua struttura stateless non è suscettibile ad attacchi di frammentazione che colpiscono dispositivi stateful come i gateway VPN, i firewall o gli equilibratori di carico. AED è progettato per stare ai margini della rete, tra Internet e i dispositivi di rete stateful, con lo scopo di proteggere questi ultimi dai numerosi attacchi architettati per minarne la funzionalità. Nel caso di un imponente attacco volumetrico progettato per saturare il circuito di Internet, la funzione cloud signaling di AED indirizza il traffico automaticamente verso una protezione dagli attacchi DDoS basata sul cloud come Arbor Cloud® di NETSCOUT® o quella del tuo ISP.

In generale, AED è in grado di neutralizzare la minaccia DDoS e il pericolo per tutti i dispositivi stateful, aiutando così la tua organizzazione nell'impegno costante a mantenere la disponibilità di applicazioni e servizi di primaria importanza.

Sintesi

Gli attacchi DDoS stanno aumentando in termini di frequenza e complessità se si considerano la quantità e la varietà dei vettori coinvolti in ogni attacco. Il numero maggiore di impiegati che lavorano da casa a causa della pandemia è un aspetto positivo per gli aggressori poiché hanno a loro disposizione una più ampia superficie di minaccia grazie ai dispositivi VPN e ai firewall. Non a caso, sebbene questi dispositivi siano parte integrante delle disposizioni di sicurezza e della strategia di protezione della rete, le interruzioni sono aumentate perché vengono presi di mira proprio questi dispositivi stateful. Se non lo ha già fatto, questo incremento di attacchi andrà a incidere negativamente sulla disponibilità dei servizi per i tuoi clienti o utenti finali, con inevitabili ripercussioni sui profitti. Il miglior modo per proteggersi dagli attacchi DDoS è adottare un approccio ibrido, affidandosi a una soluzione difensiva da attacchi DDoS basata sul cloud, on premise, integrata, stateless come AED, capace di proteggere i dispositivi stateful da altri attacchi.

NETSCOUT

Sede Centrale
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Telefono: +1 978-614-4000
www.netscout.com

Informazioni Commerciali
Gratis negli USA: 800-309-4804
(Numeri internazionali sotto)

Assistenza Prodotti
Gratis negli USA: 888-357-7667
(Numeri internazionali sotto)

NETSCOUT garantisce la vendita, l'assistenza e i servizi in oltre 32 Paesi. Gli indirizzi delle varie sedi nel mondo e i relativi numeri di telefono internazionali sono elencati nel sito web di NETSCOUT: www.netscout.com/company/contact-us

SECUC_015_IT-2102 10/2021