Vantaggi, e rischi di sicurezza, dal Networking "Software Defined"

È consuetudine consolidata che le organizzazioni scelgano di aumentare la capacità di banda della propria rete acquistando più hardware. Questo approccio, non sempre efficace,può trasformarsi in un costoso errore se le risorse di rete aggiuntive non vengono pienamente utilizzate. La tecnologia progredisce, ma la storia trova modo di ripetersi. Una prima trasformazione, avviata fino dai tempi dei protocolli di rete di mainframe, (come quelli della Systems Network Architecture), ha portato all'adozione generalizzata del protocollo di rete Transmission Control Protocol/Internet Protocol (IP). Questa transizione è stata contestuale all'introduzione del personal computer (PC), che utilizza una tecnologia di elaborazione di tipo client-server. Oggi si verifica una nuova transizione, rapida e dirompente, dall'uso dei PC a quello dei dispositivi mobili, come gli smartphone. Questa volta la chiave è l'introduzione dei modelli di virtualizzazione e di elaborazione in cloud e, a quanto pare, il futuro del networking si fonderà sempre di più sugli automatismi software. Viene da chiedersi come si evolveranno le reti e come una moderna infrastruttura di rete potrà rispondere alla dinamica dei requisiti imposti dagli utenti finali, dalle attività commerciali e dalle istituzioni governative.

La crescita del numero di dispositivi connessi e la loro dispersione a livello mondiale hanno aumentato la complessità e la difficoltà di gestire i dispositivi stessi e il relativo traffico di rete. I costi per riconfigurare a mano questi dispositivi e rispondere così ad ogni esigenza di modifica sono molto elevati. Inoltre è spesso difficile, se non quasi impossibile, riconfigurare tempestivamente una rete tradizionale per reagire a errori umani e/o a eventi dannosi. SDN (Software Defined Networking) gioca sulla virtualizzazione per accrescere notevolmente l'efficienza della rete e, di conseguenza, semplifica la gestione dell'insieme di queste risorse e permette soluzioni atte ad aumentare la capacità senza eccessivo impegno finanziario.[1]

Vantaggi del Software Defined Networking (SDN)

Cos'è SDN? La struttura SDN è un nuovo concetto che si discosta dal disegno tradizionale di rete. Utilizza controlli di natura software per semplificare l'attuazione delle policy tramite un controller centralizzato. Separa i dati e le funzioni di controllo dei dispositivi di rete, quali router e switch, sulla base di un ben definito protocollo API (Application Program Interface).[2]

L'architettura SDN si articola su tre strati logici separati: lo strato applicativo, quello di controllo e quello dei dati. Lo strato applicativo incorpora le applicazioni SDN, che comunicano i requisiti della rete al controller software SDN. A sua volta, il controller software SDN interpreta questi requisiti e attua i dettami della policy di rete dallo strato di controllo, che determina come i dati devono fluire dai dispositivi di rete. Il controller SDN è il centro nevralgico dell'architettura SDN, gestisce tutte le funzioni complesse e traduce i requisiti in regole specifiche di basso livello. Lo strato dati, infine, contiene i dispositivi di rete, ad esempio router e switch, che fanno fluire i dati dopo aver ricevuto l'autorizzazione dal controller SDN. In sostanza, SDN disaccoppia il controllo della rete dalle funzioni di inoltro, consentendo di programmare direttamente il protocollo di rete ai fini dei servizi applicativi e di rete, a prescindere dall'infrastruttura sottostante.[3]

Dal momento che SDN utilizza un controller centralizzato composto di applicazioni software, uno dei vantaggi maggiori dell'implementazione di SDN è la sua flessibilità. Poiché il controller SDN si assume le funzioni più complesse (ad es., esegue la gestione "intelligente" della rete e il monitoraggio in tempo reale del suo assetto), i dispositivi devono semplicemente accettare gli ordini dal controller SDN. Questo permette ai dispositivi di rete di

Tony Wang
È direttore delle pratiche di gestione dei rischi IT in Williams Adley. Vanta oltre 15 anni di esperienza nella valutazione dei controlli interni, dei sistemi informatici e dello sviluppo del software. Prima di entrare in Williams Adley, Wang ha ricoperto varie posizioni manageriali in BDO USA, Ernst & Young e Lockheed Martin, dove ha seguito clienti in vari settori, focalizzandosi in particolare sull'ambito governativo, sanità, produzione, tecnologico, servizi non-profit e finanziari. Le sue aree di specializzazione comprendono l'auditing dei processi di ingegnerizzazione, l'auditing finanziario integrato, l'assurance delle informazioni, l'auditing della sicurezza IT, la valutazione del ciclo di sviluppo del software e l'integrazione e la valutazione dei sistemi. Oltre alle responsabilità verso i clienti, Wang ha dedicato una quota significativa della sua attività di lavoro allo sviluppo del business, al reclutamento nei campus, alla consulenza e allo sviluppo e formazione di auditor IT.

Un controller centralizzato conferisce flessibilità, programmabilità in tempo reale e consente un elevato indice di redditività del capitale investito (ROI) semplificando simultaneamente il disegno della rete.

operare sul flusso dei dati senza tener conto delle specificità dei protocolli di comunicazione dei vari fornitori. Ne consegue che gli amministratori di rete fruiscono di una grande flessibilità per configurare, gestire, proteggere e ottimizzare i dispositivi di rete.[4]

Inoltre il controller SDN è il centro nevralgico dell'architettura SDN ed è molto più semplice modificare programmi o applicazioni software

> **“Nel momento in cui le società adottano la tecnologia cloud, SDN sarà in grado di semplificare il disegno globale della rete sfruttando la virtualizzazione per automatizzare le operazioni di gestione della rete.”**

anziché riconfigurare a mano ogni singolo dispositivo di rete. Per le aziende che vogliono adeguarsi all'incessante dinamica dei requisiti, si riduce pertanto la necessità di investire in nuovi,costosi dispositivi di rete. Quindi SDN rappresenta una soluzione molto efficiente in termini di costo. In effetti SDN è progettata per permettere di liberarsi dai vincoli imposti dagli approcci individuali dei fornitori (i fornitori hanno la propria console di gestione e i propri set di comandi) e consente alle aziende di promuovere l'innovazione e migliorare l'interoperabilità delle reti. Ne risulta un notevole aumento del ROI.

Le reti tradizionali vengono per lo più gestite utilizzando console di controllo con un'interfaccia a riga di comando che determina un forte impegno di manualità per gli amministratori di rete[5] Nel momento in cui le società adottano la tecnologia cloud, SDN sarà in grado di semplificare il disegno globale della rete sfruttando la virtualizzazione per automatizzare le operazioni di gestione della rete stessa.

Rischi di sicurezza per SDN

L'architettura SDN è esposta a molti dei problemi di sicurezza tipici dell'architettura tradizionale di rete. Le nuove funzionalità dell'SDN centralizzato, che conferiscono maggiore flessibilità, programmabilità in tempo reale e che semplificano i controlli, introducono purtroppo anche ulteriori minacce per la sicurezza. SDN è esposta a rischi di sicurezza di varia natura collegati al suo disegno architetturale complessivo, che si articola nei tre strati di controllo, applicazione e dati.

Uno dei fattori di rischio più significativi è la possibilità di attacchi al controller SDN nello strato di controllo. A motivo della struttura centrica dell'SDN, il controller SDN ne è anche il centro nevralgico. Per arrivare a manipolare l'intera rete, agli aggressori basta concentrare gli attacchi sul controller SDN.[6] Se un aggressore riesce a ottenere l'accesso, il controller SDN che è stato invaso può essere utilizzato per comandare i dispositivi di rete sotto il suo controllo (ad es., gli switch) in modo da mandare a vuoto tutto il traffico in entrata oda lanciare pericolosi attacchi contro altri obiettivi, ad esempio inviando traffico superfluo a un bersaglio per esaurirne le risorse.[7] Per limitare questo rischio, è essenziale rafforzare la sicurezza del sistema operativo che ospita il controller SDN e prevenire l'accesso non autorizzato al controller stesso. Inoltre lo strato di controllo è soggetto ad attacchi DDoS (Distributed Denial-of-Service). Gli switch SDN possono intasare il controller con un gran numero di query, causa potenziale di ritardi o di perdita delle query. Una difesa possibile dagli attacchi DDoS consiste nel prevedere più Controller

Se un aggressore riesce a inserirsi nel controller SDN, può interferire con le applicazioni SDN, e manipolare le applicazioni di sicurezza in modo da riprogrammare il flusso del traffico di rete attraverso il controller SDN.

fisici in parallelo, invece di solo uno. Quando gli switch sono collegati a più controller SDN, uno di essi può operare come master degli switch. Quando un controller master deve elaborare un carico di query elevato, può dirottare il carico su altri controller meno impegnati, che saranno il master per alcuni degli switch assegnati. Questo suddivide il carico tra i controller SDN, riducendo così l'effetto degli attacchi DDoS.

Relativamente allo strato dei dati, gli switch sono vulnerabili anche ad attacchi DoS (Denial-of-Service). Un utente ostile può intasare gli switch con carichi eccessivi, causando la perdita di pacchetti validi quando la capacità del buffer di uno switch viene superata. Vi sono molti modi per neutralizzare questi attacchi, tra cui caching proattivo delle regole, aggregazione delle regole e riduzione del ritardo di comunicazione tra switch e controller SDN. Anche l'aumento della capacità del buffer degli switch può ridurre il rischio di un attacco DoS.[8]

Lo scambio di messaggi tra strato di controllo e strato dei dati è esposto ad attacchi man-in-the-middle. L'aggressore potrebbe riuscire a modificare le regole inviate dal controller SDN agli switch, allo scopo di assumerne il controllo. Una delle contromosse più efficaci è la cifratura dei messaggi con l'uso di firme digitali, per proteggere l'integrità e verificare l'autenticità dei messaggi.

Nello strato applicativo, anche la programmabilità in tempo reale è soggetta a vulnerabilità significative. In particolare, se l'aggressore riesce a compromettere le applicazioni di sicurezza SDN, egli può anche manipolare il flusso del traffico attraverso il controller SDN. Se le applicazioni SDN vengono compromesse, lo è anche l'intera rete.[9] Per ridurre in modo significativo tale rischio di sicurezza, è essenziale che prassi di codifica sicura siano introdotte e rese vincolanti, con procedimenti estesi di controllo modifiche e di verifica dell'integrità, inglobati nel ciclo di sviluppo del software.

Conclusioni

La virtualizzazione dei server, le unità mobili e il cloud computing stanno diventando la nuova via per rispondere alla dinamica dei requisiti di servizio. Con l'evoluzione di queste tecnologie, l'architettura di rete tradizionale inizia a mostrarsi insufficiente a soddisfare la crescita delle esigenze. L'architettura SDN virtualizza le reti e le trasforma in piattaforme flessibili e programmabili. Il futuro del networking si affiderà sempre più al software ed SDN ne diverrà a sua volta la nuova norma.
D'altra parte, la sicurezza nell'uso pratico dell'SDN richiede che i rischi critici di sicurezza del controller e delle applicazioni SDN siano prima posti adeguatamente sotto controllo.

Note finali

1 Underdahl, B.; G. Kinghorn; *Software Defined Networking for Dummies*, John Wiley & Sons, USA, 2015
2 Stallings, W.; "Software-Defined Networks and OpenFlow," *The Internet Protocol Journal*, vol. 16, no. 1, Marzo 2013, p. 2-14
3 Open Networking Foundation, *https://www.opennetworking.org/sdn-resources/sdn-definition*
4 Open Networking Foundation, *Software-Defined Networking: The New Norm for Networks*, 13 aprile 2012, *https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf*
5 Kim, H.; N. Feamster; "Improving Network Management With Software Defined Networking," *IEEE Communications Magazine*, vol. 51, iss. 2, Febbraio 2013, p. 114-119
6 Open Networking Foundation, *Principles and Practices for Securing Software-Defined Networks*, Gennaio 2015, *https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf*
7 Mehiar, D.; B. Hamdaoui; M. Guizani; A. Rayes; "Software-defined Networking Security: Pros and Cons," *IEEE Communications Magazine*, vol. 53, iss. 6, Giugno 2015
8 Dabbagh, M.; B. Haimdaoui; M. Guizani; A. Rayes; "Software-Defined Networking Security: Pros and Cons," *IEEE Communications Magazine*, vol. 53, iss. 6, Maggio 2015
9 Lim, A.; "Security Risks in SDN and Other New Software Issues," RSA Conference 2015, Luglio 2015