VMWARE NSX CLOUD

Funzionalità di rete e sicurezza coerenti per applicazioni eseguite in modo nativo nei cloud pubblici

IN BREVE

VMware NSX® Cloud fornisce funzionalità di rete e sicurezza coerenti per le applicazioni eseguite in modo nativo nel cloud pubblico. NSX Cloud utilizza lo stesso pannello di gestione e controllo di NSX Data Center per offrire una singola soluzione di rete e sicurezza che si estende dal data center privato al cloud pubblico.

VANTAGGI PRINCIPALI

Le funzionalità di rete e sicurezza comuni a tutti i cloud pubblici, come AWS e Azure, consentono non solo di migliorare notevolmente la scalabilità, il controllo e la visibilità ma anche di ridurre le spese OpEx.

- Scalabilità semplificata di reti virtuali, zone di disponibilità, aree e cloud pubblici.
- Controllo preciso dei servizi di sicurezza e rete che assicura la protezione e la standardizzazione delle applicazioni.
- Visibilità end-to-end delle reti e della sicurezza per garantire l'integrità e la compliance delle applicazioni nei cloud pubblici.

PREZZI

- Prezzo basato su un abbonamento (licenze a termine per 1 o 3 anni)
- Prezzo basato sulle vCPU utilizzate dai carichi di lavoro attivati nel cloud pubblico, indipendentemente dal numero di reti virtuali (ad esempio, VPC AWS, VNet Azure)
- Non è richiesta alcuna licenza NSX Data Center per i casi d'uso relativi al solo cloud

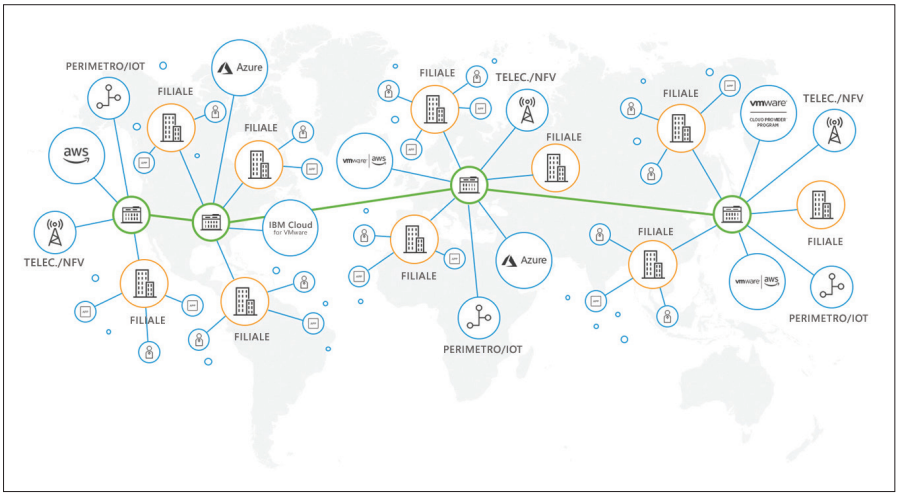

Figura 1: VCN (Virtual Cloud Network)

Una rete creata appositamente per il cloud

VMware NSX Cloud fornisce funzionalità di rete e sicurezza per le applicazioni eseguite in modo nativo nei cloud pubblici. Integrato nella famiglia di soluzioni VMware NSX, VMware NSX Cloud abilita la rete VCN (Virtual Cloud Network), un approccio Software-Defined al networking che si estende a data center, cloud, endpoint e oggetti.

Casi d'uso

Sicurezza coerente su qualsiasi cloud

NSX Cloud consente di utilizzare le stesse policy per i carichi di lavoro eseguiti su diversi cloud pubblici. NSX Cloud utilizza lo stesso pannello di controllo e lo stesso data plane di NSX Data Center per assicurare una gestione delle policy end-to-end su tutti i data center e i cloud. La policy viene definita una sola volta e applicata ai carichi di lavoro ovunque (reti CVN, aree, zone di disponibilità e diversi cloud provider). Le policy di sicurezza vengono applicate dinamicamente a ciascun carico di lavoro in base agli attributi di applicazione e ai tag definiti dall'utente. I carichi di lavoro fuori controllo o compromessi possono essere messi automaticamente in quarantena se non presentano la corretta policy di sicurezza per la microsegmentazione.

Controllo accurato sulle reti cloud

VMware NSX Cloud è stato sviluppato per gli ambienti di cloud pubblico nativi come Amazon (AWS) e Microsoft Azure. NSX Cloud completa i servizi nativi forniti da questi provider di cloud pubblico. Con NSX Cloud è possibile continuare a utilizzare per i carichi di lavoro i servizi di infrastruttura e applicativi dei provider di cloud pubblico, senza alcuna limitazione (ad esempio, AWS ELB/Azure Load Balancer, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute e Amazon RDS/Azure Database). La gestione del provisioning e della configurazione può essere automatizzata tramite richieste API REST utilizzando gli strumenti di automazione esistenti.

PER ULTERIORI INFORMAZIONI O PER ACQUISTARE LE SOLUZIONI VMWARE

CHIAMA IL NUMERO
(+39) 02 3041 2700

VISITA L'INDIRIZZO
www.vmware.com/it/products/nsx-cloud.html o http://www.vmware.com/it/products oppure cerca online un rivenditore autorizzato

Visibilità e controllo delle operation end-to-end

VMware NSX Cloud fornisce interfacce e protocolli standard per l'accesso ai dati di rete e sicurezza dalle reti cloud. Le informazioni su flussi, pacchetti ed eventi sono disponibili tramite IPFIX, Traceflow, mirroring delle porte e Syslog. Questi dati possono essere gestiti con gli strumenti per le operation disponibili on-site e utilizzati per abilitare una visibilità end-to-end dettagliata per il monitoraggio, la risoluzione dei problemi e l'audit. Le informazioni dettagliate sulle operation consentono di accelerare notevolmente il processo di identificazione e risoluzione dei problemi di connettività, prestazioni e sicurezza della rete per l'intero deployment di cloud ibrido, incluse le applicazioni on-site e nel cloud pubblico.

Funzionalità principali

Reti e sicurezza multi-cloud e multisito: NSX Cloud estende le funzionalità di rete e sicurezza agli endpoint su più cloud e, grazie all'integrazione con NSX Data Center, consente di gestire le reti e la sicurezza su più cloud e siti del data center.

Microsegmentazione: assicura il controllo del traffico est-ovest tra i carichi di lavoro delle applicazioni eseguiti in modo nativo nei cloud pubblici.

Gruppi di sicurezza: è possibile definire regole e gruppi di sicurezza in base a numerosi costrutti di policy, come nome dell'istanza, tipo di sistema operativo, ID AMI e tag definiti dall'utente.

Policy dinamica: la policy di sicurezza viene applicata dinamicamente in base agli attributi dell'istanza e ai tag definiti dall'utente. Le policy seguono automaticamente le istanze quando vengono spostate all'interno di uno stesso cloud o in altri cloud.

Quarantena delle istanze: i carichi di lavoro fuori controllo o compromessi eseguiti nel cloud pubblico che non presentano la sicurezza della microsegmentazione vengono messi in quarantena. Le istanze in quarantena non possono comunicare sulla rete cloud.

Architettura distribuita: l'architettura distribuita del firewall di NSX Cloud elimina la necessità di traffico e hop di rete aggiuntivi, poiché le policy vengono applicate a ogni istanza nell'interfaccia della rete virtuale invece di instradarle attraverso un firewall esterno.

Edge Firewall: NSX Cloud fornisce un firewall di tipo stateful che filtra il traffico nord-sud tra le istanze sulle reti virtuali e sulla rete Internet pubblica.

API RESTful: le API RESTful e gli strumenti di automazione consentono di eseguire on demand il provisioning e la configurazione dell'infrastruttura di rete e sicurezza in modo programmatico.

Template: è possibile utilizzare gli strumenti di automazione e orchestrazione esistenti per creare template di applicazioni standard e semplificare il provisioning e la gestione dei servizi di rete e sicurezza nei cloud pubblici.

Visibilità del traffico est-ovest: è possibile utilizzare gli strumenti esistenti per la gestione delle operation successive per ottenere visibilità sul traffico est-ovest all'interno di un VPC e tra diversi VPC.

Registri della sicurezza: questi registri forniscono visibilità in tempo reale e audit degli eventi di sicurezza come gli incidenti di quarantena e di tipo "consenti/nega". Le informazioni sugli eventi di sicurezza vengono inviate a un server Syslog o SIEM.

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