VMware NSX

L'IT al passo con il business

"La tecnologia continua ad accelerare a un ritmo incredibile, promettendo grandi vantaggi alle organizzazioni che mostrano spirito d'iniziativa."

Bart Van Ark, Ph.D.
Executive Vice President,
Chief Economist e Strategy Officer
The Conference Board

VMware NSX® è la piattaforma di sicurezza e virtualizzazione della rete che consente l'adozione di VMware Cloud Networking Solutions con un approccio Software-Defined al networking che si estende a data center, cloud e framework delle applicazioni. Con NSX, networking e sicurezza si avvicinano all'applicazione, indipendentemente da dove viene eseguita, ovvero macchine virtuali (VM), container o server fisici. Analogamente al modello operativo delle VM, il provisioning e la gestione delle reti sono indipendenti dall'hardware sottostante. NSX riproduce l'intero modello della rete nel software, consentendo di creare e distribuire in pochi secondi qualsiasi topologia di rete, da quella più semplice alle più complesse reti multi-tier. Gli utenti possono creare molteplici reti virtuali con requisiti diversi e sfruttare una combinazione di servizi offerti tramite NSX o da un ampio ecosistema di integrazioni di terze parti, che vanno dai firewall di nuova generazione alle soluzioni di gestione delle prestazioni, per creare ambienti intrinsecamente più agili e sicuri. Questi servizi possono poi essere estesi a una varietà di endpoint all'interno di uno stesso cloud e tra cloud diversi.

Requisiti contrastanti implicano compromessi

La velocità e l'agilità, una solida sicurezza e l'alta disponibilità delle applicazioni sono tutte priorità estremamente importanti da perseguire per le organizzazioni IT. Le organizzazioni dipendono così tanto da un'infrastruttura delle applicazioni solida che l'IT è sempre più quella base che consente loro di innovare e avere successo nel percorso di digital transformation. Tuttavia, l'elevata velocità del cambiamento e le mutevoli aspettative nell'IT causano un cambiamento costante delle priorità che non di rado compromette l'efficacia della distribuzione.

L'IT è consapevole e risente dei frequenti attriti causati dall'assecondare diverse parti interessate per rispondere a queste richieste e molte volte è costretto a dare la precedenza a una priorità IT piuttosto che a un'altra. Ad esempio, date le rigide complessità associate alla sicurezza, spesso la protezione di un'applicazione ne compromette la velocità di deployment. Compromessi simili riguardano spesso anche la disponibilità delle applicazioni negli ambienti, ponendo effettivamente l'IT in contrasto con l'organizzazione nel suo complesso e viceversa.

Il risultato finale di questi compromessi e attriti costanti ha enormi conseguenze per l'IT, poiché provoca gravi lacune in diverse aree di responsabilità: le organizzazioni non riescono a rispondere velocemente alle richieste, ci sono vulnerabilità negli ambienti cloud/data center e manca agilità complessiva.

Vantaggi principali

- Sicurezza granulare: previene la diffusione laterale delle minacce nell'ambiente con una policy di sicurezza microsegmentata a livello di carico di lavoro
- Velocità e agilità: riduce il tempo di provisioning della rete da giorni a secondi e migliora l'efficienza operativa attraverso l'automazione
- Policy e operation coerenti: gestisce in modo coerente le policy di networking e sicurezza indipendentemente dalla topologia di rete fisica tra data center, public cloud e private cloud e framework delle applicazioni

Sfruttare il pieno potenziale dell'infrastruttura

La maggior parte delle organizzazioni ha già componenti di elaborazione virtualizzati nei propri data center. Inoltre, molte organizzazioni hanno anche deciso di virtualizzare lo storage e oltre il 70% di queste ha già adottato o prevede di adottare il Software-Defined Storage.

Questa astrazione della funzionalità dall'hardware al software permette alle organizzazioni il rapido provisioning dei componenti applicativi, lo spostamento dei sistemi virtuali all'interno di un data center e tra data center diversi e l'automazione dei processi critici. Senza la virtualizzazione di switching, routing, bilanciamento del carico e firewall, il pieno valore del Software-Defined Data Center rimarrebbe inespresso.

Le organizzazioni che possiedono architetture di rete radicate nell'hardware non possono competere con la velocità, l'agilità e la sicurezza delle aziende che utilizzano reti virtualizzate. Lo stato dell'organizzazione è quindi vincolato a quello della rete.

È necessario adottare un approccio completamente nuovo al networking del data center, evitando di dover continuare a scegliere tra velocità e sicurezza o tra sicurezza e agilità. Le regole del data center che hanno impedito alle organizzazioni di sfruttare tutte le loro potenzialità devono essere riscritte per garantire all'IT la possibilità di operare in completa libertà, senza dover scendere a compromessi. Come ormai compreso da migliaia di organizzazioni, questo nuovo approccio si realizza con la virtualizzazione della rete.

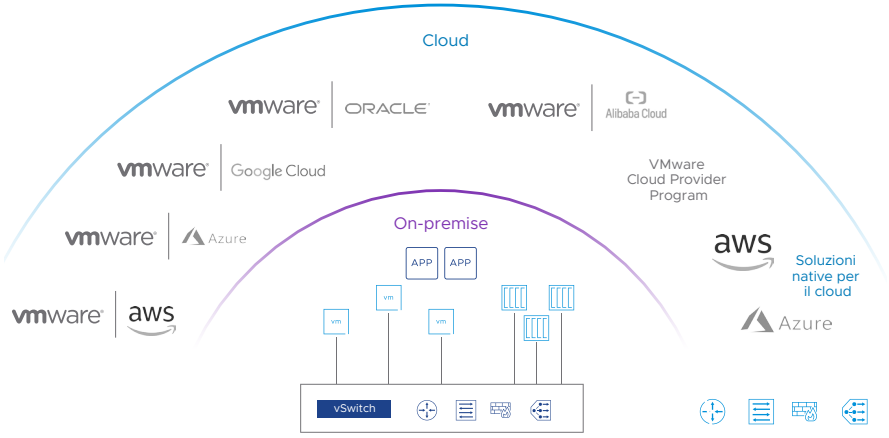

Figura 1. Networking e sicurezza coerenti con NSX.

Spostando i servizi di rete e sicurezza nel layer di virtualizzazione del data center, la virtualizzazione della rete permette all'IT di creare interi ambienti per applicazioni, eseguirne la snapshot, archiviarli, spostarli, eliminarli e ripristinarli con la stessa semplicità e velocità con cui ora è possibile attivare le macchine virtuali. NSX estende le comuni policy di networking e sicurezza in framework applicativi e ambienti eterogenei, consentendo di ottenere questi vantaggi tra data center, private cloud e public cloud, applicazioni tradizionali e applicazioni moderne. Questo, a sua volta, abilita livelli di sicurezza ed efficienza prima irraggiungibili dal punto di vista operativo ed economico.

Caratteristiche principali

- Firewall di tipo stateful distribuito: abilita il firewall di tipo stateful fino al layer 7, integrato nel kernel dell'hypervisor, distribuito in tutto l'ambiente con integrazione diretta in Cloud Native, public cloud nativi e host bare-metal
- Microsegmentazione context-aware: crea policy e gruppi di sicurezza in modo dinamico e li aggiorna automaticamente in base a numerosi attributi e alle informazioni delle applicazioni layer 7 per abilitare una policy di microsegmentazione adattiva
- Cloud Management: si integra in modo nativo con VMware vRealize® Suite, OpenStack e altro ancora e supporta completamente Terraform Provider, moduli Ansible e integrazione con PowerShell
- Integrazione di terze parti: migliora i servizi di sicurezza e networking avanzato attraverso un ecosistema di vendor di terze parti leader del settore
- Supporto nativo per il cloud: supporta networking e sicurezza avanzati di classe enterprise su piattaforme di container, VM e host bare-metal con visibilità sulla rete di container
- NSX Intelligence®: riduce il tempo necessario per rilevare, analizzare e applicare le policy di segmentazione delle applicazioni senza nuovi strumenti o agenti da distribuire; semplifica le operation di sicurezza con sicurezza intrinseca integrata nell'infrastruttura
- NSX Distributed IDS/IPS®: si tratta di un motore di rilevamento delle minacce che rileva il movimento laterale sul traffico est-ovest utilizzando funzionalità di analisi distribuita integrate e la distribuzione di firme selezionate

NSX consente all'IT di diventare un fattore strategico per l'innovazione dell'organizzazione, potendo soddisfare contemporaneamente tutte le richieste delle numerose parti interessate senza che si verifichino conflitti e che le richieste stesse si escludano a vicenda. L'IT può ora fornire livelli di sicurezza senza precedenti, a un ritmo sempre al passo con il business.

Sicurezza intrinseca

VMware NSX sfrutta una visibilità unica sulla composizione delle applicazioni, dalle comunicazioni di rete al comportamento a livello di processo su singoli carichi di lavoro, grazie dalla sua posizione integrata nell'hypervisor e ad altri punti di controllo nativi su cui sono costruite le applicazioni. Questa visibilità favorisce la creazione automatizzata di policy di sicurezza della rete in base al livello di sicurezza desiderato per l'applicazione. Questo riduce il tempo che i team della sicurezza delle informazioni/dell'IT e dello sviluppo delle applicazioni impiegano nei cicli di revisione della sicurezza.

Consente inoltre l'estensione e l'applicazione delle policy di sicurezza in più data center e ambienti hybrid cloud e consente un controllo diffuso delle applicazioni create su VM, container e server bare-metal. NSX Intelligence fornisce continua visibilità su tutto il data center per semplificare e automatizzare radicalmente l'operatività della microsegmentazione.

NSX Distributed IDS/IPS aiuta a raggiungere facilmente la compliance, creare zone di sicurezza virtuali e rilevare il movimento laterale delle minacce sul traffico est-ovest. NSX estende inoltre la visibilità e il controllo ai servizi di sicurezza di terze parti, come firewall di nuova generazione, sistema di prevenzione delle intrusioni (IPS)/sistema di rilevamento delle intrusioni (IDS) e strumenti antivirus, migliorandone l'efficacia.

NSX sposta la sicurezza da un processo aggiuntivo reattivo del ciclo di vita dello sviluppo delle applicazioni a un passaggio proattivo, integrato e automatizzato nel ciclo di vita. I carichi di lavoro appena sottoposti a provisioning ereditano automaticamente le policy di sicurezza che conservano per tutto il ciclo di vita. Quando i carichi di lavoro diventano obsoleti, lo diventano anche le relative policy di sicurezza, il che ne riduce la proliferazione e ne semplifica la gestione.

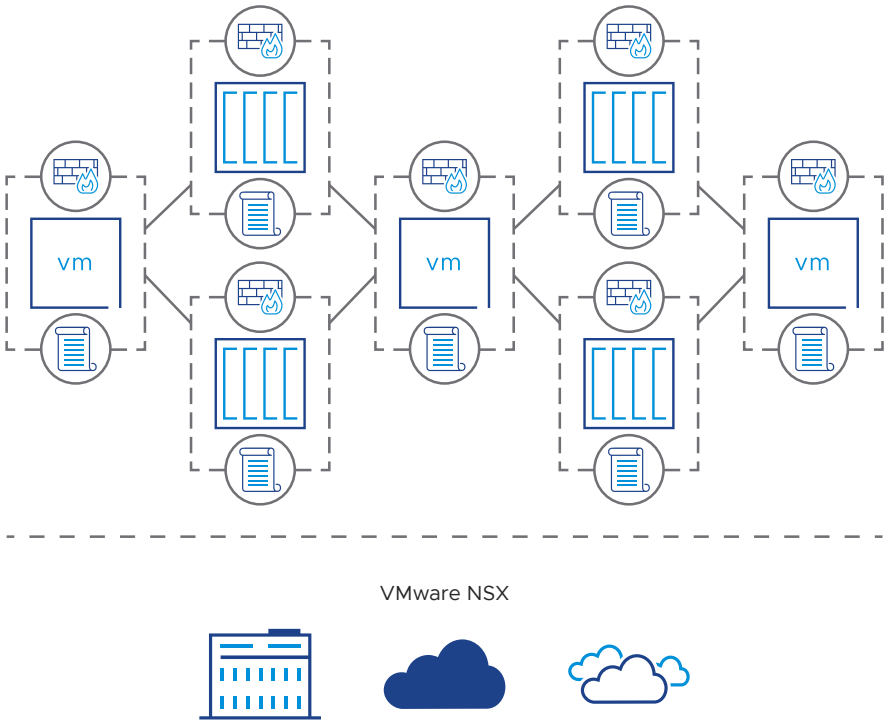

Figura 2. Applicazione della sicurezza al livello più granulare del data center.

Automazione

Con le organizzazioni che continuano ad accelerare il ritmo e a estendere l'ambito delle proprie attività, l'automazione di networking e sicurezza virtualizzati assicura che i servizi e le applicazioni vengano creati e distribuiti al passo con il business. Eliminando, attraverso l'automazione, le attività di provisioning della rete manuali e soggette a errori, la velocità di deployment delle applicazioni aumenta notevolmente.

VMware NSX abbinato a un software di Cloud Management (ad esempio VMware vRealize Automation Cloud™) può gestire il provisioning, il deployment, le operation e la dismissione dell'infrastruttura e delle applicazioni di networking e sicurezza da un control plane centrale. Integrando il ciclo di vita di networking e sicurezza nel processo tramite strumenti come Terraform e Ansible, VMware automatizza tutte le operation dell'infrastruttura ed elimina i colli di bottiglia di networking e sicurezza nel ciclo di vita delle applicazioni.

L'automazione per il networking e la sicurezza delle app, sia di quelle tradizionali basate su VM sia delle nuove app basate su container, è resa possibile dall'estensione delle comuni policy di networking e sicurezza in entrambi i framework. Inoltre, ciò consente il deployment, la mobility e il ritiro automatici delle applicazioni nei data center on-premise, nei private cloud e nei public cloud.

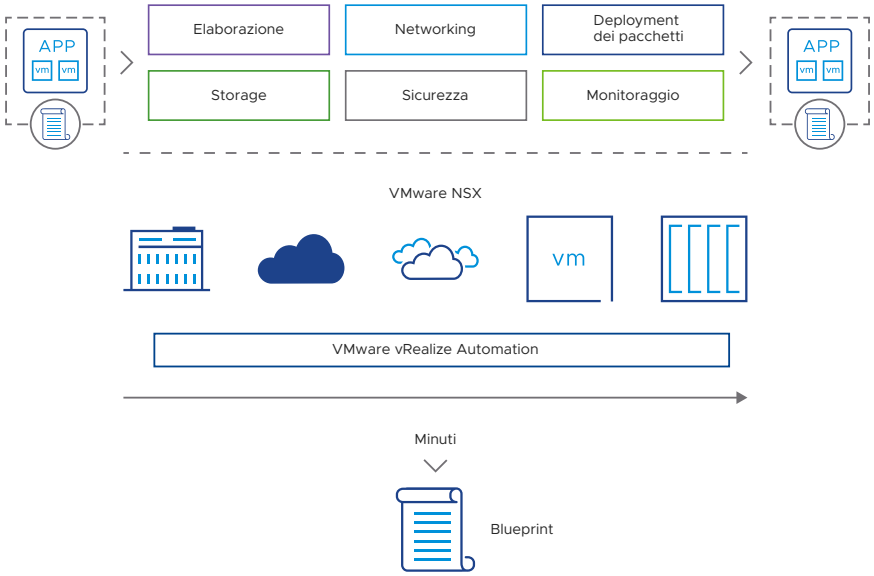

Figura 3. Deployment rapidi e ripetibili con networking e sicurezza automatizzati.

Multi-cloud networking

NSX e NSX Cloud™ forniscono un modello di networking e sicurezza unificato tra più siti, eliminando la configurazione della rete manuale e raggiungendo un'elevata efficienza operativa attraverso l'automazione della rete. Le policy di rete e sicurezza rimangono associate al singolo carico di lavoro in tutto il suo ciclo di vita, semplificando la gestione delle policy negli ambienti hybrid cloud e multi-cloud. La federazione NSX permette la gestione delle policy centralizzata tra vari ambienti (on-premise e cloud), offrendo semplicità operativa e un'applicazione coerente tra i cloud.

Questo consente inoltre alle organizzazioni di migrare le VM o interi data center da una posizione all'altra con un downtime delle applicazioni minimo o nullo. Di conseguenza, le organizzazioni possono accelerare il ripristino durante le migrazioni pianificate e le interruzioni non pianificate. Con rete e sicurezza in ambienti eterogenei, le organizzazioni possono inoltre sfruttare le risorse di vari data center fisici come unico private cloud. Questa forma di raggruppamento delle risorse in pool con data center attivo-attivo prende il nome di multi-data center pooling o metro pooling.

Insieme, offrono mobility delle applicazioni fluida e sicura, agevolando la migrazione da e verso il cloud o tra siti fisici. NSX e NSX Cloud estendono la stessa piattaforma di rete e sicurezza virtualizzata che utilizzano le organizzazioni IT nella loro infrastruttura nel cloud o in altri siti, per un processo di migrazione rapido e con intervento manuale minimo.

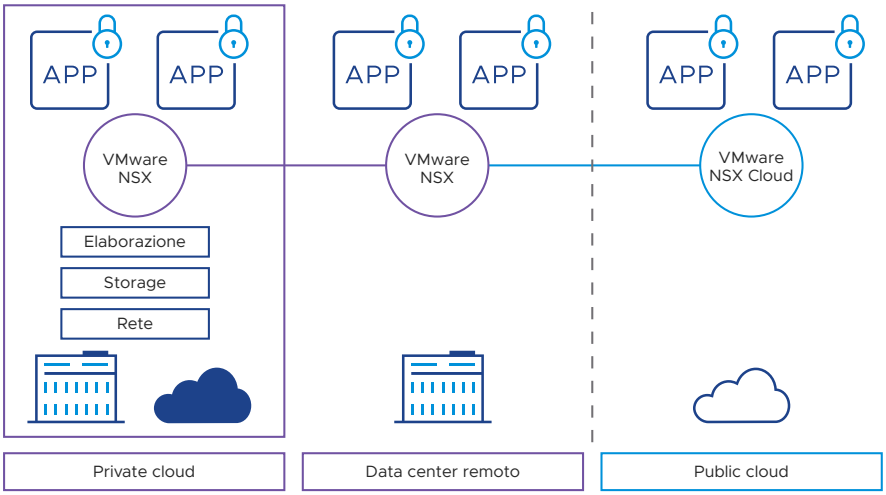

Figura 4. Networking e sicurezza coerenti tra più siti e cloud e riduzione dell'impatto delle interruzioni.

Networking e sicurezza per le app moderne

VMware NSX si integra alle piattaforme di app nuove per offrire funzionalità di networking e sicurezza (come bilanciamento del carico, firewall, switching e routing), il tutto completamente nel software e usufruibile in modalità basata su API e Infrastructure-as-Code.

Poiché le applicazioni si basano sempre di più su architetture di microservizi e container, è necessario saper connettere e proteggere queste nuove applicazioni fino al singolo carico di lavoro. NSX tratta i container e i microservizi come cittadini di serie A, proprio come qualsiasi altro carico di lavoro o endpoint, compresa la possibilità di networking L3. Può eseguire networking da container a container, come anche creare microsegmenti fino al livello del singolo container, abilitando la microsegmentazione per i microservizi, con policy che seguono i carichi di lavoro nelle loro fasi di provisioning, modifica, spostamento e dismissione.

NSX si integra con più piattaforme di orchestrazione di container e applicazioni, hypervisor e ambienti public cloud. Si integra anche nelle piattaforme di applicazioni per portare networking e sicurezza intrinseci e agili nelle nuove applicazioni man mano che vengono sviluppate.

Ulteriori informazioni

Per saperne di più, consulta le seguenti risorse:

- *Pagina del prodotto VMware NSX*
- *Scheda tecnica VMware NSX*
- *Panoramica della soluzione VMware NSX Intelligence*
- *Pagina del prodotto VMware NSX Distributed IDS/IPS*

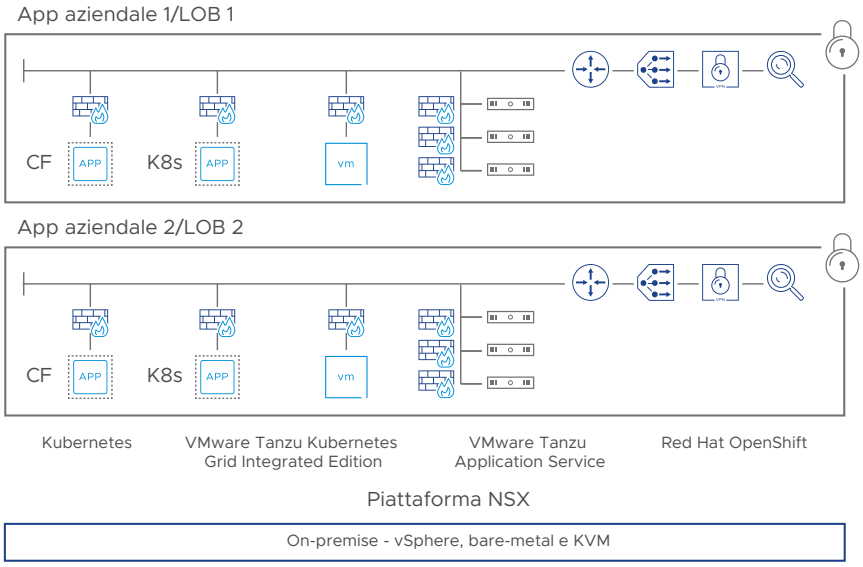

Figura 5. Networking e sicurezza avanzati per carichi di lavoro containerizzati in più framework applicativi, piattaforme, siti e cloud.

Aumentare il valore aziendale oggi e gettare le basi per il futuro

Per le organizzazioni che lo hanno distribuito, NSX diventa presto il fattore determinante per il successo delle organizzazioni IT, nonché una parte fondamentale dell'infrastruttura del data center e delle strategie multi-cloud. Oggi, migliaia di clienti NSX aumentano il valore per l'organizzazione distribuendo alcune delle loro applicazioni più sensibili e critiche su reti virtuali veloci, agili e sicure in un modo che semplicemente non può essere raggiunto sulle tradizionali reti basate su hardware.

Questa evoluzione in ambito di networking e sicurezza permette ai clienti NSX di ottenere vantaggi significativi e immediati e inoltre elimina le attività complesse e dispendiose in termini di tempo che in precedenza occupavano gran parte della larghezza di banda dell'organizzazione. Questo, a sua volta, offre alle organizzazioni la possibilità di considerare strategie organizzative migliori nella pianificazione del loro futuro e consente alle funzioni IT pertinenti di supportare questa vision.

Item No.: 1356650aq-so-nsx-a4_IT 4/23