Application Delivery Controller

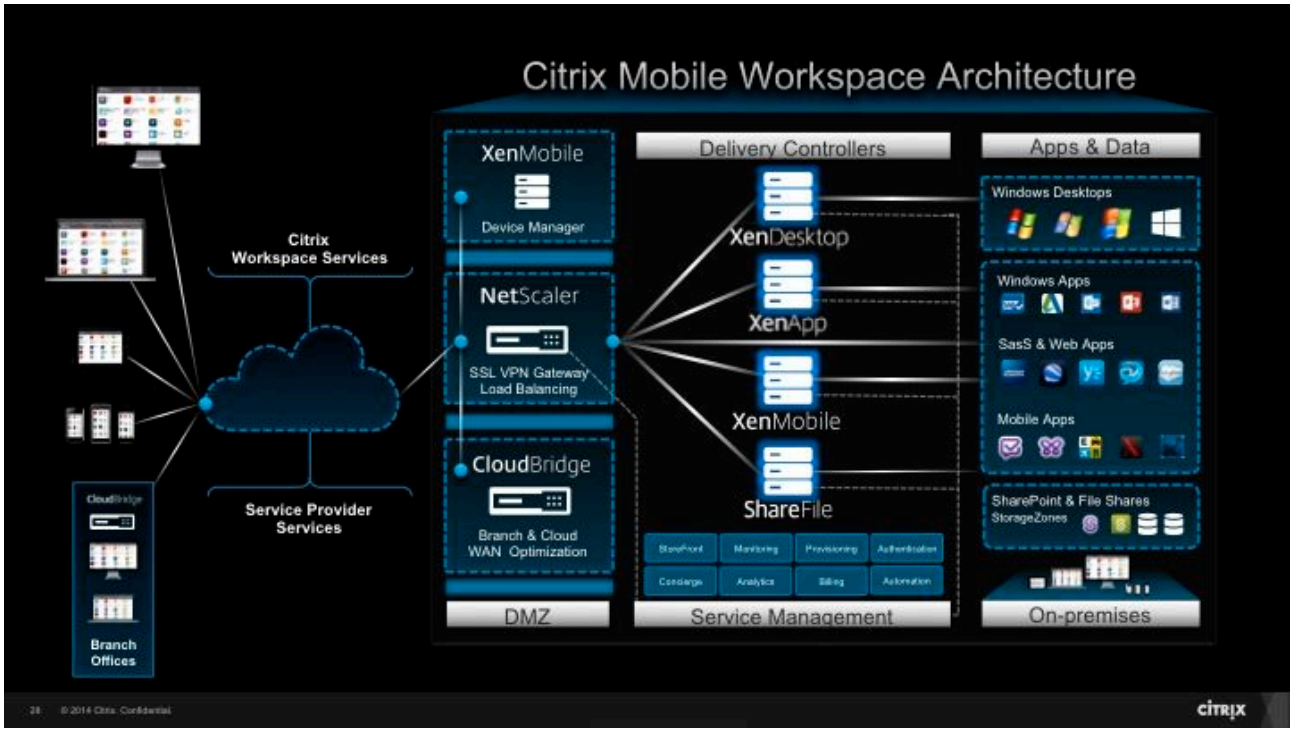
David Cenciotti
Systems Engineer, Cloud Networking Group
Citrix Systems

Gli Application Delivery Controller (ADC) svolgono un ruolo fondamentale nella protezione delle organizzazioni dai cyber attack e più specificatamente degli attacchi Denial of Service.

Oltre a garantire la distribuzione del traffico sui sistemi situati nel datacenter (o distribuiti su più siti), in base a logiche di prossimità, carico o stato della rete, gli ADC ottimizzano le performance dei server e delle applicazioni di Back End (ovvero di quell'area di un'applicazione non visibile direttamente agli utenti poiché preposta alla generazione e alla modifica dei contenuti, anche mediante accesso ai database) dei quali verificano continuamente lo "stato di salute". Ma non solo.
Gli ADC di nuova generazione hanno piena visibilità (fino al livello 7 della pila ISO/OSI) del traffico e del relativo contesto applicativo, e dispongono dell'intelligenza e delle capacità necessarie per identificare e mitigare gli attacchi, discriminando tra utenti legittimi e attaccanti.

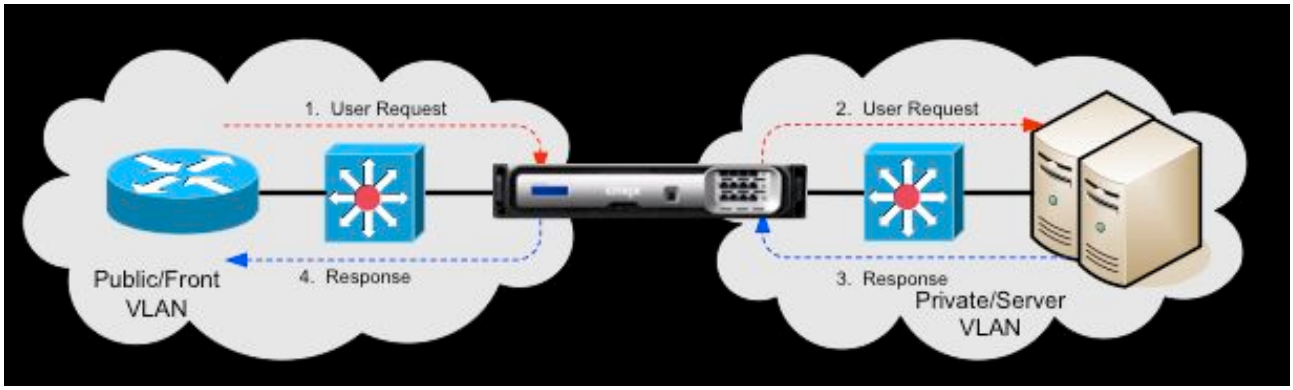
Gli Application Delivery Controller sono dei sistemi, fisici, virtualizzati o piattaforme "multi-tenant" (cioè appliance fisiche sulle quali è possibile istanziare diverse macchine virtuali), che rappresentano l'evoluzione dei tradizionali Load Balancer (Bilanciatori di Carico). La loro funzione di base è quindi quella di prendere in carico il traffico destinato alle applicazioni situate nel Back End della rete e distribuirlo sui server di destinazione in base a criteri di carico, raggiungibilità, performance della rete o contenuto. In pratica, il loro compito primario è garantire la continuità di un servizio verificando che i sistemi informatici preposti ad erogarlo siano in grado di farlo. Qualora, per un qualsiasi motivo, il server o l'applicazione di Back End non soddisfino uno dei criteri previsti dall'amministratore, l'ADC provvederà a ridirigere le richieste dei client solo verso quei sistemi in grado servirle; un processo del tutto trasparente ai client, ma fondamentale per evitare anche le più brevi (ma costosissime) interruzioni di servizio.
Nel corso degli anni, in virtù della loro centralità nell'ambito della distribuzione del traffico, gli ADC hanno acquisito ulteriore "intelligenza" concentrando una moltitudine di ruoli e di funzioni, anche inerenti alla sicurezza, tra cui: Health Monitoring; SSL Offloading, Bridging e Proxying;

VPN SSL Concentrator, Caching (Integrated o per mezzo di redirection verso un cache engine esterno); GSLB (Global Server Load Balancing); Link Load Balancing; Content Switching; Content Filtering; WAF (Web Application Firewall); Surge Control; Denial of Service Protection; TCP Optimization (Multiplexing, SACK, MTU discovery, ecc.); L2 Extension. Inoltre, gli ADC svolgono l'importante ruolo di Front End per l'accesso a tutte le soluzioni di Application & Desktop Virtualization, Access and Data Security, Data Sharing ed Enterprise Mobility Management.



Come funziona un ADC

Finora si è parlato di ADC principalmente in termini di feature rese disponibili; tuttavia, conoscere i principi di funzionamento di questi sistemi è utile per comprenderne il vero valore aggiunto nel contrasto e nella mitigazione degli attacchi.
In una configurazione-tipo, a livello di architettura logica, un ADC risiede tra i client e i server da bilanciare, comportandosi da transparent proxy: i client terminano le sessioni sull'ADC che a sua volta che, a sua volta, instaurerà nuove sessioni verso i server di backend. In questa maniera, del tutto trasparente ai client - che crederanno di "parlare" direttamente con i server - viene spezzata la comunicazione tra quello che potremmo considerare l'"esterno" della rete e il "cuore" della stessa, dove sono presenti gli applicativi e i database: tutto il traffico passa per il bilanciatore, che una volta effettuate le verifiche previste, lo inoltrerà verso le reali destinazioni.

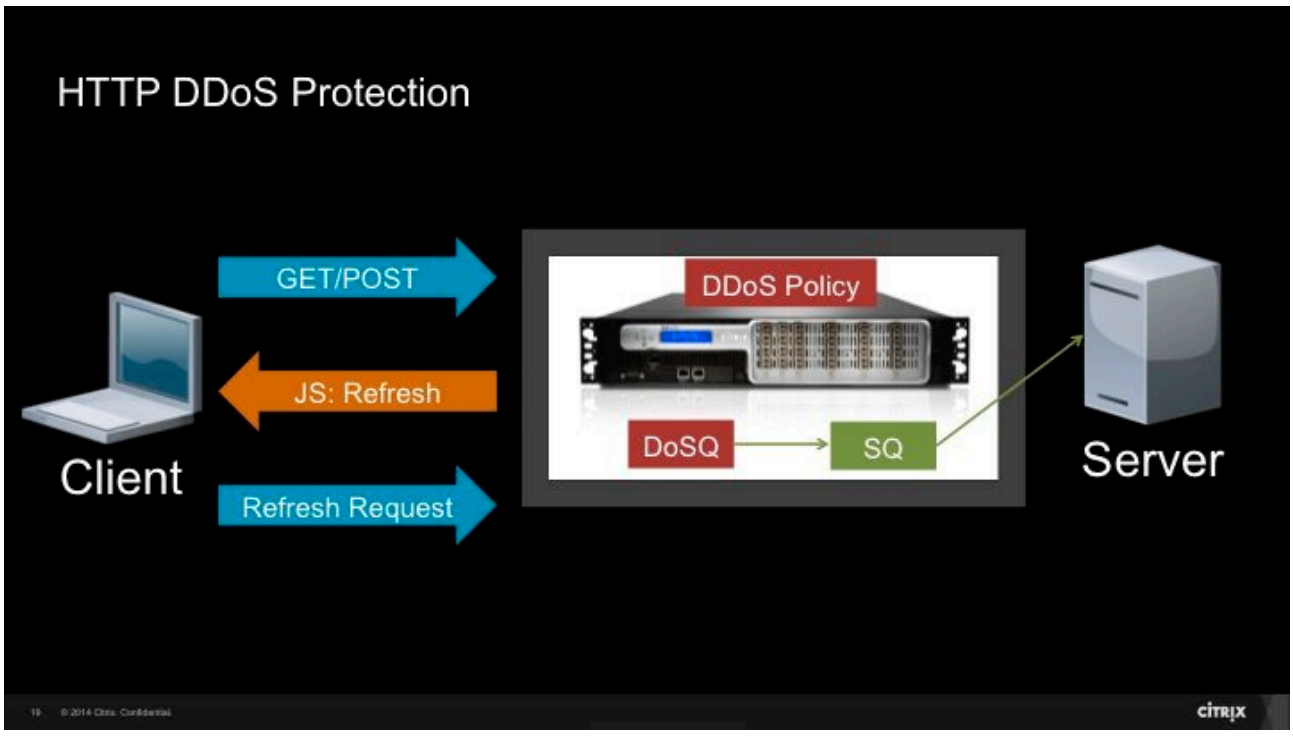


Come già accennato, per garantire agli utenti la fruizione del servizio senza soluzione di continuità, l'ADC monitorizza costantemente lo stato di salute del pool di sistemi di destinazione. Tale processo avviene mediante il monitoraggio dei servizi. Il Monitoring consiste nell'utilizzazione di tutta una serie di controlli (detti monitor o probe) per determinare se un sistema sia in grado di gestire il traffico e quindi debba essere mantenuto nel novero di quelli verso i quali l'ADC gira il traffico. I monitor più comuni sono il Ping, che verifica la raggiungibilità di rete del server mediante pacchetti ICMP, e il TCP, che prevede l'esecuzione della prima parte di un three-way handshake tra l'ADC e il server di Back End, terminato prima che la sessione TCP sia stabilita e che serve per "certificare" la capacità del sistema di accettare nuove sessioni. Ma ne esistono ovviamente anche di più complessi, come quelli che permettono di effettuare delle verifiche sul contenuto del codice HTML di una pagina Web, o quelli che attraverso trap SNMP verificano il carico CPU della macchina di destinazione per rilevare eventuali, rischiose, sofferenze. Generalmente, i vari monitor resi disponibili dall'ADC sono aperti a personalizzazioni anche piuttosto spinte, necessarie ad adattarli allo specifico comportamento di un'applicazione mentre, per le realtà applicative più complesse, è possibile combinare i monitor attribuendo agli stessi pesi differenti al fine di definire metriche di tipo "custom" su cui basare le decisioni di distribuzione del traffico. È addirittura possibile verificare l'health state di un sistema attraverso l'esecuzione di uno script lanciato dal bilanciatore.
E' proprio il processo di monitoring a conferire all'Application Delivery un ruolo fondamentale nell'ambito della sicurezza di un'infrastruttura informatica.

Il ruolo degli ADC in ambito Security

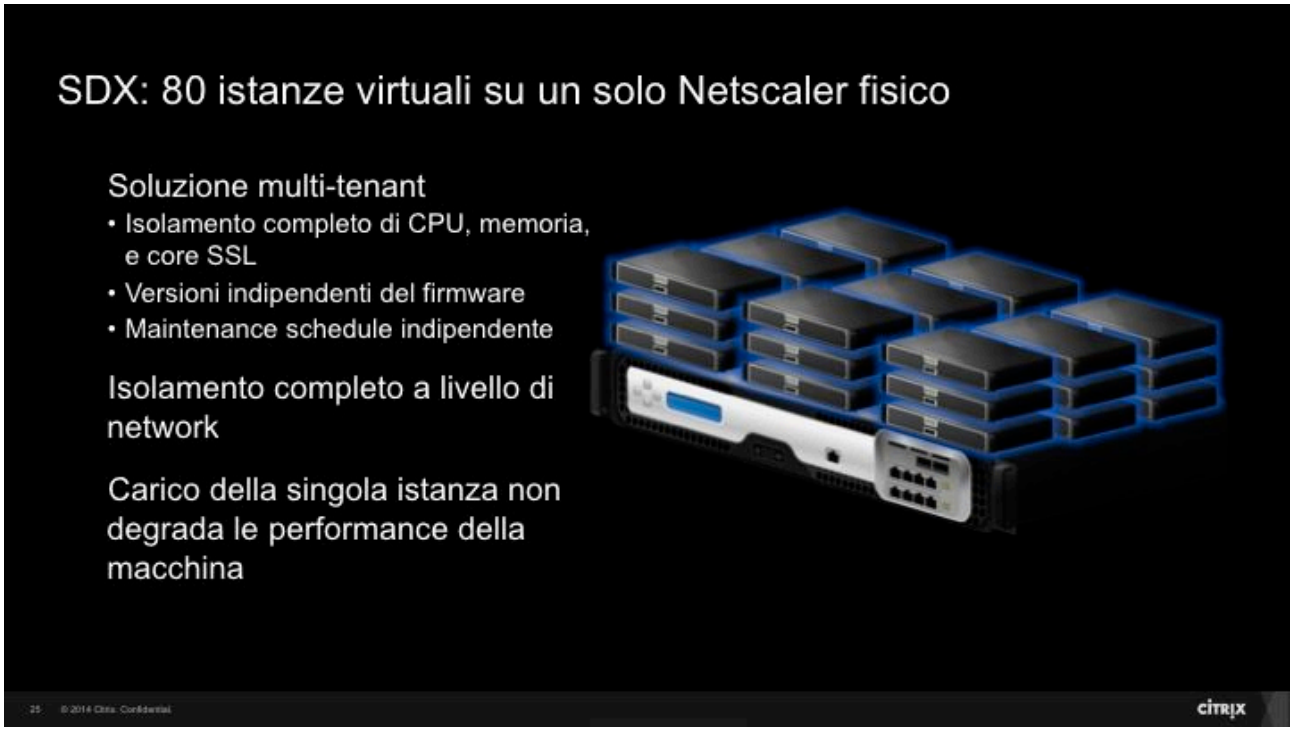
Sia ben chiaro, un bilanciatore non può sostituire strumenti di security dedicati. Tuttavia, in virtù delle proprie modalità operative, fornisce un considerevole valore aggiunto in caso di attacco cibernetico integrandosi con il resto dell'architettura di sicurezza. Difatti, l'ADC è l'unico "oggetto" all'interno della rete che interroga continuamente i server e le applicazioni di Back End, prendendo decisioni anche sulla base del risultato dell'health check eseguito sugli stessi. Firewall, IPS (Intrusion Prevention System) e altri sistemi normalmente preposti alla protezione da attacchi dall'esterno e dall'interno della rete, non verificano lo stato dei sistemi, ma normalmente si limitano a validare il traffico diretto agli stessi. L'ADC, oltre ad essere lo strumento con funzioni di sicurezza più "prossimo" al cuore della rete, agisce direttamente su traffico che gestisce sulla base delle politiche impostate, sull'esito dell'inspection e soprattutto sullo stato di salute dei server. Pertanto, oltre a poter mitigare attacchi dovuti al traffico malevolo degli attaccanti è in grado di proteggere i sistemi critici di un'organizzazione, anche da DoS in un certo senso involontari, ovvero causati da overload di traffico lecito. Senza dimenticare che il concetto di bilanciamento fu introdotto proprio per garantire la continuità del servizio a livello di server farm o distribuito su scala geografica (mediante GSLB), e rendere l'infrastruttura più resiliente ai fault o alle temporanee indisponibilità delle applicazioni (per attacchi o avarie).
Inoltre, tradizionalmente, in contesti che richiedono maggiore capacità elaborativa, gli ADC sono utilizzati proprio per bilanciare il carico verso batterie di Firewall poste a protezione delle isole applicative o dei CED, divenendo, di fatto, veri e propri "abilitatori" della stessa infrastruttura di sicurezza.
Il ruolo del bilanciatore nella protezione dei sistemi si è reso ancora più importante con l'introduzione di ulteriori feature di sicurezza come il WAF, l'HTTP DDoS Protection e il Surge Control corredati da vari strumenti di visibility e reporting.
Il Web Application Firewall è il firewall applicativo che filtra il traffico dei servizi Web, ovvero HTTP, HTTPS e XML. Alcuni ADC hanno a bordo un WAF che implementa un security model ibrido, ovvero basato su un motore di apprendimento delle caratteristiche dell'applicazione secondo

il “modello di sicurezza positivo”, per la protezione dagli “zero day”, ed un set di alcune migliaia di signature (“modello di sicurezza negativo”) per la protezione dagli attacchi noti. Per quel che concerne il motore di apprendimento, l’engine rileva automaticamente il comportamento lecito ed atteso per ciascuna applicazione o servizio al fine di proteggere le Web Application da diversi vettori di attacco quali: SQL Injection, Cross Site Scripting, CSRF (Cross Site Resource Forgery), Buffer Overflow, Cookie Tampering, Forceful Browsing, Web Form Security e, per quanto riguarda l'XML: XSS, SQL Injection, Malicious code or objects, Badly-formed XML requests, DoS.
Per quel che riguarda le signature, il WAF attinge alle firme degli attacchi (aggiornate in modalità automatica o manuale) del mondo Snort.
L’HTTP DDoS Protection è invece una funzionalità che si basa sull'invio di un javascript ai client che forza il refresh della pagina e il settaggio di uno specifico cookie, la cui presenza determina l’inoltro o meno verso i portali protetti. In pratica, raggiunta una determinata soglia di sessioni HTTP, l’ADC inizia a sondare i client in modo tale da verificare se il traffico verso i server è generato da utenti “umani”, ovvero browser che si presentano con il cookie corretto, o se si tratti di traffico registrato. Ovviamente, l’adozione di tecniche di DDoS mitigation non previene disservizi causati dalla saturazione dei link, nei confronti dei quali un ADC non sarebbe molto efficace. Tuttavia, abilitare questo tipo di controllo su un ADC consente di discriminare gli utenti leciti dai sistemi legati ad una botnet, per ridurre il carico sui sistemi di Back End e garantire la continuità del servizio per il tempo necessario ad adottare, lato carrier, ulteriori contromisure di contrasto. Sebbene possa sembrare poca cosa, scartare il traffico generato da bot e continuare ad erogare un servizio per qualche minuto in più potrebbe essere di vitale importanza per un’organizzazione (o per un intero paese) in caso di cyber attack. Ecco dunque spiegata la presenza di questo tipo di contromisura di sicurezza su un bilanciatore.



Un’altra funzionalità importante resa disponibile dai più avanzati ADC è il Surge Control. Attraverso la feature di Surge Protection, il bilanciatore permette di creare delle regole ad hoc per ritardare l'apertura delle nuove sessioni verso il Back End, in modo tale da consentire ai server di smaltire un po’ di traffico prima di prenderne in carico di nuovo. Questa tipologia di offloading (che si unisce all’offload dell’SSL, al caching e al multiplexing per alleggerire il carico sui server) è particolarmente utile in caso di DoS indotti da picchi di traffico (lecito) causati ad esempio dalla pubblicazione e successiva diffusione di un link ad un contenuto interno su social network o siti

d’informazione. Non essendo un attacco in senso stretto, il traffico generato dal contenuto “virale” passerebbe il controllo dei Firewall, facendo però collassare il Web Server preposto alla pubblicazione dello stesso. La presenza di un ADC con tale capacità permette di ovviare a questo problema, applicando un breve ritardo sull’apertura di nuove sessioni in base a tre modalità di gestione del sovraccarico di traffico: rilassato, moderato e aggressivo con ritardi incrementali.



Infine, non è da sottovalutare la possibilità di consolidare sull’ADC ulteriori funzionalità di sicurezza, attraverso l’integrazione di prodotti di terze parti ospitati come istanze virtuali di bilanciatori multi-tenant: si parla in questo caso di SDA, Software Defined Appliance, perfettamente integrabile in una moderna SDN (Software Defined Network).

Software Defined Network

Ai progressi in termini di capacità di calcolo e virtualizzazione si è a lungo opposta una certa rigidità della rete che rappresenta tuttora un ostacolo per la realizzazione di architetture di rete e cloud flessibili, scalabili e in grado di ottimizzare le performance delle applicazioni e la user experience degli utenti. I dispositivi di rete sono apparati fisici con capacità fisse, collegati secondo topologie statiche e con policy di accesso e sicurezza poco flessibili, e normalmente sono caratterizzati da una certa complessità di gestione: in altri termini, sono del tutto inadeguati ai moderni concetti di cloud-computing.
È questa la ragione per cui in ambito networking è stato sviluppato un nuovo paradigma architetturale che prende il nome di Software-Defined Network (SDN). In termini generici, l'SDN è una rete intelligente, in cui le applicazioni sono in grado di programmare gli apparati di rete per ottimizzare la distribuzione dei contenuti, grazie alla separazione sugli apparati stessi dei meccanismi di controllo dei flussi da quelli di instradamento del traffico (disaccoppiamento Control Plane e Data Plane). È indubbio che in virtù del ruolo centrale che rivestono nel delivery applicativo e della sicurezza, anche i moderni ADC debbano poter essere controllati e configurati da una SDN, in special modo se offrono servizi ad alto valore aggiunto come quelli brevemente descritti in questo articolo.