MICROSEGMENTAZIONE CONTEXT-AWARE CON VMWARE NSX DATA CENTER

Protezione della rete dalla diffusione laterale delle minacce

Le applicazioni moderne sono complesse, distribuite e dinamiche

Le aziende di oggi stanno cercando nuovi modi per gestire il proprio business in un ambiente iperconnesso in cui le applicazioni e i dati sono essenziali. Le applicazioni moderne sono distribuite su più data center e cloud e si estendono oltre il perimetro aziendale.

La virtualizzazione, insieme all'avvento dell'approccio DevOps, della containerizzazione e dei microservizi, ha consentito di accelerare la creazione e la modifica delle applicazioni. A causa della natura distribuita delle applicazioni moderne e della velocità con cui cambiano, garantire la sicurezza è molto complicato.

Le strategie di sicurezza legacy non sono più efficaci

Con la continua proliferazione delle applicazioni, gli approcci di sicurezza tradizionali incentrati sul perimetro non sono più in grado di assicurare la protezione delle applicazioni e dei dati. I cybercriminali hanno dimostrato più volte di poter violare o eludere le misure di sicurezza del perimetro. Una volta all'interno, possono spostarsi indisturbati lateralmente, da un server all'altro, alla ricerca di informazioni da rubare o bloccare in attesa del pagamento di un riscatto.

Nell'era delle moderne applicazioni distribuite, i team responsabili delle reti e della sicurezza IT spesso devono gestire diverse policy di sicurezza per le varie parti dell'ambiente. Ciò crea delle falle nello stato di sicurezza generale.

Sicurezza coerente dal data center al cloud, fino al perimetro

Con VMware NSX® Data Center è possibile definire le policy di sicurezza in modo coerente per l'intero ambiente, indipendentemente dal tipo di applicazione e dalla posizione in cui viene distribuita. Le policy vengono applicate a livello di singolo carico di lavoro, abilitando la segmentazione dei carichi di lavoro eseguiti sullo stesso host fisico senza dover instradare (hairpinning) il traffico attraverso un firewall esterno, virtuale o fisico. Questo livello granulare di sicurezza prende il nome di microsegmentazione.

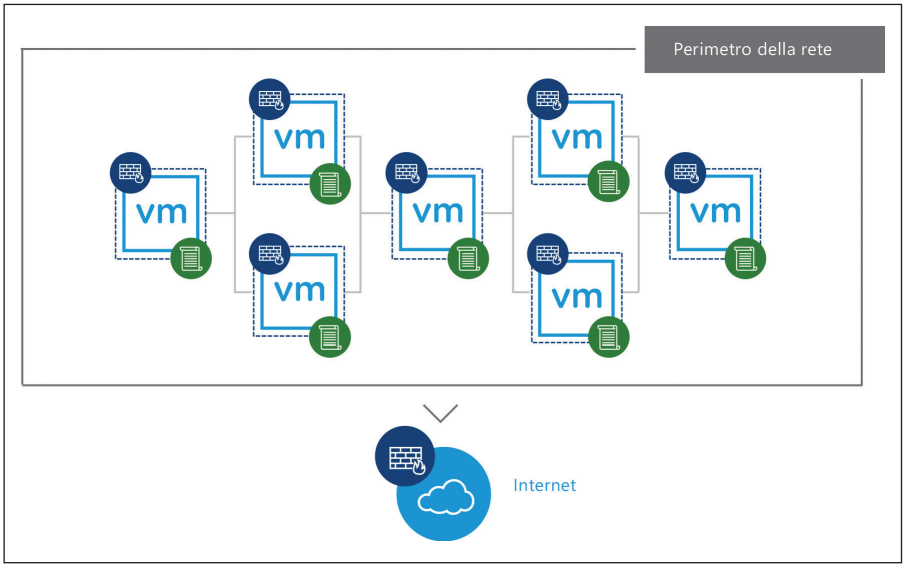

Figura 1. Il termine microsegmentazione indica l'applicazione della policy di sicurezza della rete a livello di singolo carico di lavoro.

"Con l'aumento del numero dei dispositivi IoT, per garantire una protezione superiore è necessaria una maggiore segmentazione della rete in modo che le minacce non possano spostarsi lateralmente nel data center"

CHRISTOPHER FRENZ
DIRECTOR OF INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

vmware®

CONCETTI CHIAVE

- La natura dinamica e distribuita delle applicazioni moderne rende inadeguati i sistemi di sicurezza tradizionali incentrati sulla protezione del perimetro.
- VMware NSX Data Center abilita la microsegmentazione per proteggere le applicazioni dalla diffusione laterale delle minacce.
- La policy di sicurezza viene definita in base al contesto dell'applicazione e applicata ai singoli carichi di lavoro.
- La sicurezza viene distribuita in modo uniforme dal data center al cloud, fino al perimetro.

I microsegmenti creati con NSX Data Center sono definiti e gestiti nel software, per questo sono agili e automatizzabili. I nuovi carichi di lavoro ereditano automaticamente le policy di sicurezza, che li seguiranno durante tutto il loro ciclo di vita, indipendentemente da dove vengono distribuiti o spostati.

Microsegmentazione context-aware e sicurezza allineata alle applicazioni e ai dati

La possibilità di definire le policy di sicurezza in base a fattori fondamentali è importante quanto la distribuzione coerente delle policy. NSX Data Center separa la policy di sicurezza dagli attributi di rete statici (come indirizzo IP, porta e protocollo) e consente di definire le policy in base alla comprensione del contesto dell'applicazione e dell'infrastruttura. Il contesto include gli attributi dell'utente, dell'identità e del carico di lavoro (come il sistema operativo) o addirittura gli ambiti della compliance normativa.

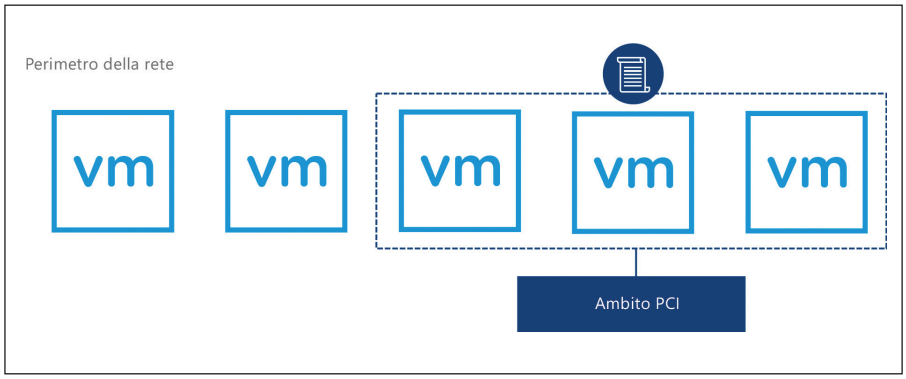

Figura 2. In NSX Data Center è possibile definire microsegmenti in base a numerosi contesti diversi, come ad esempio gli ambiti della compliance normativa.

La microsegmentazione context-aware di NSX Data Center assicura ai team responsabili della sicurezza della rete la flessibilità necessaria per proteggere le applicazioni e i dati in base a fattori fondamentali. Ad esempio, NSX Data Center può essere utilizzato per proteggere un deployment VDI (Virtual Desktop Infrastructure) attraverso l'applicazione di una policy di rete basata sul contesto dell'utente, fino al livello della singola sessione RDSH. Le policy di sicurezza possono essere applicate anche a tutti i carichi di lavoro che rientrano negli standard PCI (Payment Card Industry) indipendentemente dalla loro posizione fisica nell'ambiente.

Servizi di sicurezza avanzati disponibili quando e dove servono

NSX Data Center consente di inserire servizi di sicurezza avanzati di terze parti in un microsegmento specifico. Invece di instradare tutto il traffico di rete attraverso un dispositivo fisico o un'appliance virtuale, come un firewall di nuova generazione (NGFW) o un sistema di rilevamento delle intrusioni (IDS)/prevenzione delle intrusioni (IPS), NSX Data Center può indirizzare dinamicamente traffici specifici verso questi servizi a livello di rete virtuale. In questo modo, i servizi di sicurezza avanzati possono essere inseriti nei punti giusti, al momento giusto, ottimizzando l'efficienza del traffico di rete e migliorando allo stesso tempo l'efficacia degli stessi servizi di sicurezza.

Visibilità del traffico di rete dell'intero ambiente

Per realizzare la microsegmentazione è necessario innanzitutto comprendere i flussi dell'odierno traffico di rete. VMware Network Insight™ offre una vista completa di tutto il traffico di rete del data center, sia fisico che virtuale. Dopo aver analizzato il traffico di rete, VMware Network Insight consiglierà automaticamente le policy di microsegmentazione che potranno quindi essere implementate con NSX Data Center.

È possibile iniziare subito con una valutazione gratuita della rete virtuale per analizzare il traffico di rete corrente e procedere con la definizione del progetto di microsegmentazione. Per ulteriori informazioni visita l'indirizzo www.vmware.com/it/products/nsx/security.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.com/it