AWS Whitepaper

Creazione di un'infrastruttura multi-rete scalabile e sicura VPC AWS

Creazione di un'infrastruttura multi-rete scalabile e sicura VPC AWS: AWS Whitepaper

Table of Contents

Creazione di un'infrastruttura di rete AWS multi-VPC scalabile e sicura

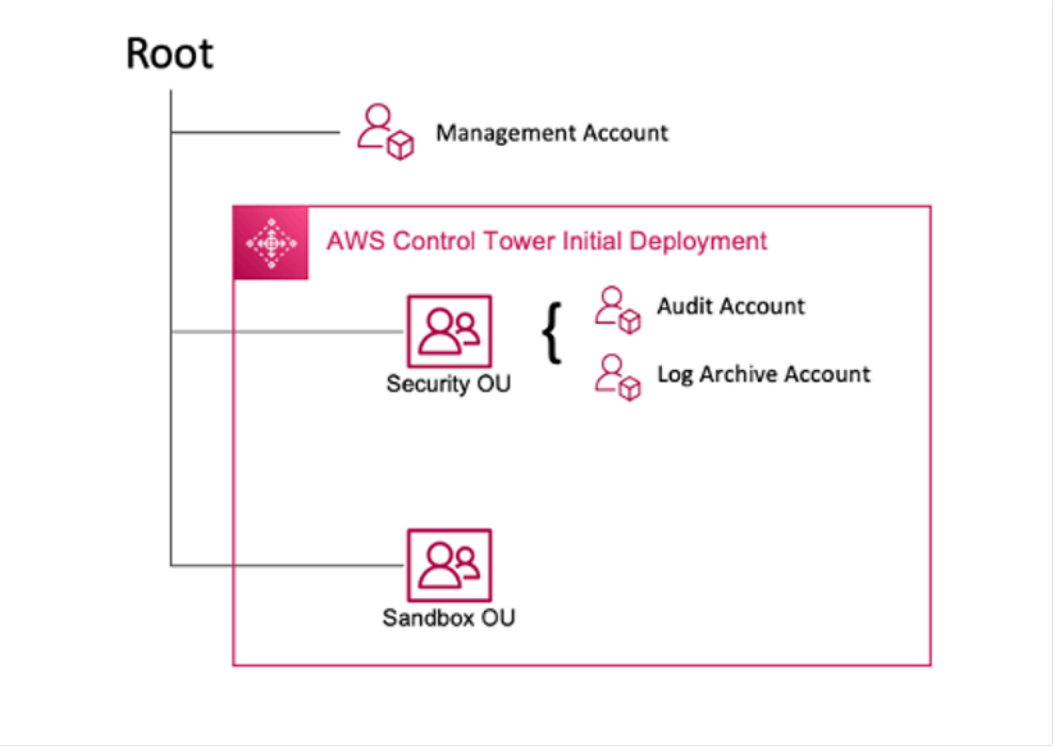
Data di pubblicazione: 17 aprile 2024 () Cronologia dei documenti

I clienti di Amazon Web Services (AWS) spesso si affidano a centinaia di account e cloud privati virtuali (VPC) per segmentare i propri carichi di lavoro ed espandere la propria presenza. Questo livello di scalabilità spesso crea problemi relativi alla condivisione delle risorse, alla connettività tra VPC e alle strutture locali alla connettività VPC.

Questo white paper descrive le best practice per creare architetture di rete scalabili e sicure in una rete di grandi dimensioni utilizzando AWS servizi come Amazon Virtual Private Cloud (Amazon VPC),, AWS Transit Gateway, AWS PrivateLinkGateway Load AWS Direct ConnectBalancer e Amazon Route 53. AWS Network Firewall Presenta soluzioni per la gestione di un'infrastruttura in crescita, garantendo scalabilità, alta disponibilità e sicurezza mantenendo bassi i costi generali.

Introduzione

AWS i clienti iniziano creando risorse in un unico AWS account che rappresenta un limite di gestione che segmenta autorizzazioni, costi e servizi. Tuttavia, man mano che l'organizzazione del cliente cresce, diventa necessaria una maggiore segmentazione dei servizi per monitorare i costi, controllare l'accesso e fornire una gestione ambientale più semplice. Una soluzione multi-account risolve questi problemi fornendo account specifici per i servizi IT e gli utenti all'interno di un'organizzazione. AWS fornisce diversi strumenti per gestire e configurare questa infrastruttura, tra cui. AWS Control Tower



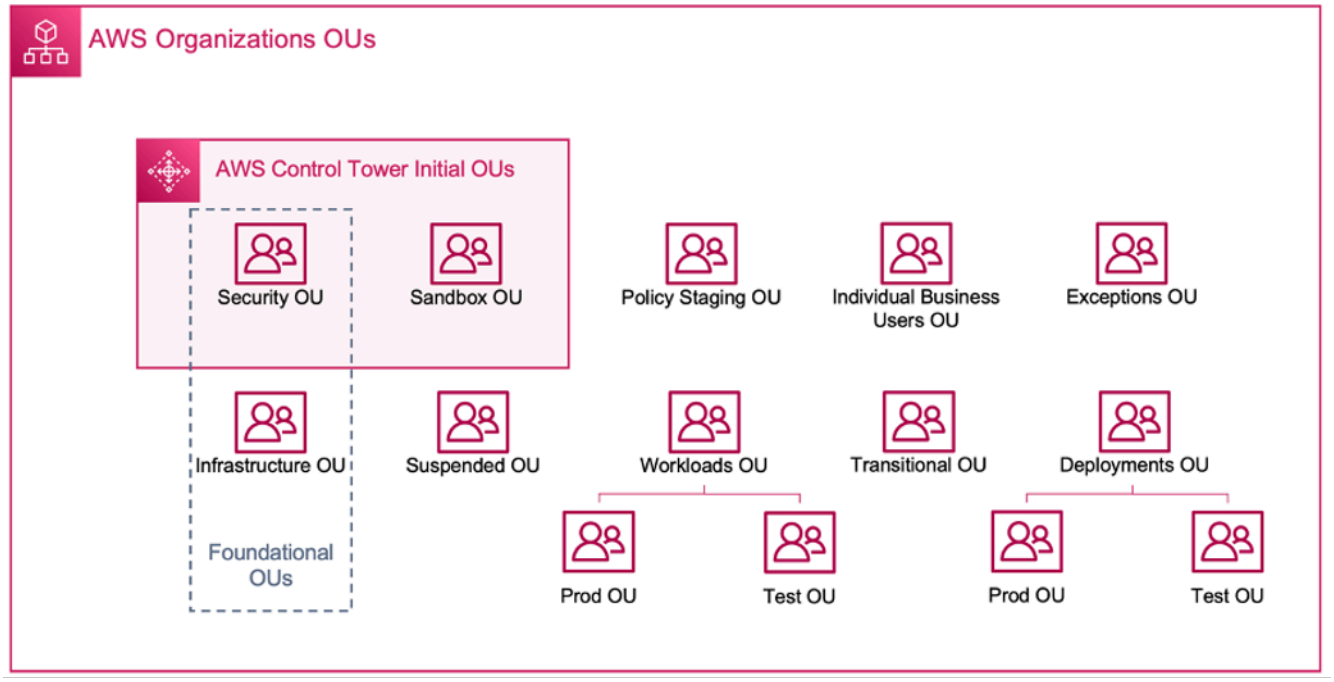
AWS Installazione iniziale di Control Tower

Quando configuri un ambiente multi-account utilizzando AWS Control Tower, vengono create due unità organizzative (OU):

- Unità organizzativa di sicurezza: all'interno di questa unità organizzativa, AWS Control Tower crea due account:
- Archivio dei log
- Verifica (questo account corrisponde all'account Security Tooling discusso in precedenza nella guida).
- Sandbox OU: questa unità organizzativa è la destinazione predefinita per gli account creati all'interno. AWS Control Tower Contiene account in cui i builder possono esplorare e sperimentare AWS servizi e altri strumenti e servizi, in base alle politiche di utilizzo accettabile del team.

AWS Control Tower consente di creare, registrare e gestire unità organizzative aggiuntive per espandere l'ambiente iniziale e implementare le linee guida.

Il diagramma seguente mostra le unità organizzative inizialmente distribuite da. AWS Control TowerÈ possibile espandere l' AWS ambiente per implementare una qualsiasi delle unità organizzative consigliate incluse nel diagramma, per soddisfare i requisiti.



AWS unità organizzative

Per ulteriori dettagli sull'utilizzo di ambienti con più account AWS Control Tower, consultare l'Appendice E del white paper Organization Your AWS Environment Using Multiple Accounts.

> **Note**
>
> In questo white paper, «Control Tower» è un termine generico per la configurazione multi-account/multi-VPC scalabile, sicura e performante in cui vengono distribuiti i carichi di lavoro. Questa configurazione può essere creata utilizzando diversi strumenti. Puoi trovare ulteriori informazioni sulle migliori pratiche, i principi di progettazione e i vantaggi di Multi-Account Cloud Foundation nel white paper Organizing Your AWS Environment Using Multiple Accounts.

La maggior parte dei clienti inizia con pochi VPC per implementare la propria infrastruttura. Il numero di VPC creati da un cliente è in genere correlato al numero di account, utenti e ambienti in più fasi (produzione, sviluppo, test e così via). Con l'aumento dell'utilizzo del cloud, cresce anche il numero di utenti, unità aziendali, applicazioni e regioni con cui un cliente interagisce, il che porta alla creazione di nuovi VPC.

Con l'aumento del numero di VPC, la gestione cross-VPC diventa essenziale per il funzionamento della rete cloud del cliente. Questo white paper illustra le best practice per tre aree specifiche della connettività cross-VPC e ibrida:

- Connettività di rete: interconnessione di VPC e reti locali su larga scala.
- Sicurezza di rete: creazione di punti di uscita centralizzati per l'accesso a Internet e agli endpoint, come il gateway NAT (Network Address Translation), gli endpoint VPC e i Gateway Load Balancer. AWS PrivateLinkAWS Network Firewall
- Gestione DNS: risoluzione del DNS all'interno della Control Tower e del DNS ibrido.

Pianificazione e gestione degli indirizzi IP

Per creare un design di rete multi-VPC scalabile e multi-account, la pianificazione e la gestione degli indirizzi IP sono fondamentali. Un buon schema di indirizzamento IP deve tenere conto delle esigenze di rete attuali e future. L'IP dello schema di indirizzi IP deve coprire i carichi di lavoro on-premise, i carichi di lavoro cloud e deve consentire anche future espansioni (ad esempio, l'aggiunta di nuove Regioni AWS unità aziendali e fusioni o acquisizioni). Dovrebbe inoltre impedire ai team di creare inavvertitamente CIDR IP sovrapposti. Se si desidera che IP CIDR si sovrappongano, ad esempio per carichi di lavoro isolati o disconnessi, questa decisione deve essere consapevole e tenere conto delle implicazioni sul routing, sulla sicurezza e sui costi. Potrebbe inoltre essere necessario prendere in considerazione la creazione dei processi di approvazione necessari per tali eccezioni. Un buon schema di indirizzamento IP aiuta anche a semplificare la progettazione della rete e la configurazione del routing.

Considerazioni chiave:

- Pianifica in anticipo lo schema di indirizzamento IP (IP pubblici e privati) e seleziona uno strumento di gestione degli indirizzi IP per allocare, gestire e tenere traccia dell'utilizzo degli indirizzi IP in tutti i carichi di lavoro.
- Utilizza schemi di indirizzamento IP gerarchici e riepilogativi.
- Pianifica un'assegnazione IP coerente in base all'ambiente Regione AWS, all'organizzazione o all'unità aziendale.
- Designate CIDR IP distinti (sia IPv4 che IPv6) per reti locali e cloud.
- Previeni e monitora in modo proattivo i CIDR IP sovrapposti.
- Dimensiona i tuoi CIDR IP in modo appropriato per consentire la scalabilità e la crescita futura.

- Abilita i carichi di lavoro per la compatibilità IPv6 o dual-stack per ridurre i conflitti IP e ovviare all'esaurimento dello spazio IPv4.

Puoi utilizzare Amazon VPC IP Address Manager (IPAM) per semplificare la pianificazione, il tracciamento e il monitoraggio degli indirizzi IP pubblici e privati per i tuoi carichi di lavoro. AWS IPAM ti consente di organizzare, allocare, monitorare e condividere lo spazio degli indirizzi IP su più e. Regioni AWS Account AWS Inoltre, aiuta con l'allocazione automatica dei CIDR ai VPC utilizzando regole aziendali specifiche.

Consulta le best practice di Amazon VPC IP Address Manager, Gestione dei pool IP tra VPC e regioni utilizzando Amazon VPC IP Address Manager e IP Address Management per i post di AWS Control Tower blog su come apprendere le migliori pratiche di indirizzamento IP e come utilizzare IPAM per gestire i pool IP tra VPC, e. Regioni AWS AWS Control Tower

Sei Well-Architected?

Il AWS Well-Architected Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando AWS Well-Architected Tool, disponibile gratuitamente in AWS Management Console, puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

Per ulteriori indicazioni e best practice da parte degli esperti per la tua architettura cloud (implementazioni dell'architettura di riferimento, diagrammi e white paper), consulta l'Architecture Center.AWS

Connettività da VPC a VPC

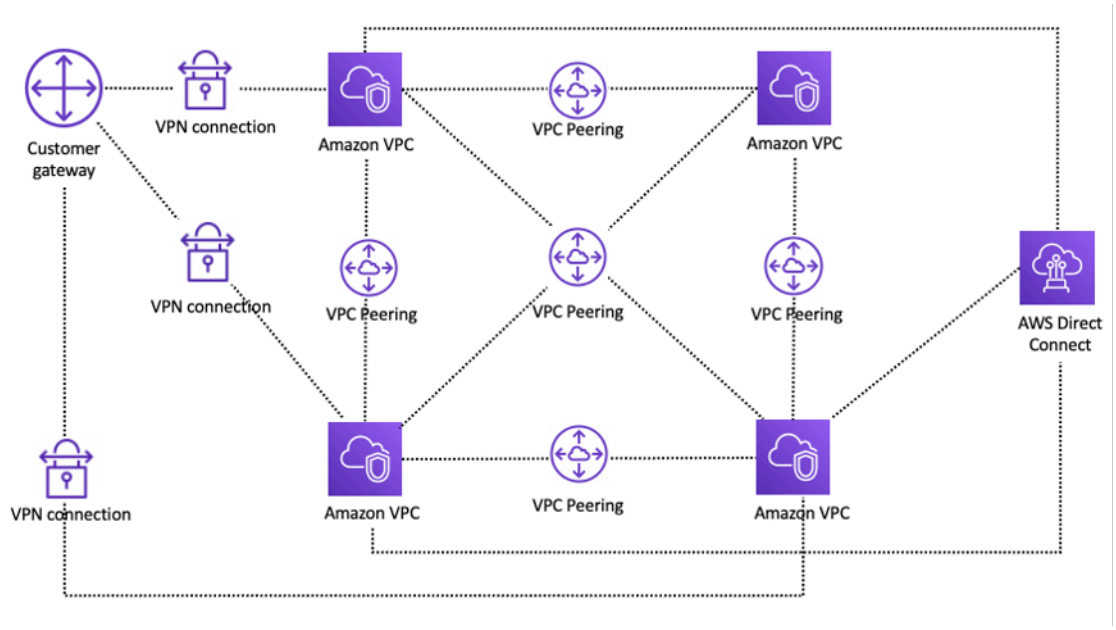
I clienti possono utilizzare due diversi modelli di connettività VPC per configurare ambienti multi-VPC: da molti a molti o hub and spoke. Nell' many-to-many approccio, il traffico tra ogni VPC viene gestito individualmente tra ogni VPC. Nel hub-and-spoke modello, tutto il traffico inter-VPC fluisce attraverso una risorsa centrale, che indirizza il traffico in base a regole stabilite.

Peering VPC

Il primo modo per connettere due VPC consiste nell'utilizzare il peering VPC. In questa configurazione, una connessione consente la connettività bidirezionale completa tra i VPC. Questa connessione peering viene utilizzata per instradare il traffico tra i VPC. È inoltre possibile eseguire il peering di VPC con account e regioni AWS diversi. Tutti i trasferimenti di dati tramite una connessione peering VPC che rimane all'interno di una zona di disponibilità sono gratuiti. Tutti i trasferimenti di dati tramite una connessione peering VPC che attraversa le zone di disponibilità vengono addebitati alle tariffe di trasferimento dati standard locali. Se i VPC sono collegati in peering tra regioni, verranno applicati i costi standard per il trasferimento di dati tra regioni.

Il peering VPC è point-to-point connettività e non supporta il routing transitivo. Ad esempio, se disponi di una connessione peering VPC tra VPC A e VPC B e tra VPC A e VPC C, un'istanza in VPC B non può transitare attraverso VPC A per raggiungere VPC C. Per instradare i pacchetti tra VPC B e VPC C, è necessario creare una connessione peering VPC diretta.

Su larga scala, quando si dispone di decine o centinaia di VPC, l'interconnessione con il peering può portare a una rete di centinaia o migliaia di connessioni peering. Un gran numero di connessioni può essere difficile da gestire e scalare. Ad esempio, se disponi di 100 VPC e desideri configurare un peering a rete completa tra di essi, saranno necessarie 4.950 connessioni peering [`n(n-1)/2`], dove `n` è il numero totale di VPC. Esiste un limite massimo di 125 connessioni peering attive per VPC.



Configurazione della rete tramite peering VPC

Se si utilizza il peering VPC, è necessario effettuare la connettività locale (VPN e/o Direct Connect) su ciascun VPC. Le risorse in un VPC non possono essere raggiunte in locale utilizzando la connettività ibrida di un VPC peerizzato, come illustrato nella figura precedente.

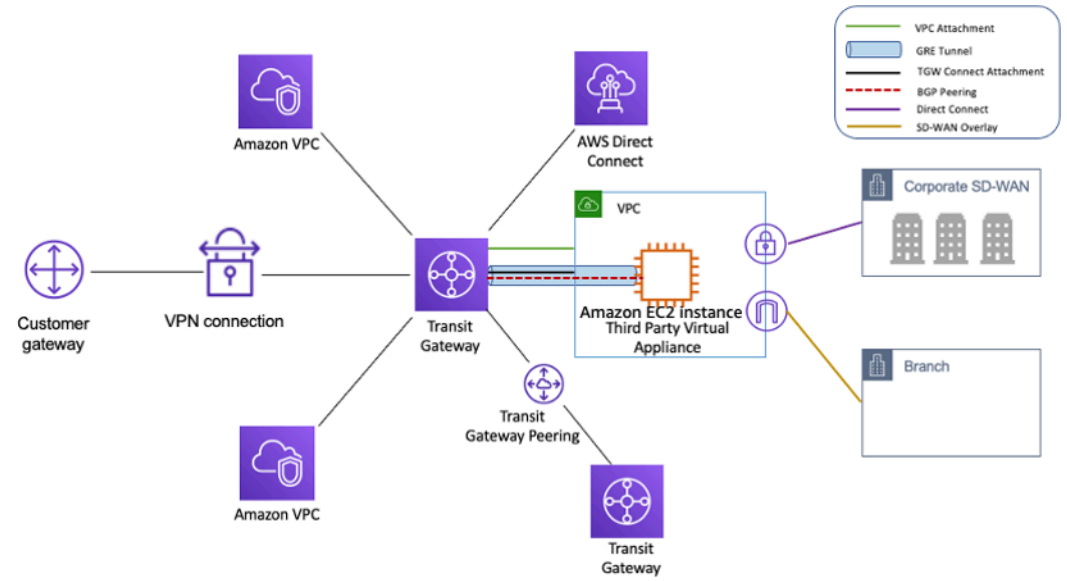
Il peering VPC viene utilizzato al meglio quando le risorse di un VPC devono comunicare con le risorse di un altro VPC, l'ambiente di entrambi i VPC è controllato e protetto e il numero di VPC da connettere è inferiore a 10 (per consentire la gestione individuale di ciascuna connessione). Il peering VPC offre il costo complessivo più basso e le prestazioni aggregate più elevate rispetto ad altre opzioni per la connettività tra VPC.

AWS Transit Gateway

AWS Transit Gatewayoffre un design hub and spoke per connettere VPC e reti locali come servizio completamente gestito senza richiedere il provisioning di appliance virtuali di terze parti. Non è richiesto alcun overlay VPN e AWS gestisce disponibilità e scalabilità elevate.

Transit Gateway consente ai clienti di connettere migliaia di VPC. È possibile collegare tutta la connettività ibrida (connessioni VPN e Direct Connect) a un singolo gateway, consolidando e controllando l'intera configurazione di AWS routing dell'organizzazione in un unico posto (fare riferimento alla figura seguente). Transit Gateway controlla il modo in cui il traffico viene instradato tra tutte le reti spoke connesse utilizzando tabelle di routing. Questo hub-and-spoke modello semplifica

la gestione e riduce i costi operativi perché i VPC si connettono solo all'istanza Transit Gateway per accedere alle reti connesse.



Design del mozzo e del raggio con AWS Transit Gateway

Transit Gateway è una risorsa regionale e può connettere migliaia di VPC all'interno dello stesso Regione AWS. È possibile connettere più gateway tramite una singola connessione Direct Connect per una connettività ibrida. In genere, puoi utilizzare una sola istanza Transit Gateway per connettere tutte le istanze VPC in una determinata regione e utilizzare le tabelle di routing Transit Gateway per isolarle dove necessario. Tieni presente che non sono necessari gateway di transito aggiuntivi per un'elevata disponibilità, poiché i gateway di transito sono altamente disponibili fin dalla progettazione; per la ridondanza, utilizza un unico gateway in ogni regione. Tuttavia, esiste un valido motivo per creare più gateway per limitare gli errori di configurazione del raggio di esplosione, separare le operazioni sul piano di controllo e quelle amministrative. ease-of-use

Con il peering Transit Gateway, i clienti possono peerizzare le proprie istanze Transit Gateway all'interno della stessa o di più regioni e instradare il traffico tra di esse. Utilizza la stessa infrastruttura sottostante del peering VPC ed è quindi crittografato. Per ulteriori informazioni, consulta Creazione di una rete globale utilizzando il peering interregionale di AWS Transit Gateway e AWS Transit Gateway ora supporta il peering intra-regionale.

Inserisci l'istanza Transit Gateway della tua organizzazione nel relativo account Network Services. Ciò consente la gestione centralizzata da parte degli ingegneri di rete che gestiscono l'account dei servizi di rete. Usa AWS Resource Access Manager (RAM) per condividere un'istanza Transit Gateway per connettere VPC tra più account della tua AWS Organization all'interno della stessa regione.AWS RAM ti consente di condividere AWS risorse in modo semplice e sicuro con qualsiasi

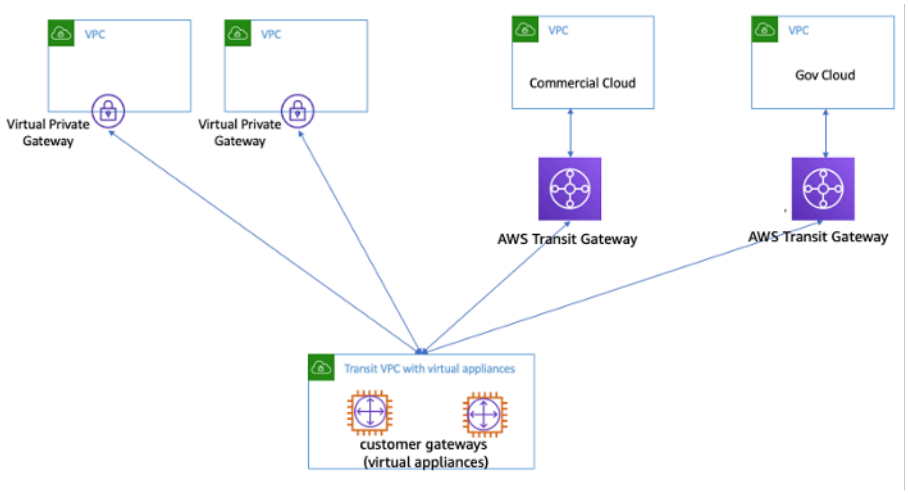
Account AWS AWS Organization o all'interno di essa. Per ulteriori informazioni, consulta gli allegati Automating AWS Transit Gateway a un gateway di transito in un post di blog sull'account centrale.

Transit Gateway consente inoltre di stabilire la connettività tra l'infrastruttura SD-WAN e l' AWS utilizzo di Transit Gateway Connect. Utilizza un allegato Transit Gateway Connect con Border Gateway Protocol (BGP) per il routing dinamico e il protocollo tunnel Generic Routing Encapsulation (GRE) per prestazioni elevate, offrendo fino a 20 Gbps di larghezza di banda totale per allegato Connect (fino a quattro peer Transit Gateway Connect per allegato Connect). Utilizzando Transit Gateway Connect, puoi integrare sia l'infrastruttura SD-WAN locale che le appliance SD-WAN in esecuzione nel cloud tramite un allegato o AWS Direct Connect un allegato VPC come livello di trasporto sottostante. Consulta Semplifica la connettività SD-WAN con AWS Transit Gateway Connect per architetture di riferimento e configurazione dettagliata.

Soluzione Transit VPC

I VPC Transit possono creare connettività tra VPC con un mezzo diverso rispetto al peering VPC, introducendo un design hub and spoke per la connettività tra VPC. In una rete VPC di transito, un VPC centrale (il VPC hub) si connette a tutti gli altri VPC (Spoke VPC) tramite una connessione VPN che in genere sfrutta BGP su IPSec. Il VPC centrale contiene istanze Amazon Elastic Compute Cloud (Amazon EC2) che eseguono appliance software che indirizzano il traffico in entrata verso le rispettive destinazioni utilizzando l'overlay VPN. Il peering VPC Transit presenta i seguenti vantaggi:

- Il routing transitivo è abilitato utilizzando la rete VPN overlay, che consente una progettazione hub and spoke.
- Quando si utilizza software di fornitori terzi sull'istanza EC2 nel VPC Hub Transit, è possibile utilizzare le funzionalità del fornitore relative alla sicurezza avanzata (firewall di livello 7/Intrusion Prevention System (IPS) /Intrusion Detection System (IDS)). Se i clienti utilizzano lo stesso software in locale, traggono vantaggio da un'esperienza operativa/di monitoraggio unificata.
- L'architettura Transit VPC consente la connettività che può essere desiderata in alcuni casi d'uso. Ad esempio, puoi connettere un' GovCloud istanza AWS e un VPC della regione commerciale o un'istanza Transit Gateway a un VPC di transito e abilitare la connettività inter-VPC tra le due regioni. Valuta i tuoi requisiti di sicurezza e conformità quando prendi in considerazione questa opzione. Per una maggiore sicurezza, è possibile implementare un modello di ispezione centralizzato utilizzando i modelli di progettazione descritti più avanti in questo white paper.



VPC di transito con appliance virtuali

Transit VPC presenta alcune sfide, come costi più elevati per l'esecuzione di appliance virtuali di fornitori terzi su EC2 in base alle dimensioni e alla famiglia di istanze, un throughput limitato per connessione VPN (fino a 1,25 Gbps per tunnel VPN) e costi aggiuntivi di configurazione, gestione e resilienza (i clienti sono responsabili della gestione dell'HA e della ridondanza delle istanze EC2 che eseguono le appliance virtuali di fornitori terzi).

Peering VPC, Transit VPC e Transit Gateway

Tabella 1 — Confronto della connettività

Criteri	Peering VPC	VPC di transito	Gateway di transito	PrivateLink	WAN nel cloud	VPC Lattice
Ambito	Regionale/ globale	Regionale	Regionale	Regionale	Globale	Regionale
Architettura	Maglia completa	Basato su VPN hub-and-spoke	Basato su allegati hub-and-spoke	Modello di fornitore o consumatore	Basato sugli allegati, multiregione	Connettività da app a app
Dimensionare	125 peer attivi/VPC	Dipende dal router	5000 allegati per regione	Nessun limite	5000 allegati	500 associazi

Criteri	Peering VPC	VPC di transito	Gateway di transito	PrivateLink	WAN nel cloud	VPC Lattice
		virtuale/ EC2			per rete principale	oni VPC per servizio
Segmentazione	Gruppi di sicurezza	Gestito dal cliente	Tabelle delle rotte Transit Gateway	Nessuna segmentazione	Segmenti	Politiche di servizio e di rete di assistenza
Latenza	Minimo	Extra, a causa del sovraccarico di crittografia della VPN	Transit Gateway hop aggiuntivo	Il traffico rimane sulla spina dorsale di AWS, i clienti dovrebbero testarlo	Utilizza lo stesso piano dati del Transit Gateway	Il traffico rimane sulla spina dorsale di AWS, i clienti dovrebbero testarlo
Limite larghezza di banda	Limiti per istanza, nessun limite aggregato	Soggetto ai limiti di larghezza di banda delle istanze EC2 in base alla dimensione/famiglia	Fino a 100 Gbps (burst) per allegato	10 Gbps per zona di disponibilità, scalabilità automatica fino a 100 Gbps	Fino a 100 Gbps (burst) / allegato	10 Gbps per zona di disponibilità

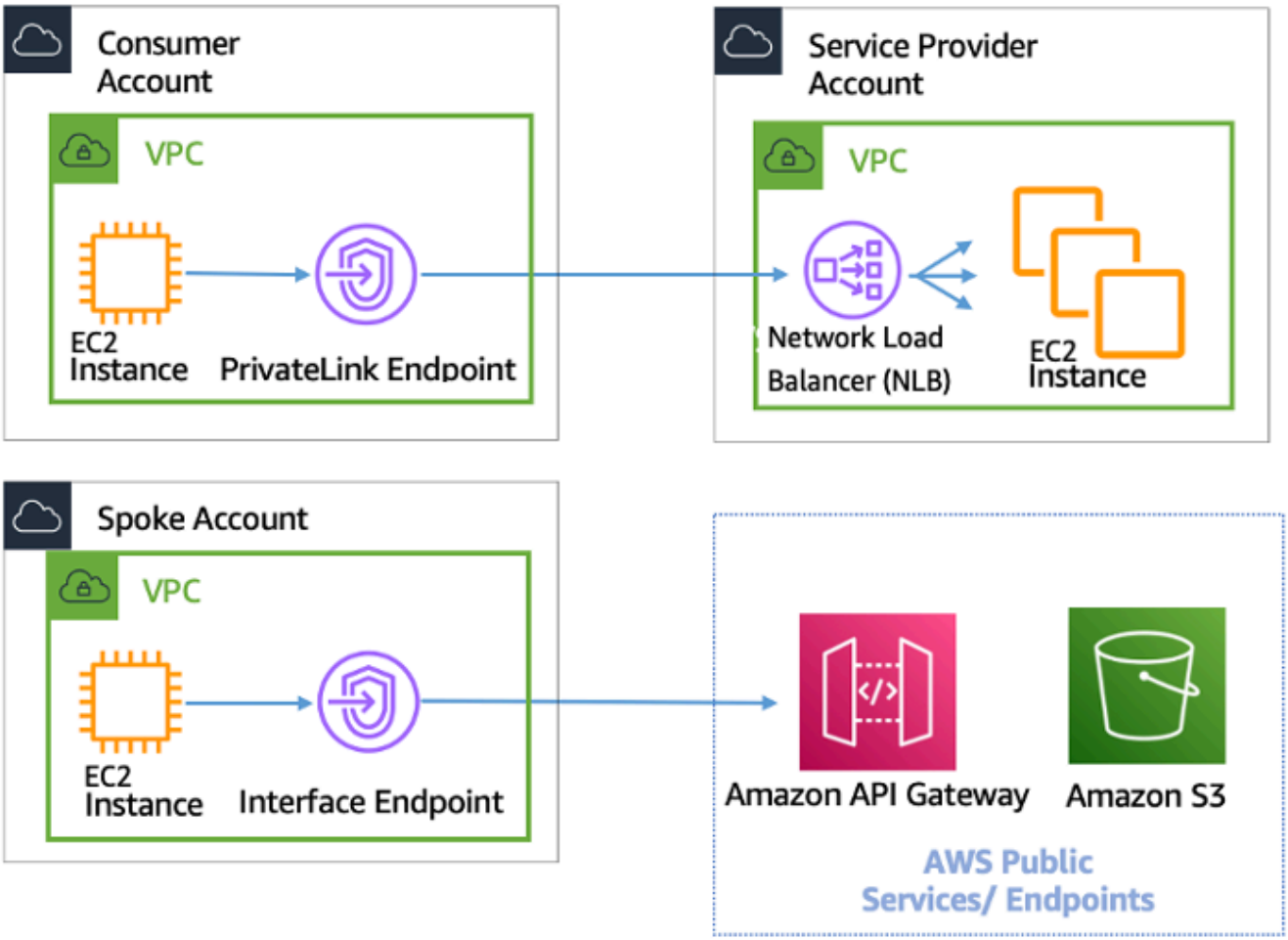
Criteri	Peering VPC	VPC di transito	Gateway di transito	PrivateLink	WAN nel cloud	VPC Lattice
Visibilità	Log di flusso VPC	Registri e metriche di flusso VPC CloudWatch	Transit Gateway Network Manager, log di flusso VPC, metriche CloudWatch	CloudWatch Metriche	Network Manager, log di flusso VPC, metriche CloudWatch	CloudWatch Registri di accesso
Gruppo di sicurezza riferimenti incrociati	Supportato	Non supportato	Non supportato	Non supportato	Non supportato	Non applicabile
Supporto IPv6	Supportato	Dipende dall'appliance virtuale	Supportato	Supportato	Supportato	Supportato

AWS PrivateLink

AWS PrivateLinkfornisce connettività privata tra VPC, servizi AWS e reti locali senza esporre il traffico alla rete Internet pubblica. Gli endpoint VPC di interfaccia, alimentati da AWS PrivateLink, semplificano la connessione AWS e altri servizi su diversi account e VPC per semplificare in modo significativo l'architettura di rete. Ciò consente ai clienti che desiderano esporre privatamente un servizio/applicazione che risiede in un VPC (fornitore di servizi) ad altri VPC (consumatore) all'interno Regione AWS in modo che solo i VPC consumer avviino connessioni al VPC del provider di servizi. Un esempio di ciò è la possibilità per le applicazioni private di accedere alle API dei provider di servizi.

Per utilizzarlo AWS PrivateLink, crea un Network Load Balancer per la tua applicazione nel tuo VPC e crea una configurazione del servizio endpoint VPC che punti a quel load balancer. Un utente del servizio crea quindi un endpoint di interfaccia per il tuo servizio. Questo crea un'interfaccia di rete elastica (ENI) nella sottorete dei consumatori con un indirizzo IP privato che funge da punto di ingresso per il traffico destinato al servizio. Non è necessario che il consumatore e il servizio si trovino nello stesso VPC. Se il VPC è diverso, i VPC del consumatore e del fornitore di servizi possono avere intervalli di indirizzi IP sovrapposti. Oltre a creare l'endpoint VPC di interfaccia per accedere ai servizi in altri VPC, puoi creare endpoint VPC di interfaccia per accedere privatamente ai servizi AWS PrivateLink AWS supportati, come mostrato nella figura seguente.

Con Application Load Balancer (ALB) come obiettivo di NLB, ora puoi combinare le funzionalità di routing avanzate di ALB con. AWS PrivateLink Per le architetture di riferimento e la configurazione dettagliata, fare riferimento a Target Group for Network Load Balancer di tipo Application Load Balancer.



AWS PrivateLink per la connettività ad altri VPC e servizi AWS

La scelta tra Transit Gateway, peering VPC e dipende dalla AWS PrivateLink connettività.

- AWS PrivateLink— Da utilizzare AWS PrivateLink quando si dispone di una configurazione client/server in cui si desidera consentire a uno o più VPC consumer l'accesso unidirezionale a un servizio specifico o a un insieme di istanze nel VPC del provider di servizi o determinati servizi. AWS Solo i client con accesso nel VPC consumer possono avviare una connessione al servizio nel VPC o nel servizio del provider di servizi. AWS Questa è anche una buona opzione quando client e server nei due VPC hanno indirizzi IP sovrapposti perché AWS PrivateLink utilizza ENI all'interno del VPC client in modo da garantire che non vi siano conflitti IP con il provider di servizi. Puoi accedere agli AWS PrivateLink endpoint tramite peering VPC, VPN, Transit Gateway, Cloud WAN e. AWS Direct Connect
- Peering VPC e Transit Gateway: utilizza il peering VPC e il Transit Gateway quando desideri abilitare la connettività IP di livello 3 tra VPC.

  La tua architettura conterrà un mix di queste tecnologie per soddisfare diversi casi d'uso. Tutti questi servizi possono essere combinati e gestiti tra loro. Ad esempio, è necessario AWS PrivateLink gestire la connettività client-server in stile API, il peering VPC per gestire i requisiti di connettività diretta laddove i gruppi di posizionamento possano ancora essere desiderati all'interno della connettività regionale o interregionale e Transit Gateway per semplificare la connettività dei VPC su larga scala, nonché il consolidamento dell'edge per la connettività ibrida.

Condivisione VPC

La condivisione dei VPC è utile quando l'isolamento della rete tra i team non deve essere gestito in modo rigoroso dal proprietario del VPC, ma gli utenti e le autorizzazioni a livello di account devono esserlo. Con Shared VPC, più account AWS creano le proprie risorse applicative (come le istanze Amazon EC2) in Amazon VPC condivisi e gestiti centralmente. In questo modello, l'account proprietario del VPC (proprietario) condivide una o più sottoreti con altri account (partecipanti). Una volta condivisa una sottorete, i partecipanti possono visualizzare, creare, modificare ed eliminare le proprie risorse delle applicazioni nelle sottoreti condivise. Non possono invece visualizzare, modificare o eliminare le risorse che appartengono ad altri partecipanti o al proprietario del VPC. La sicurezza tra le risorse nei VPC condivisi viene gestita tramite gruppi di sicurezza, elenchi di controllo degli accessi alla rete (NAC) o tramite un firewall tra le sottoreti.

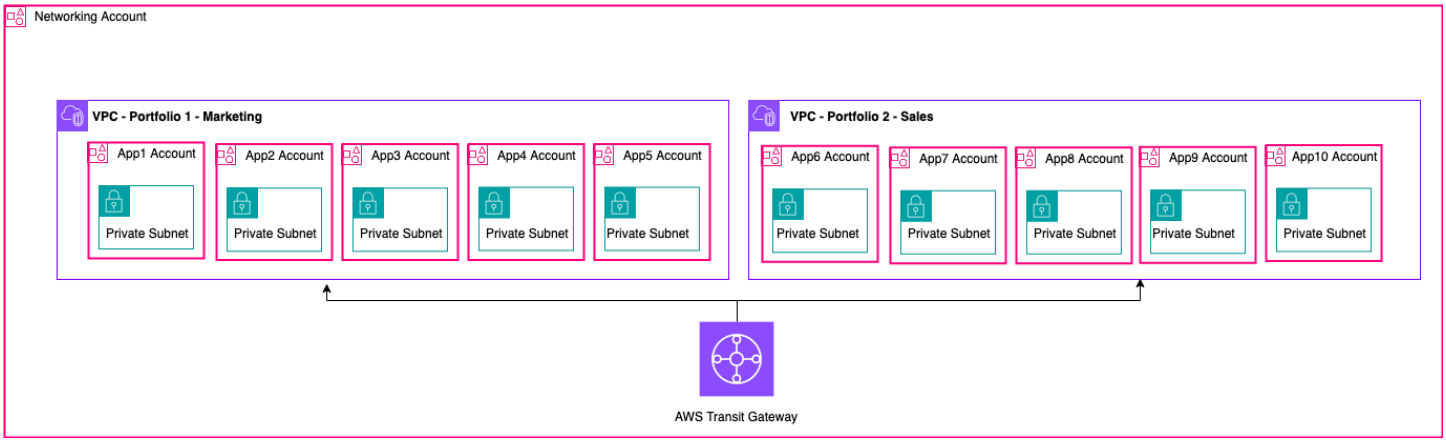
Vantaggi della condivisione VPC:

- Design semplificato: nessuna complessità relativa alla connettività tra VPC
- Meno VPC gestiti
- Separazione delle mansioni tra i team di rete e i proprietari delle applicazioni
- Migliore utilizzo degli indirizzi IPv4
- Costi inferiori: nessun costo di trasferimento dei dati tra istanze appartenenti a account diversi all'interno della stessa zona di disponibilità

> **Note**
>
> Quando condividi una sottorete con più account, i partecipanti dovrebbero avere un certo livello di collaborazione poiché condividono lo spazio IP e le risorse di rete. Se necessario, puoi scegliere di condividere una sottorete diversa per ogni account partecipante. Una sottorete per partecipante consente all'ACL di rete di fornire l'isolamento della rete oltre ai gruppi di sicurezza.

La maggior parte delle architetture dei clienti conterrà più VPC, molti dei quali verranno condivisi con due o più account. Transit Gateway e il peering VPC possono essere utilizzati per connettere i VPC condivisi. Ad esempio, supponiamo di avere 10 applicazioni. Ogni applicazione richiede il proprio account AWS. Le app possono essere classificate in due portafogli di applicazioni (le app all'interno dello stesso portafoglio hanno requisiti di rete simili, l'app da 1 a 5 in «Marketing» e l'app 6-10 in «Vendite»).

Puoi avere un VPC per portafoglio di applicazioni (due VPC in totale) e il VPC è condiviso con i diversi account del proprietario dell'applicazione all'interno di quel portafoglio. I proprietari delle app distribuiscono le app nei rispettivi VPC condivisi (in questo caso, nelle diverse sottoreti per la segmentazione e l'isolamento delle rotte di rete tramite NAC). I due VPC condivisi sono collegati tramite Transit Gateway. Con questa configurazione, potresti passare dalla necessità di connettere 10 VPC a solo due, come illustrato nella figura seguente.

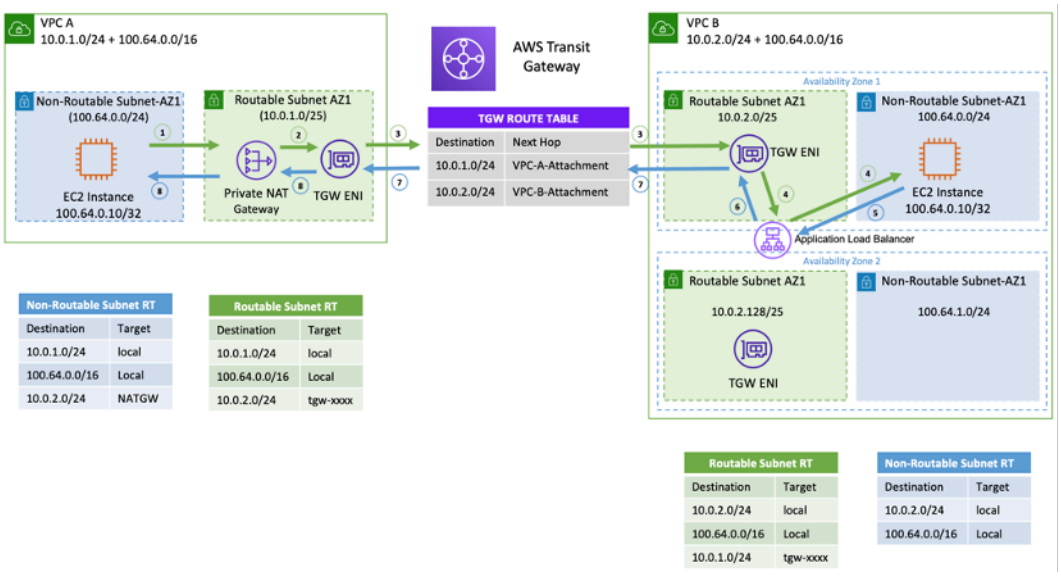


Esempio di configurazione: VPC condiviso

> **Note**
>
> I partecipanti alla condivisione VPC non possono creare tutte le risorse AWS in una sottorete condivisa. Per ulteriori informazioni, consulta la sezione Limitazioni nella documentazione sulla condivisione VPC.
> Per ulteriori informazioni sulle considerazioni chiave e sulle best practice per la condivisione di VPC, consulta il post sul blog Condivisione VPC: considerazioni chiave e best practice.

Gateway NAT privato

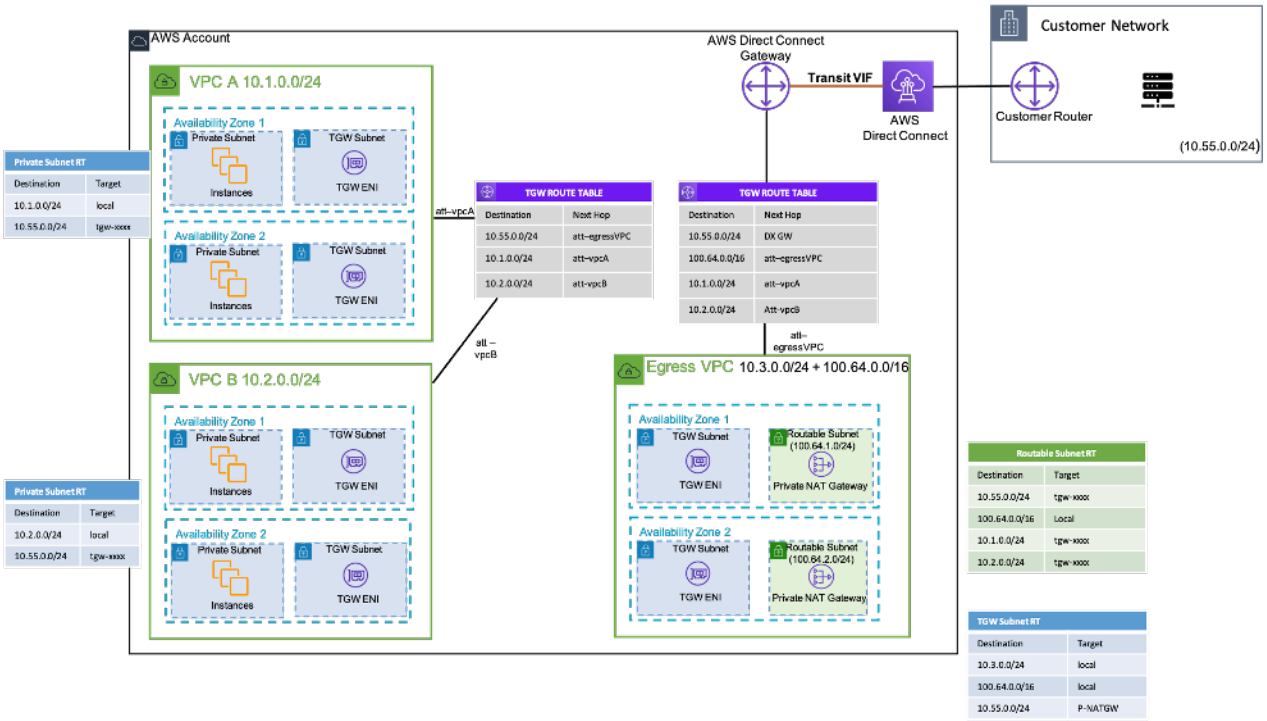
I team spesso lavorano in modo indipendente e possono creare un nuovo VPC per un progetto, che può avere blocchi CIDR (classless inter-domain routing) sovrapposti. Per quanto riguarda l'integrazione, potrebbero voler abilitare la comunicazione tra reti con CIDR sovrapposti, cosa che non è realizzabile tramite funzionalità come il peering VPC e il Transit Gateway. Un gateway NAT privato può essere utile in questo caso d'uso. Il gateway NAT privato utilizza un indirizzo IP privato univoco per eseguire il NAT di origine per l'indirizzo IP di origine sovrapposto, mentre ELB esegue il NAT di destinazione per l'indirizzo IP di destinazione sovrapposto. Puoi indirizzare il traffico dal tuo gateway NAT privato ad altri VPC o reti locali utilizzando Transit Gateway o un gateway privato virtuale.



Esempio di configurazione: gateway NAT privato

La figura precedente mostra due sottoreti non instradabili (CIDR sovrapposti) in VPC A e B. Per stabilire una connessione tra loro, è possibile aggiungere CIDR secondari non sovrapposti/instradabili (`100.64.0.0/16`sottoreti instradabili e) a VPC A e B, rispettivamente. `10.0.1.0/24` `10.0.2.0/24` I CIDR routabili devono essere allocati dal team di gestione della rete responsabile dell'allocazione IP. Un gateway NAT privato viene aggiunto alla sottorete instradabile in VPC A con un indirizzo IP di. `10.0.1.125` Il gateway NAT privato esegue la traduzione degli indirizzi di rete di origine su richieste provenienti da istanze nella sottorete non instradabile di VPC A (`100.64.0.10`) come `10.0.1.125` l'ENI del gateway NAT privato. Ora il traffico può essere indirizzato a un indirizzo IP instradabile assegnato all'Application Load Balancer (ALB) in VPC B `10.0.2.10` (), che ha una destinazione di. `100.64.0.10` Il traffico viene instradato attraverso Transit Gateway. Il traffico di ritorno viene elaborato dal gateway NAT privato fino all'istanza Amazon EC2 originale che richiede la connessione.

Il gateway NAT privato può essere utilizzato anche quando la rete locale limita l'accesso agli IP approvati. Le reti locali di pochi clienti sono tenute per conformità a comunicare solo con reti private (senza IGW) solo attraverso un blocco contiguo limitato di IP approvati di proprietà del cliente. Invece di assegnare a ogni istanza un IP separato dal blocco, è possibile eseguire carichi di lavoro di grandi dimensioni su AWS VPC dietro ogni IP consentito utilizzando un gateway NAT privato. Per i dettagli, consulta il post di blog Come risolvere l'esaurimento dell'IP privato con la soluzione NAT privata.



Esempio di configurazione: come utilizzare un gateway NAT privato per fornire IP approvati per la rete locale

AWS WAN nel cloud

AWS Cloud WAN è un nuovo modo di connettere le reti tra loro che in precedenza potevamo fare con Transit Gateway, VPC Peering e tunnel VPN IPSEC. In precedenza, dovevi configurare uno o più VPC, collegarli tra loro con uno dei metodi precedenti e utilizzare IPSEC VPN o connetterti a reti locali. AWS Direct Connect I costrutti di rete e di sicurezza sarebbero definiti in un posto e le reti in un altro. Cloud WAN ti consente di centralizzare tutti questi costrutti in un unico posto. In base alle policy, è possibile segmentare le reti per determinare chi può parlare con chi e isolare il traffico di produzione attraverso questi segmenti dai carichi di lavoro di sviluppo o test o dalle reti locali.

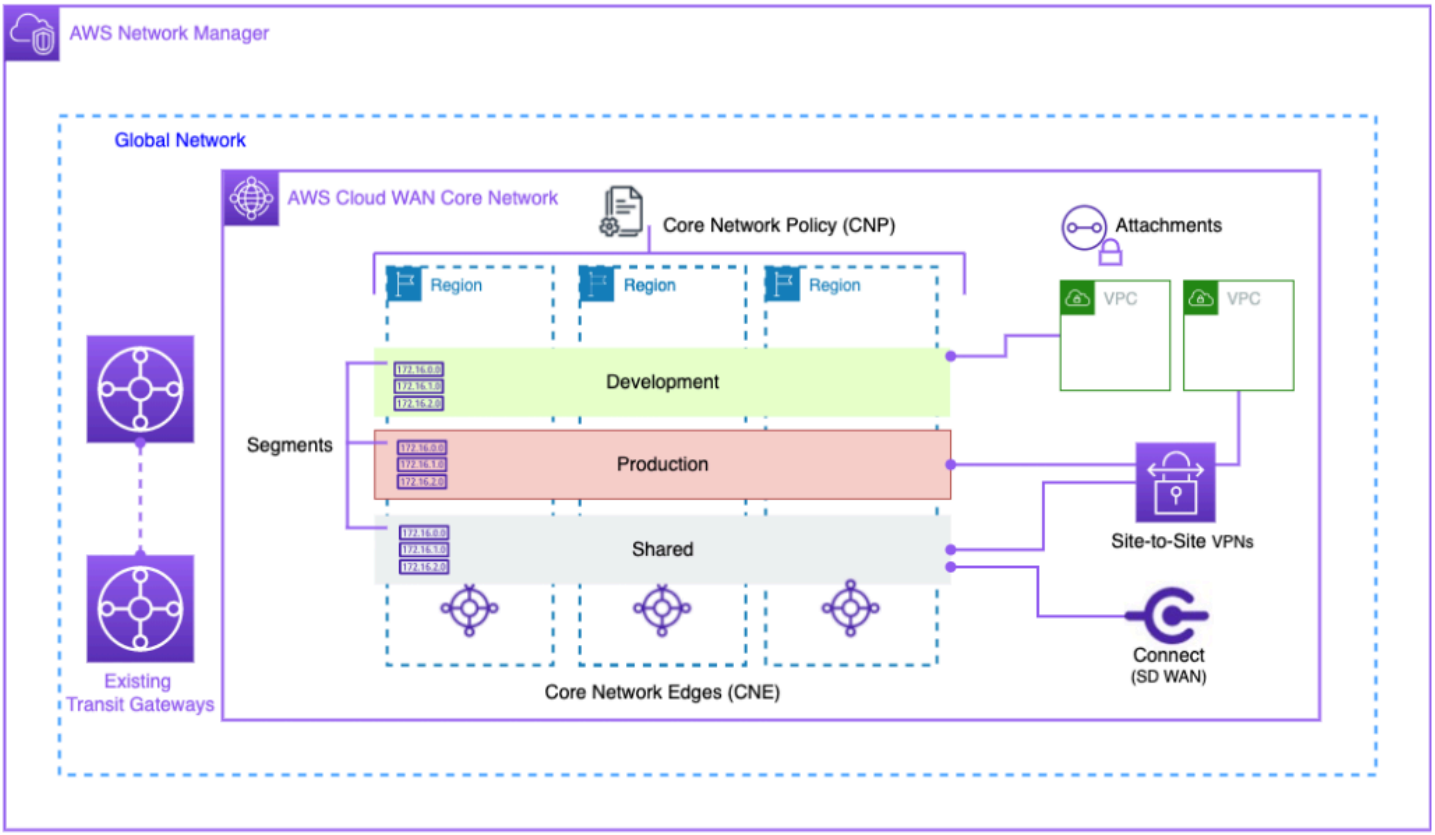


Diagramma a blocchi di Cloud WAN

Gestisci la tua rete globale tramite l'interfaccia utente e le API di AWS Network Manager. La rete globale è il contenitore a livello di root per tutti gli oggetti di rete; la rete centrale è la parte della rete globale gestita da AWS. Una politica di rete principale (CNP) è un documento di policy in un'unica versione che definisce tutti gli aspetti della rete principale. Gli allegati sono tutte le connessioni o le risorse che desideri aggiungere alla tua rete principale. Un core network edge (CNE) è un punto di connessione locale per gli allegati conformi alla policy. I segmenti di rete sono domini di routing che, per impostazione predefinita, consentono la comunicazione solo all'interno di un segmento.

Per usare CloudWAN:

1. In AWS Network Manager, crea una rete globale e una rete centrale associata.
2. Crea un CNP che definisca i segmenti, l'intervallo ASN Regioni AWS e i tag da utilizzare per il collegamento ai segmenti.
3. Applica la politica di rete.
4. Condividi la rete principale con utenti, account o organizzazioni utilizzando il gestore degli accessi alle risorse.

5. Crea e contrassegna gli allegati.
6. Aggiorna i percorsi nei tuoi VPC collegati per includere la rete principale.

Cloud WAN è stato progettato per semplificare il processo di connessione dell'infrastruttura AWS a livello globale. Ti consente di segmentare il traffico con una politica di autorizzazioni centralizzata e di utilizzare l'infrastruttura esistente nelle sedi aziendali. Cloud WAN collega anche VPC, SD-WAN, Client VPN, firewall, VPN e risorse del data center per connettersi a Cloud WAN. Per ulteriori informazioni, consulta i post del blog AWS Cloud WAN.

AWS Cloud WAN consente una rete unificata che collega ambienti cloud e locali. Organizations utilizza firewall di nuova generazione (NGFW) e sistemi di prevenzione delle intrusioni (IPS) per la sicurezza. Il post sul blog sui modelli di migrazione e interoperabilità di AWS Cloud WAN e Transit Gateway descrive i modelli architettonici per la gestione e l'ispezione centralizzata del traffico di rete in uscita in una rete WAN cloud, incluse reti a regione singola e multiregione, e configura le tabelle di routing. Queste architetture garantiscono la sicurezza di dati e applicazioni pur mantenendo un ambiente cloud sicuro.

Per ulteriori informazioni su Cloud WAN, consulta il post sul blog Centralized Outbound Inspection Architecture in AWS Cloud WAN.

Amazon VPC Lattice

Amazon VPC Lattice è un servizio di rete di applicazioni completamente gestito che viene utilizzato per connettere, monitorare e proteggere i servizi su vari account e cloud privati virtuali. VPC Lattice aiuta a interconnettere i servizi all'interno di un limite logico, in modo da poterli gestire e scoprire in modo efficiente.

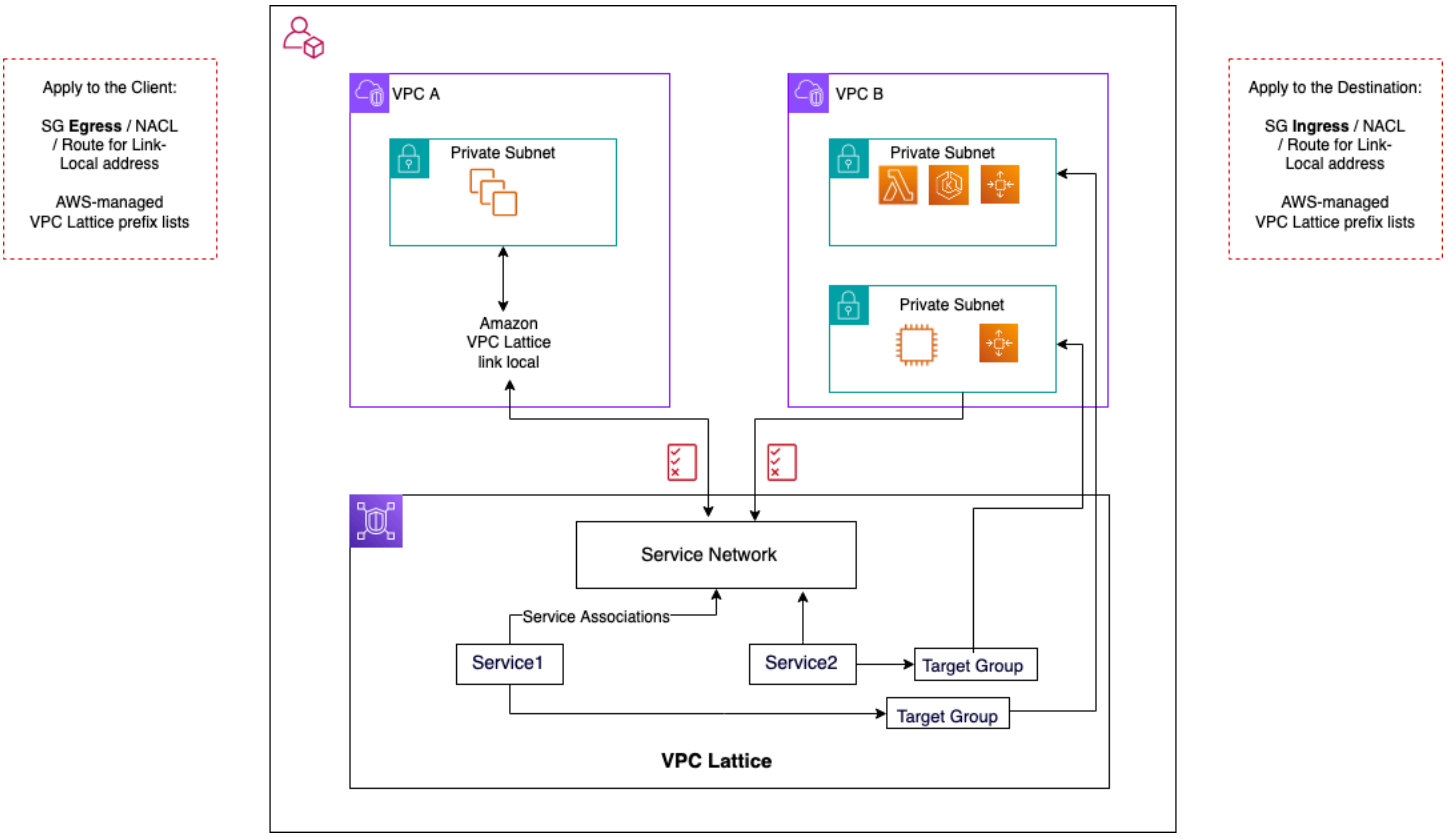
I componenti VPC Lattice sono costituiti da:

- Servizio: si tratta di un'unità di applicazione in esecuzione su un'istanza, un contenitore o una funzione Lambda ed è composta da ascoltatori, regole e gruppi target.
- Rete di servizi: questo è il limite logico utilizzato per implementare automaticamente il rilevamento e la connettività dei servizi e applicare politiche comuni di accesso e osservabilità a una raccolta di servizi.
- Politiche di autenticazione: politiche delle risorse IAM che possono essere associate a una rete di servizi o a singoli servizi per supportare l'autenticazione a livello di richiesta e l'autorizzazione specifica del contesto.

- Service Directory: una visualizzazione centralizzata dei servizi che possiedi o che sono stati condivisi con te tramite AWS Resource Access Manager.

Fasi di utilizzo di VPC Lattice:

1. Crea la rete di servizi. La rete di assistenza di solito risiede su un account di rete a cui un amministratore di rete ha pieno accesso. La rete di servizi può essere condivisa tra più account all'interno di un'organizzazione. La condivisione può essere eseguita su singoli servizi o sull'intero account di servizio.
2. Collega i VPC alla rete di servizi per abilitare il networking delle applicazioni per ogni VPC, in modo che servizi diversi possano iniziare a utilizzare altri servizi registrati all'interno della rete. I gruppi di sicurezza vengono applicati per controllare il traffico.
3. Gli sviluppatori definiscono i servizi, che vengono inseriti nell'elenco dei servizi e registrati nella rete di servizi. VPC Lattice contiene la rubrica di tutti i servizi configurati. Gli sviluppatori possono anche definire politiche di routing per utilizzare implementazioni blu/verdi. La sicurezza viene gestita a livello di rete di servizio, dove vengono definite le politiche di autenticazione e autorizzazione, e a livello di servizio in cui vengono implementate le politiche di accesso con IAM.



Flussi di comunicazione VPC Lattice

Maggiori dettagli sono disponibili nella guida per l'utente di VPC Lattice.

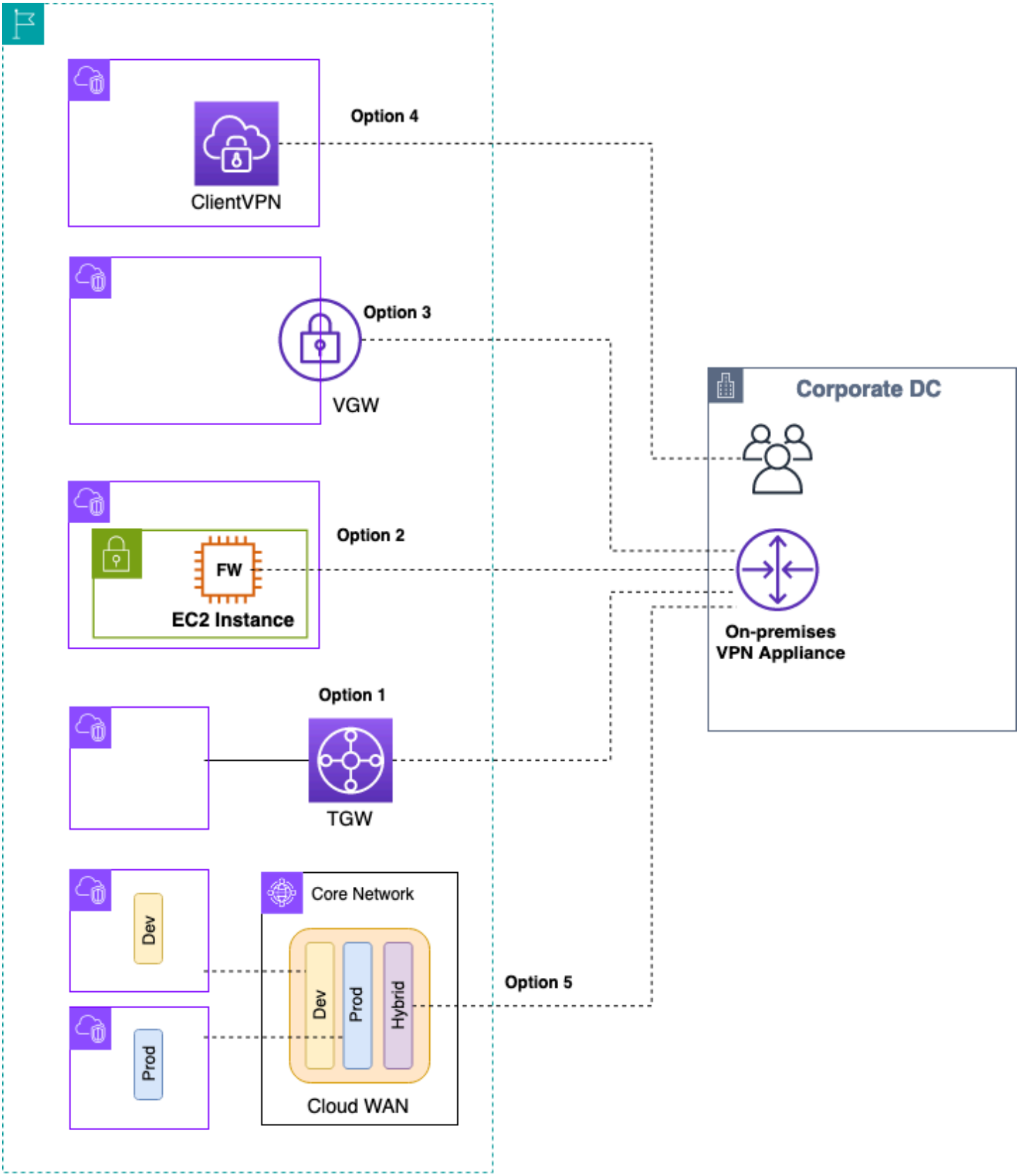
Connettività ibrida

Questa sezione si concentra sulla connessione sicura delle risorse cloud con i data center locali. Esistono tre approcci per abilitare la connettività ibrida:

- ne-to-one Connettività O: in questa configurazione, viene creata una connessione VPN e/o una VIF privata Direct Connect per ogni VPC. Ciò si ottiene utilizzando il gateway privato virtuale (VGW). Questa opzione è ideale per un numero limitato di VPC, ma man mano che un cliente ridimensiona i propri VPC, la gestione della connettività ibrida per VPC può diventare difficile.
- Consolidamento dell'edge: in questa configurazione, i clienti consolidano la connettività IT ibrida per più VPC su un unico endpoint. Tutti i VPC condividono queste connessioni ibride. Ciò si ottiene utilizzando AWS Transit Gateway e il AWS Direct Connect gateway.
- Consolidamento ibrido full mesh: in questa configurazione, i clienti consolidano la connettività per più VPC su un singolo endpoint utilizzando CloudWAN, integrato. AWS Transit Gateway Si tratta di un approccio completamente basato su policy al networking in uno o più account AWS, rappresentati in codice. Al momento, l'utilizzo AWS Direct Connect per la connettività edge richiede il peering del Transit Gateway su CloudWAN.

VPN

Esistono vari modi per configurare una VPN su AWS:



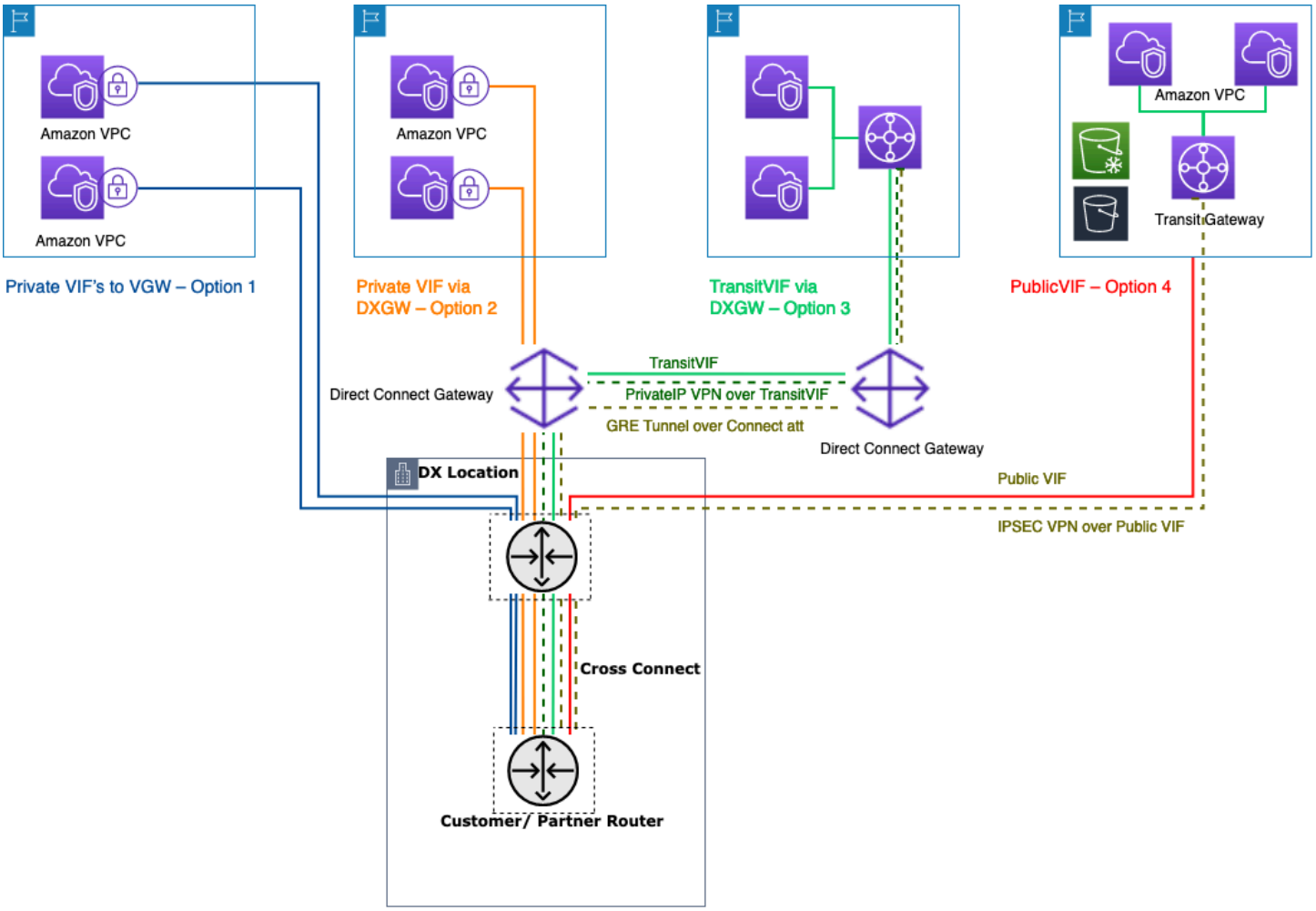
AWS VPN opzioni

- Opzione 1: consolidamento della connettività VPN su Transit Gateway: questa opzione sfrutta l'allegato Transit Gateway VPN su Transit Gateway. Transit Gateway supporta la terminazione IPSec per site-to-site VPN. I clienti possono creare tunnel VPN verso il Transit Gateway e accedere ai VPC ad esso collegati. Transit Gateway supporta connessioni VPN dinamiche statiche e basate su BGP. Transit Gateway supporta anche Equal-Cost Multi-Path (ECMP) sugli allegati VPN. Ogni connessione VPN ha un throughput massimo di 1,25 Gbps per tunnel. L'abilitazione dell'ECMP consente di aggregare la velocità effettiva tra le connessioni VPN, permettendo una scalabilità oltre il limite massimo predefinito di 1,25 Gbps. In questa opzione, paghi sia i prezzi del Transit Gateway che i AWS VPN prezzi. AWS consiglia di utilizzare questa opzione per la connettività VPN. Per ulteriori informazioni, consulta il post sul blog Scaling VPN throughput using AWS Transit Gateway.
- Opzione 2: terminare la VPN su un'istanza Amazon EC2: questa opzione viene sfruttata dai clienti nei casi limite, quando desiderano un particolare set di funzionalità software del fornitore (come Cisco DMVPN o Generic Routing Encapsulation (GRE)) o desiderano coerenza operativa tra varie implementazioni VPN. È possibile utilizzare il design VPC di transito per il consolidamento dell'edge, ma è importante ricordare che tutte le considerazioni chiave della sezione relativa al VPC di transito sono applicabili alla Connettività da VPC a VPC connettività VPN ibrida. Sei responsabile della gestione dell'alta disponibilità e paghi per l'istanza EC2 oltre ai costi di licenza e supporto del software di qualsiasi fornitore.
- Opzione 3: terminazione della VPN su un gateway privato virtuale (VGW): questa opzione di servizio VPN da sito a sito di AWS consente one-to-one un design di connettività in cui si crea una connessione VPN (costituita da un paio di tunnel VPN ridondanti) per VPC. Questo è un ottimo modo per iniziare a utilizzare la connettività VPN in AWS, ma man mano che si aumenta il numero di VPC, la gestione di un numero crescente di connessioni VPN può diventare difficile. Pertanto, la progettazione di consolidamento dell'edge che sfrutta Transit Gateway alla fine sarà un'opzione migliore. Il throughput VPN su un VGW è limitato a 1,25 Gbps per tunnel e il bilanciamento del carico ECMP non è supportato. Dal punto di vista dei prezzi, paghi solo i prezzi di AWS VPN, non ci sono costi per l'esecuzione di un VGW. Per ulteriori informazioni, consulta le sezioni AWS VPN Prezzi e AWS VPN Virtual Private Gateway.
- Opzione 4: terminare la connessione VPN sull'endpoint VPN client: AWS Client VPN è un servizio VPN gestito basato su client che consente di accedere in modo sicuro alle risorse AWS e alle risorse nella rete locale. Con Client VPN, puoi accedere alle tue risorse da qualsiasi luogo utilizzando un client VPN OpenVPN o fornito da AWS. Configurando un endpoint Client VPN, i client e gli utenti possono connettersi per stabilire una connessione VPN Transport Layer Security (TLS). Per ulteriori informazioni, consulta la documentazione di AWS Client VPN.

- Opzione 5: Consolidamento della connessione VPN su AWS Cloud WAN: questa opzione è simile alla prima opzione in questo elenco, ma utilizza la struttura CloudWAN per configurare a livello di codice le connessioni VPN tramite il documento di policy di rete.

AWS Direct Connect

Sebbene la VPN su Internet sia un'ottima opzione per iniziare, la connettività Internet potrebbe non essere affidabile per il traffico di produzione. A causa di questa inaffidabilità, molti clienti scelgono AWS Direct Connect. AWS Direct Connect è un servizio di rete che fornisce un'alternativa all'utilizzo di Internet per connettersi ad AWS. Utilizzando AWS Direct Connect, i dati che in precedenza sarebbero stati trasportati su Internet vengono forniti tramite una connessione di rete privata tra le tue strutture e AWS. In molte circostanze, le connessioni di rete private possono ridurre i costi, aumentare la larghezza di banda e fornire un'esperienza di rete più coerente rispetto alle connessioni basate su Internet. Esistono diversi modi per connettersi AWS Direct Connect ai VPC:



Metodi per connettere i data center locali utilizzando AWS Direct Connect

- Opzione 1: creazione di un'interfaccia virtuale privata (VIF) a un VGW collegato a un VPC: è possibile creare 50 VIF per connessione Direct Connect, che consentono di connettersi a un massimo di 50 VPC (un VIF fornisce la connettività a un VPC). Esiste un peering BGP per VPC. La connettività in questa configurazione è limitata alla regione AWS in cui è ospitata la sede Direct Connect. La one-to-one mappatura di VIF su VPC (e la mancanza di accesso globale) rendono questo il modo meno preferito per accedere ai VPC nella Landing Zone.
- Opzione 2: creare un VIF privato su un gateway Direct Connect associato a più VGW (ogni VGW è collegato a un VPC) — Un gateway Direct Connect è una risorsa disponibile a livello globale. Puoi creare il gateway Direct Connect in qualsiasi regione e accedervi da tutte le altre regioni, inclusa GovCloud (esclusa la Cina). Un gateway Direct Connect può connettersi a un massimo di 20 VPC (tramite VGW) a livello globale in qualsiasi account AWS tramite un'unica VIF privata. Questa è un'ottima opzione se una Landing Zone è composta da un numero limitato di VPC (dieci o meno VPC) e/o è necessario un accesso globale. Esiste una sessione di peering BGP per Direct Connect Gateway per connessione Direct Connect. Il gateway Direct Connect è destinato esclusivamente al flusso di traffico nord/sud e non consente la connettività da VPC a VPC. Per maggiori dettagli, consulta Virtual Private Gateway Associations nella documentazione. AWS Direct Connect Con questa opzione, la connettività non è limitata alla regione AWS in cui si trova la sede Direct Connect. AWS Direct Connect il gateway è solo per il flusso di traffico nord/sud e non consente la connettività da VPC a VPC. Un'eccezione a questa regola è quando una supernet viene pubblicizzata su due o più VPC i cui VGW collegati sono associati allo stesso gateway e sulla stessa interfaccia virtuale. AWS Direct Connect In questo caso, i VPC possono comunicare tra loro tramite l'endpoint. AWS Direct Connect Per maggiori dettagli, consulta la documentazione dei AWS Direct Connect gateway.
- Opzione 3: creazione di un transito VIF a un gateway Direct Connect associato a Transit Gateway: è possibile associare un'istanza Transit Gateway a un gateway Direct Connect utilizzando un Transit VIF. AWS Direct Connect ora supporta le connessioni a Transit Gateway per tutte le velocità di porta, offrendo una scelta più economica per gli utenti di Transit Gateway quando non sono richieste connessioni ad alta velocità (superiori a 1 Gbps). Ciò consente di utilizzare Direct Connect a velocità di 50, 100, 200, 300, 400 e 500 Mbps connettendosi al Transit Gateway. Transit VIF ti consente di connettere il tuo data center locale a un massimo di sei istanze Transit Gateway per AWS Direct Connect gateway (che possono connettersi a migliaia di VPC) tra diverse regioni AWS e account AWS tramite peering VIF e BGP a transito singolo. Questa è la configurazione più semplice tra le opzioni per connettere più VPC su larga scala, ma dovresti prestare attenzione alle quote Transit Gateway. Un limite fondamentale da tenere presente è che è possibile pubblicizzare

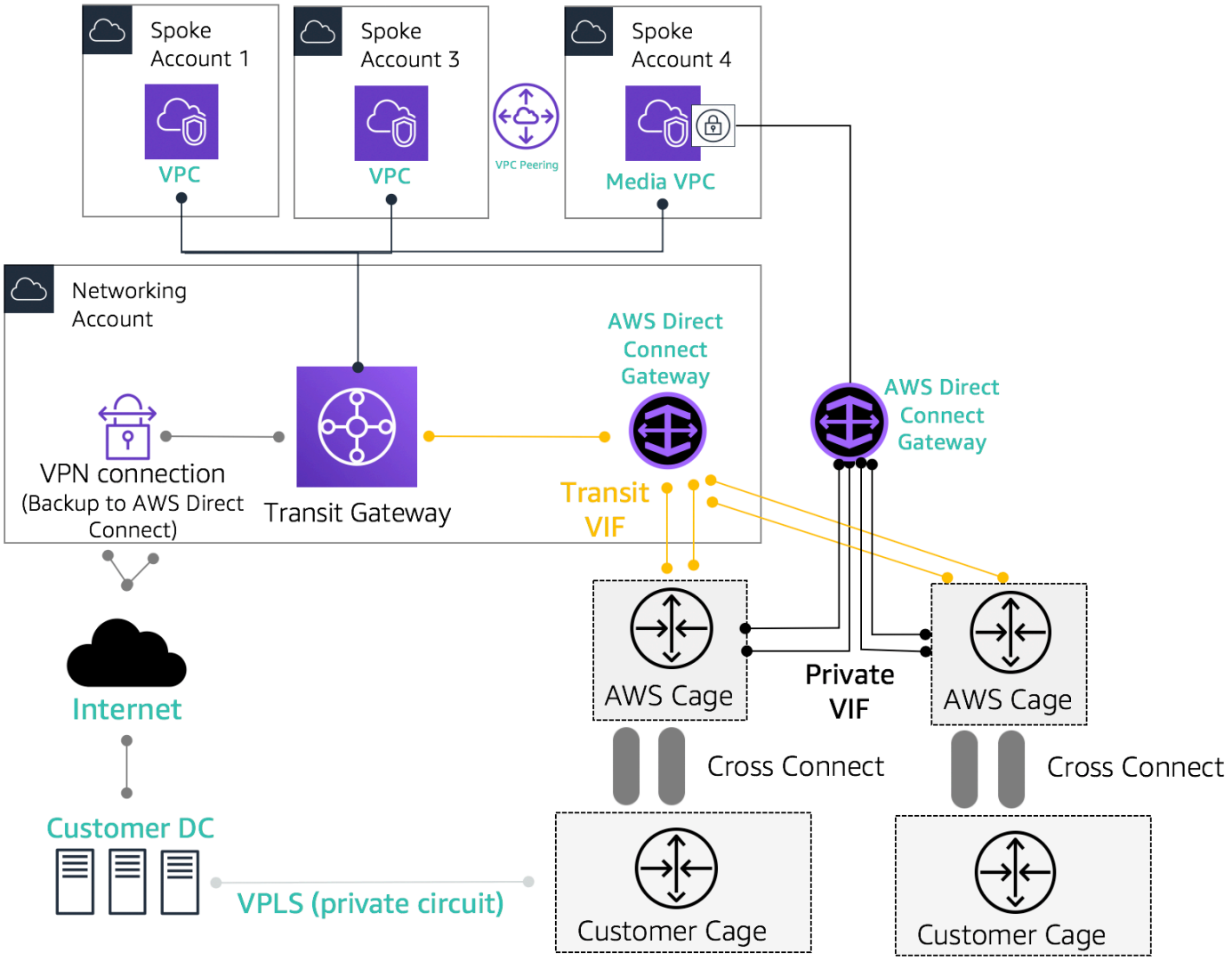
solo 200 prefissi da un Transit Gateway a un router locale tramite il Transit VIF. Con le opzioni precedenti, paghi i prezzi di Direct Connect. Per questa opzione, paghi anche i costi per gli allegati e l'elaborazione dei dati del Transit Gateway. Per ulteriori informazioni, consulta la documentazione Transit Gateway Associations on Direct Connect.

- Opzione 4: creare una connessione VPN a Transit Gateway tramite DIRECT Connect public VIF: un VIF pubblico consente di accedere a tutti i servizi pubblici e gli endpoint AWS utilizzando gli indirizzi IP pubblici. Quando crei un allegato VPN su un Transit Gateway, ottieni due indirizzi IP pubblici per gli endpoint VPN sul lato AWS. Questi IP pubblici sono raggiungibili tramite il VIF pubblico. Puoi creare tutte le connessioni VPN a tutte le istanze Transit Gateway che desideri tramite Public VIF. Quando crei un peering BGP sul VIF pubblico, AWS pubblicizza l'intero intervallo di IP pubblici di AWS sul tuo router. Per assicurarti di consentire solo un determinato traffico (ad esempio, consentire il traffico solo verso gli endpoint di terminazione VPN), ti consigliamo di utilizzare un firewall locale. Questa opzione può essere utilizzata per crittografare Direct Connect a livello di rete.
- Opzione 5: creazione di una connessione VPN a Transit Gateway AWS Direct Connect tramite VPN IP privata — Private IP VPN è una funzionalità che offre ai clienti la possibilità di distribuire connessioni VPN da sito a sito AWS tramite Direct Connect utilizzando indirizzi IP privati. Con questa funzionalità, puoi crittografare il traffico tra le tue reti locali e AWS tramite connessioni Direct Connect senza la necessità di indirizzi IP pubblici, migliorando così la sicurezza e la privacy della rete allo stesso tempo. Private IP VPN viene implementata in aggiunta ai Transit VIF, quindi consente di utilizzare Transit Gateway per la gestione centralizzata dei VPC dei clienti e delle connessioni alle reti locali in modo più sicuro, privato e scalabile.
- Opzione 6: creazione di tunnel GRE verso Transit Gateway tramite un VIF di transito: il tipo di allegato Transit Gateway Connect supporta GRE. Con Transit Gateway Connect, l'infrastruttura SD-WAN può essere connessa nativamente ad AWS senza dover configurare VPN IPSec tra le appliance virtuali di rete SD-WAN e Transit Gateway. I tunnel GRE possono essere stabiliti su un VIF di transito, con Transit Gateway Connect come tipo di allegato, che offre prestazioni di larghezza di banda più elevate rispetto a una connessione VPN. Per ulteriori informazioni, consulta il post sul blog Simplify SD-WAN connectivity with AWS Transit Gateway Connect.

L'opzione «transit VIF to Direct Connect gateway» potrebbe sembrare l'opzione migliore perché consente di consolidare tutta la connettività locale per un determinato Regione AWS punto (Transit Gateway) utilizzando una singola sessione BGP per connessione Direct Connect; tuttavia, alcuni limiti e considerazioni relativi a questa opzione potrebbero indurvi a utilizzare sia i VIF privati che quelli di transito in combinazione per i requisiti di connettività della Landing Zone.

La figura seguente illustra una configurazione di esempio in cui Transit VIF viene utilizzato come metodo predefinito per la connessione ai VPC e un VIF privato viene utilizzato per un caso d'uso periferico in cui è necessario trasferire quantità eccezionalmente elevate di dati da un data center locale al VPC multimediale. Il formato VIF privato viene utilizzato per evitare i costi di elaborazione dei dati del Transit Gateway. È consigliabile disporre di almeno due connessioni in due diverse postazioni Direct Connect per la massima ridondanza, per un totale di quattro connessioni. È possibile creare un VIF per connessione per un totale di quattro VIF privati e quattro VIF di transito. È inoltre possibile creare una VPN come connettività di backup per le connessioni. AWS Direct Connect

Con l'opzione «Create GRE tunnels to Transit Gateway over a transit VIF», ottieni la capacità di connettere nativamente la tua infrastruttura SD-WAN con AWS. Elimina la necessità di configurare VPN IPSec tra le appliance virtuali di rete SD-WAN e Transit Gateway.



Architettura di riferimento di esempio per la connettività ibrida

Utilizzate l'account Network Services per creare risorse Direct Connect che consentano la demarcazione dei confini amministrativi della rete. Le connessioni Direct Connect, i gateway Direct Connect e i gateway di transito possono risiedere tutti in un account di servizi di rete. Per condividere la AWS Direct Connect connettività con la tua Landing Zone, condividi semplicemente il Transit Gateway AWS RAM con altri account.

Sicurezza MacSec sulle connessioni Direct Connect

I clienti possono utilizzare la crittografia MAC Security Standard (MACSec) (IEEE 802.1AE) con le loro connessioni Direct Connect per connessioni dedicate da 10 Gbps e 100 Gbps in località selezionate. Con questa funzionalità, i clienti possono proteggere i propri dati a livello 2 e Direct Connect offre point-to-point la crittografia. Per abilitare la funzione Direct Connect MacSec, assicurati che i prerequisiti MacSec siano soddisfatti. Poiché MacSec protegge i collegamenti su hop-by-hop base regolare, il dispositivo deve avere un'adiacenza diretta di livello 2 con il nostro dispositivo Direct Connect. Il tuo provider dell'ultimo miglio può aiutarti a verificare che la tua connessione funzioni con MacSec. Per ulteriori informazioni, consulta Aggiungere la sicurezza MacSec alle connessioni AWS Direct Connect.

AWS Direct Connect raccomandazioni sulla resilienza

Con AWS Direct Connect, i clienti possono ottenere una connettività altamente resiliente nelle loro risorse Amazon VPC e AWS dalle loro reti locali. È buona prassi che i clienti si connettano da più data center per eliminare eventuali guasti alle ubicazioni fisiche a singolo punto. Si consiglia inoltre che, a seconda del tipo di carico di lavoro, i clienti utilizzino più di una connessione Direct Connect per la ridondanza.

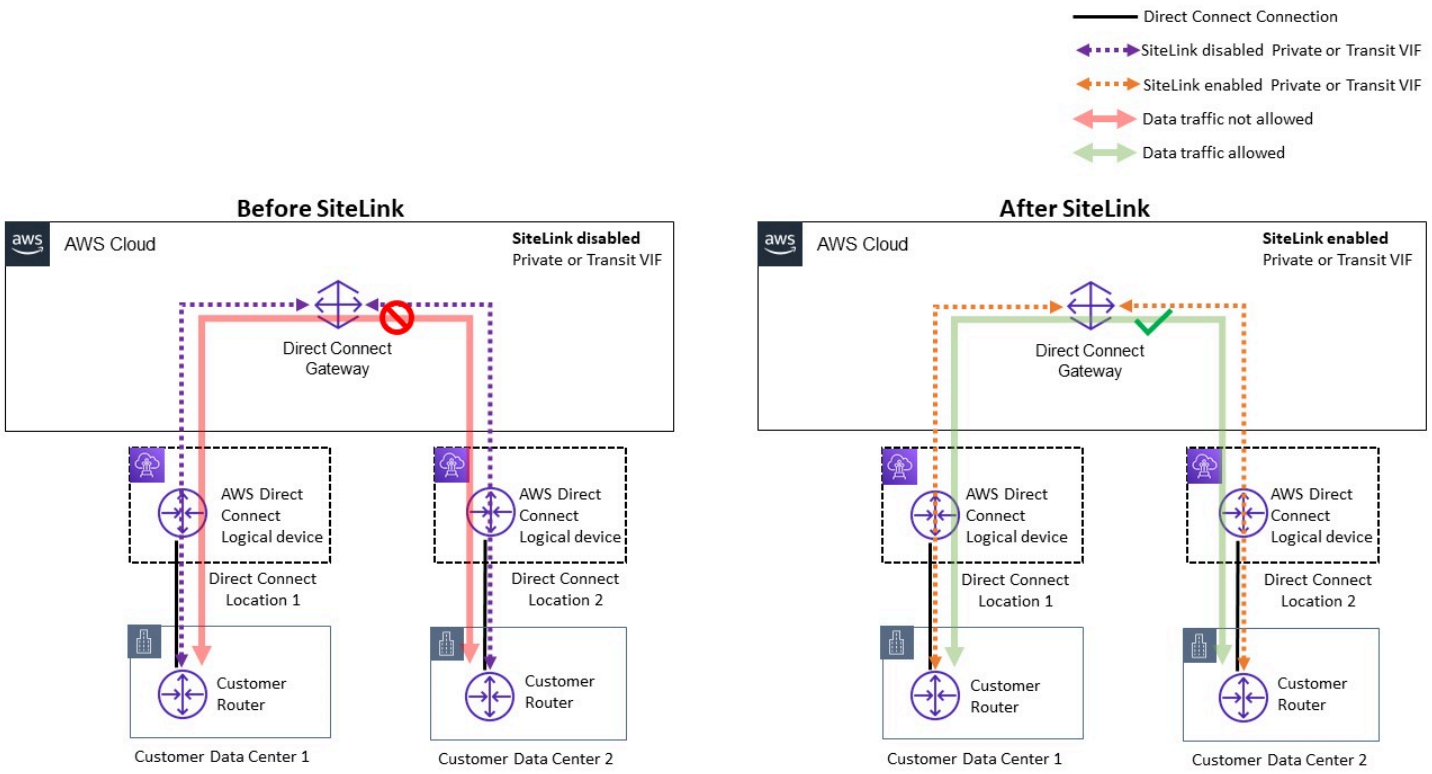
AWS offre anche il AWS Direct Connect Resiliency Toolkit, che fornisce ai clienti una procedura guidata di connessione con più modelli di ridondanza, per aiutarli a determinare quale modello funziona meglio per i loro requisiti di accordo sul livello di servizio (SLA) e a progettare di conseguenza la loro connettività ibrida utilizzando le connessioni Direct Connect. Per ulteriori informazioni, consulta la sezione Raccomandazioni sulla resilienza.AWS Direct Connect

AWS Direct Connect SiteLink

In precedenza, la configurazione dei site-to-site collegamenti per le reti locali era possibile solo utilizzando la tecnologia Direct Circuit Buildout tramite Dark Fiber o altre tecnologie, VPN IPSEC o utilizzando fornitori di circuiti di terze parti con tecnologie come MPLS o circuiti T1 legacy. MetroEthernet Con l'avvento di SiteLink, i clienti possono ora abilitare la connettività diretta per le

proprie sedi locali che terminano in una località. site-to-site AWS Direct Connect Usa il tuo circuito Direct Connect per fornire site-to-site connettività senza dover instradare il traffico attraverso i tuoi VPC, aggirando completamente la regione AWS.

Ora puoi creare pay-as-you-go connessioni globali, affidabili e affidabili tra gli uffici e i data center della tua rete globale inviando i dati lungo il percorso più veloce tra AWS Direct Connect le sedi.

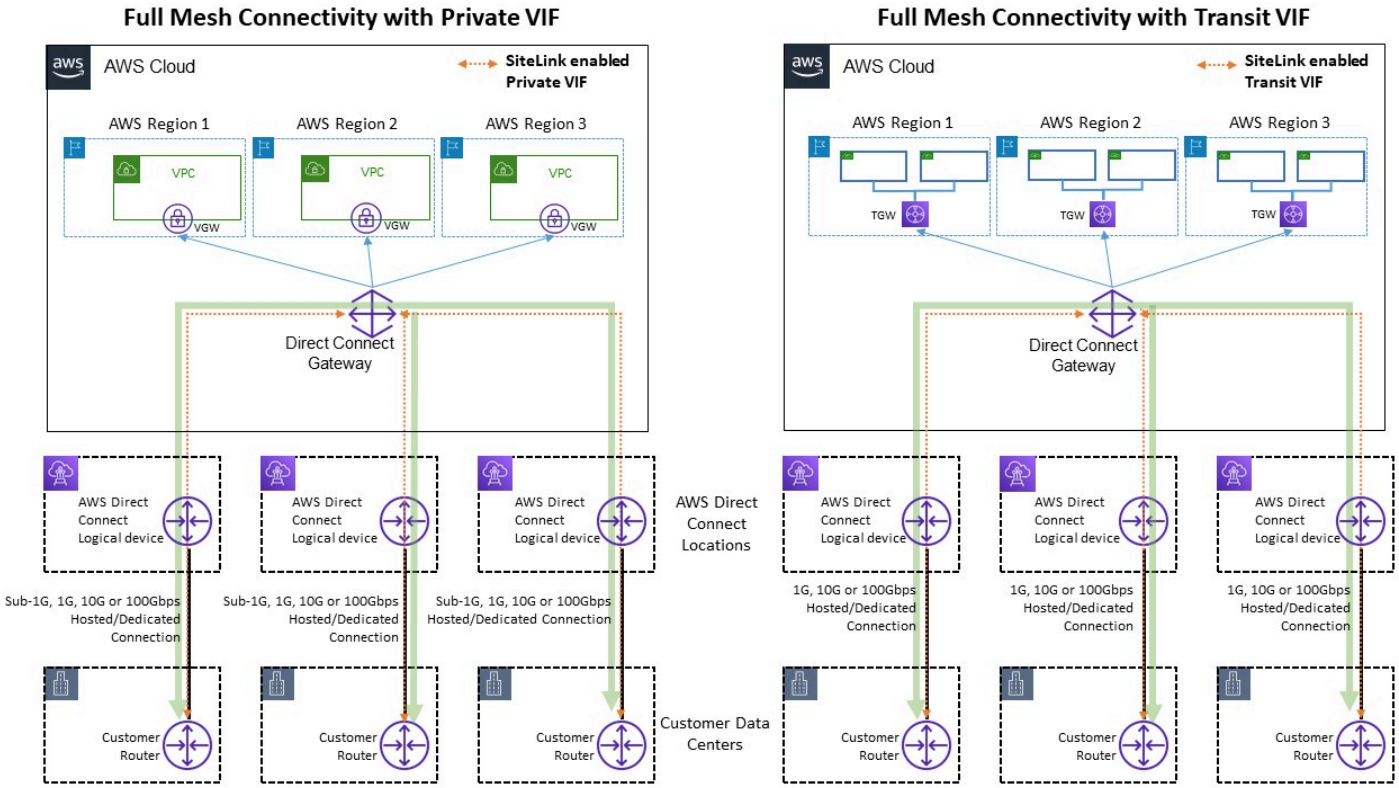


Architettura di riferimento di esempio per AWS Direct Connect SiteLink

Al momento dell'utilizzo SiteLink, devi prima connettere le tue reti locali ad AWS in una delle oltre 100 AWS Direct Connect sedi in tutto il mondo. Quindi, crei interfacce virtuali (VIF) su tali connessioni e abiliti. SiteLink Una volta che tutti i VIF sono collegati allo stesso AWS Direct Connect gateway (DXGW), puoi iniziare a inviare dati tra di loro. I tuoi dati seguono il percorso più breve tra le AWS Direct Connect ubicazioni e la destinazione, utilizzando la rete globale AWS veloce, sicura e affidabile. Non è necessario disporre di alcuna risorsa Regione AWS da utilizzare SiteLink.

Con SiteLink, il DXGW impara i prefissi IPv4/IPv6 dai router tramite VIF SiteLink abilitati, esegue l'algoritmo BGP best path, aggiorna attributi come NextHop e AS_Path e pubblicizza nuovamente questi prefissi BGP sul resto dei file VIF abilitati a quel DXGW. SiteLink Se si disattiva SiteLink su un VIF, DXGW non pubblicizzerà i prefissi locali appresi su questo VIF SiteLink agli altri VIF abilitati. I prefissi locali di un VIF SiteLink disabilitato vengono pubblicizzati solo alle associazioni

DXGW Gateway, come le istanze AWS Virtual Private Gateways (VGWS) o Transit Gateway (TGW) associate a DXGW.



Sitelink consente un esempio di flussi di traffico

SiteLink consente ai clienti di utilizzare la rete globale AWS per funzionare come connessione primaria o secondaria/di backup tra le loro postazioni remote, con larghezza di banda elevata e bassa latenza, con routing dinamico per controllare quali postazioni possono comunicare tra loro e con le risorse regionali AWS.

Per ulteriori informazioni, consulta Introducing. AWS Direct Connect SiteLink

Uscita centralizzata verso Internet

Quando distribuisci applicazioni in un ambiente con più account, molte app richiederanno l'accesso a Internet solo in uscita (ad esempio, il download di librerie, patch o aggiornamenti del sistema operativo). Ciò può essere ottenuto sia per il traffico che per il traffico. IPv4 IPv6 Ciò può essere ottenuto tramite la traduzione degli indirizzi di rete (NAT) sotto forma di NAT gateway (consigliato) o, in alternativa, un'NATistanza autogestita in esecuzione su un'istanza AmazonEC2, come mezzo per l'accesso a Internet da tutte le uscite. IPv4 Le applicazioni interne risiedono in sottoreti private, mentre i NAT gateway e le istanze EC2 NAT Amazon risiedono in una sottorete pubblica.

AWSconsiglia di utilizzare i NAT gateway perché offrono disponibilità e larghezza di banda migliori e richiedono meno sforzi da parte dell'utente per l'amministrazione. Per ulteriori informazioni, consulta Confronta gateway e istanze. NAT NAT

Per quanto riguarda IPv6 il traffico, il traffico in uscita può essere configurato in modo decentralizzato in modo da lasciare ciascuno di essi VPC attraverso un gateway Internet di sola uscita oppure può essere configurato per essere inviato a un sistema centralizzato VPC utilizzando istanze o istanze proxy. NAT I modelli sono discussi in. IPv6 Uscita centralizzata per IPv6

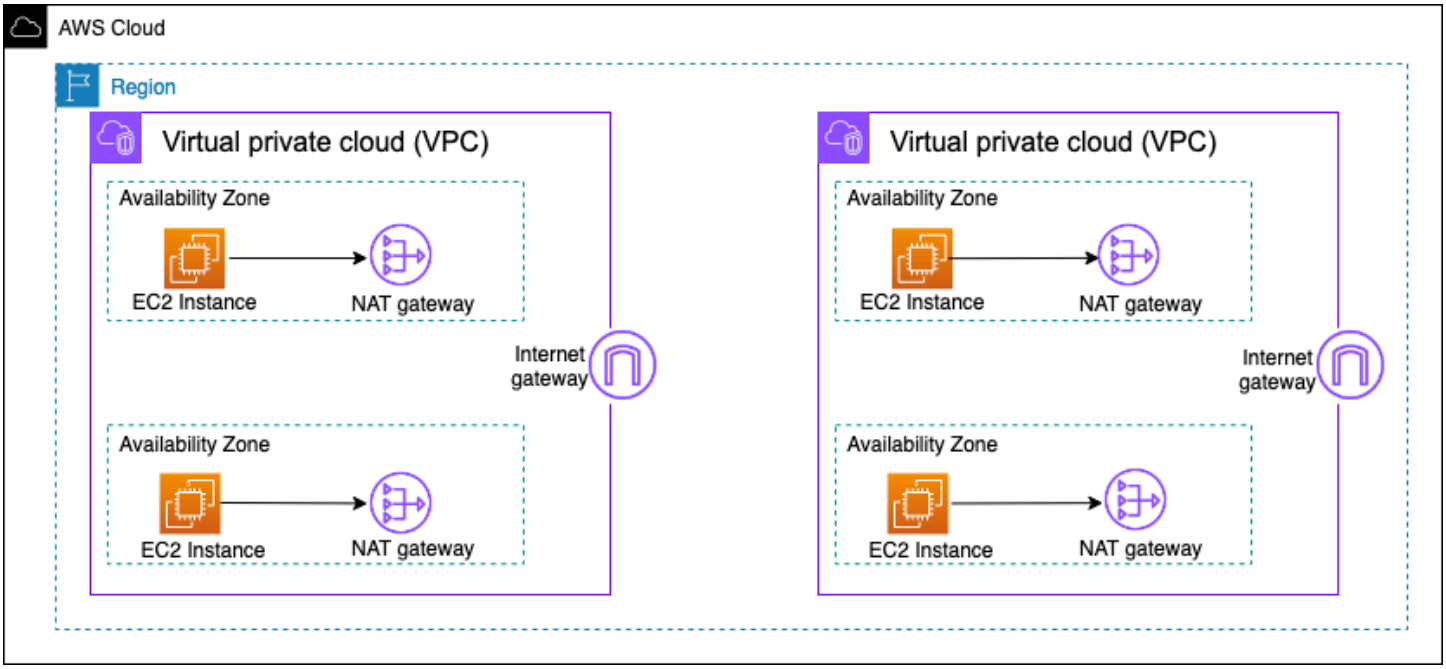
Argomenti

- Utilizzo del NAT gateway per l'uscita centralizzata IPv4
- Utilizzo del NAT gateway con AWS Network Firewall per l'uscita centralizzata IPv4
- Utilizzo del NAT gateway e del Gateway Load Balancer con EC2 istanze Amazon per l'uscita centralizzata IPv4
- Uscita centralizzata per IPv6

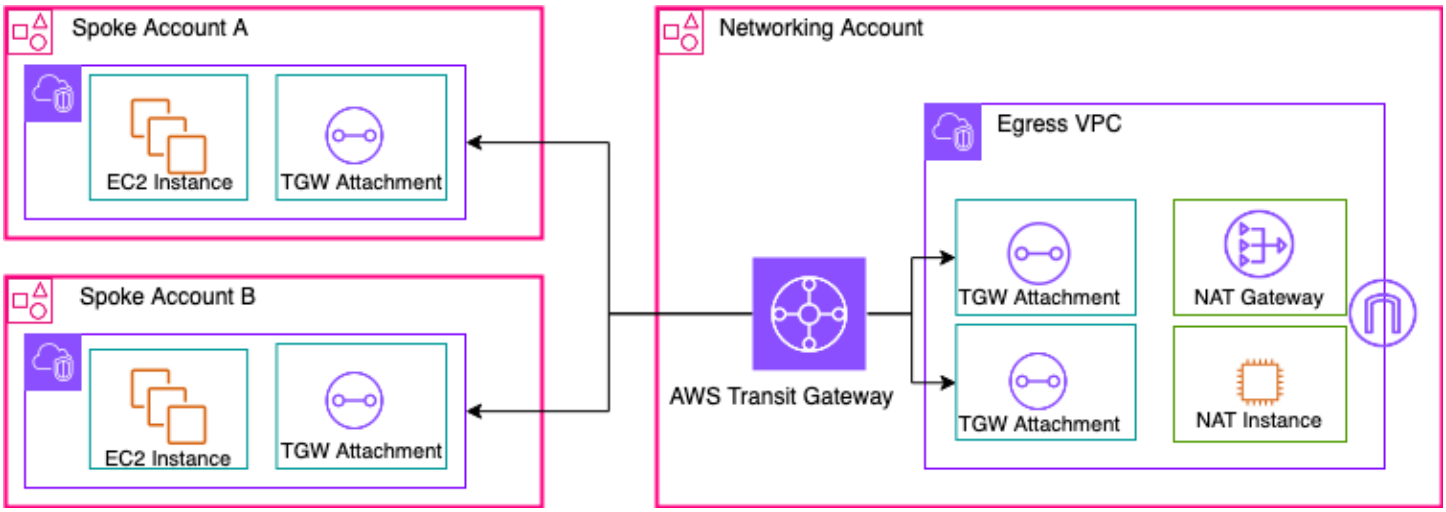
Utilizzo del NAT gateway per l'uscita centralizzata IPv4

NATgateway è un servizio gestito di traduzione degli indirizzi di rete. L'implementazione di un NAT gateway in ogni socket VPC può diventare proibitiva in termini di costi perché si paga una tariffa oraria per ogni NAT gateway distribuito (consulta i prezzi di Amazon). VPC La centralizzazione dei NAT gateway può essere un'opzione valida per ridurre i costi. Per centralizzare, si crea un'uscita separata VPC nell'account dei servizi di rete, si distribuiscono i NAT gateway in uscita e si instrada tutto il traffico in uscita VPC dallo spoke VPCs ai NAT gateway che risiedono nell'uscita utilizzando VPC Transit Gateway o WAN Cloud, come illustrato nella figura seguente.

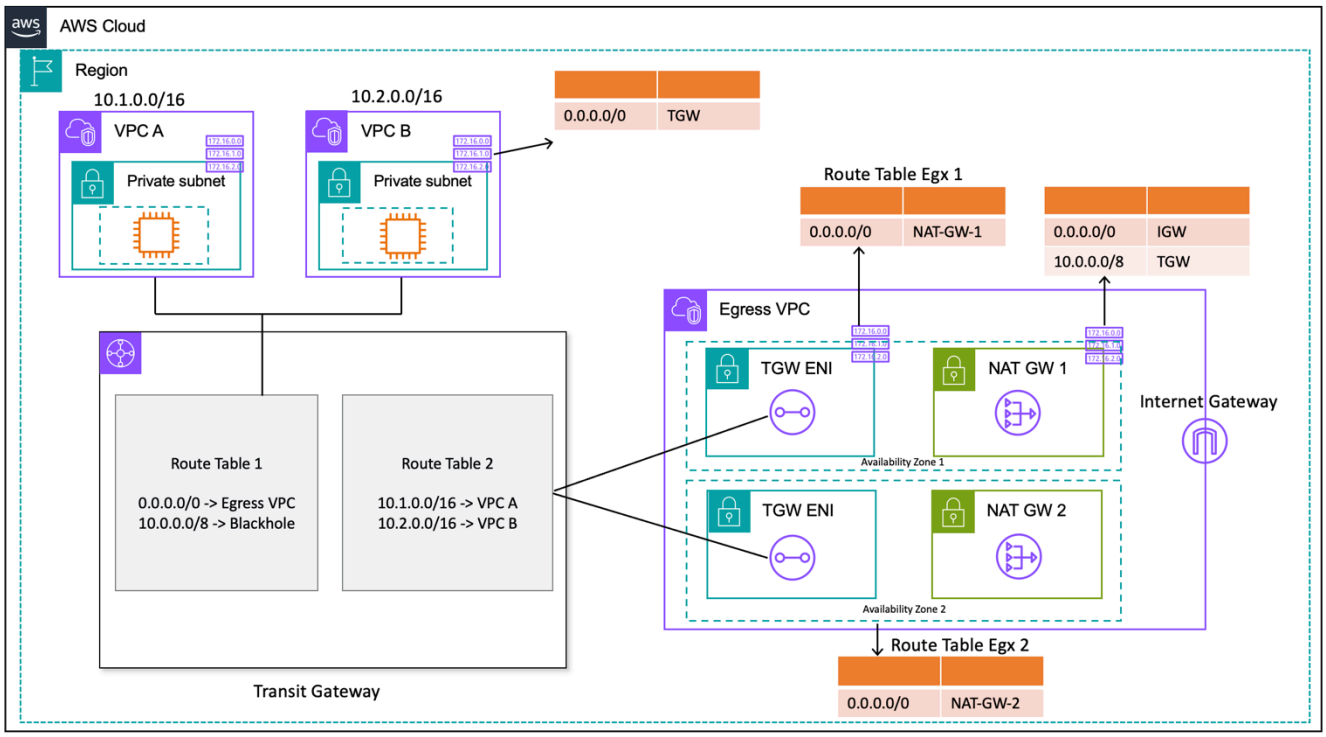
> **Note**
>
> Quando si centralizza il NAT gateway utilizzando Transit Gateway, si paga un costo aggiuntivo per l'elaborazione dei dati Transit Gateway, rispetto all'approccio decentralizzato che prevede la gestione di un NAT gateway in ogni ambiente. VPC In alcuni casi limite, quando si inviano enormi quantità di dati tramite NAT gateway da un punto aVPC, mantenere i dati in NAT locale VPC per evitare i costi di elaborazione dei dati Transit Gateway potrebbe essere un'opzione più conveniente.



Architettura gateway decentralizzata ad alta disponibilità NAT



NATGateway centralizzato con Transit Gateway (panoramica)



NATGateway centralizzato con Transit Gateway (progettazione della tabella delle rotte)

In questa configurazione, VPC gli allegati Spoke sono associati alla Route Table 1 (RT1) e vengono propagati alla Route Table 2 (). RT2 Esiste un percorso Blackhole per impedire ai due di comunicare VPCs tra loro. Se desideri consentire l'VPCintercomunicazione, puoi rimuovere l'ingresso del `10.0.0.0/8 -> Blackhole` percorso da. RT1 Ciò consente loro di comunicare tramite il gateway di transito. Puoi anche propagare gli VPC allegati spoke RT1 (o in alternativa, puoi usare una tabella di routing e associare/propagare tutto a quella), abilitando il flusso di traffico diretto tra i Transit Gateway che utilizzano. VPCs

Si aggiunge un percorso statico per indirizzare tutto il traffico in uscita. RT1 VPC A causa di questa route statica, Transit Gateway invia tutto il traffico Internet attraverso il suo percorso ENIs in uscitaVPC. Una volta in uscitaVPC, il traffico segue i percorsi definiti nella tabella delle rotte di sottorete in cui sono presenti questi Transit Gateway. ENIs Nelle tabelle di routing delle sottoreti si aggiunge un percorso che indirizza tutto il traffico verso il rispettivo NAT gateway nella stessa zona di disponibilità per ridurre al minimo il traffico tra zone di disponibilità (AZ). La tabella di NAT routing della sottorete del gateway ha Internet gateway (IGW) come hop successivo. Affinché il traffico di ritorno ritorni, è necessario aggiungere una voce statica della tabella di routing nella tabella di routing della sottorete del NAT gateway, indicando come hop successivo tutto il traffico VPC legato a spoke verso Transit Gateway.

Elevata disponibilità

Per un'elevata disponibilità, è necessario utilizzare più di un NAT gateway (uno in ogni zona di disponibilità). Se un NAT gateway non è disponibile, il traffico potrebbe essere interrotto nella zona di disponibilità che attraversa il gateway interessatoNAT. Se una zona di disponibilità non è disponibile, l'endpoint Transit Gateway e il NAT gateway in quella zona di disponibilità non funzioneranno e tutto il traffico fluirà attraverso gli endpoint Transit NAT Gateway e gateway nell'altra zona di disponibilità.

Sicurezza

Puoi fare affidamento sui gruppi di sicurezza sulle istanze di origine, sulle route blackhole nelle tabelle di routing del Transit Gateway e sulla rete ACL della sottorete in cui si trova il NAT gateway. Ad esempio, i clienti possono utilizzare ACLs le sottoreti pubbliche del NAT Gateway per consentire o bloccare gli indirizzi IP di origine o di destinazione. In alternativa, è possibile utilizzare NAT Gateway with AWS Network Firewall per l'uscita centralizzata descritta nella sezione successiva per soddisfare questo requisito.

Scalabilità

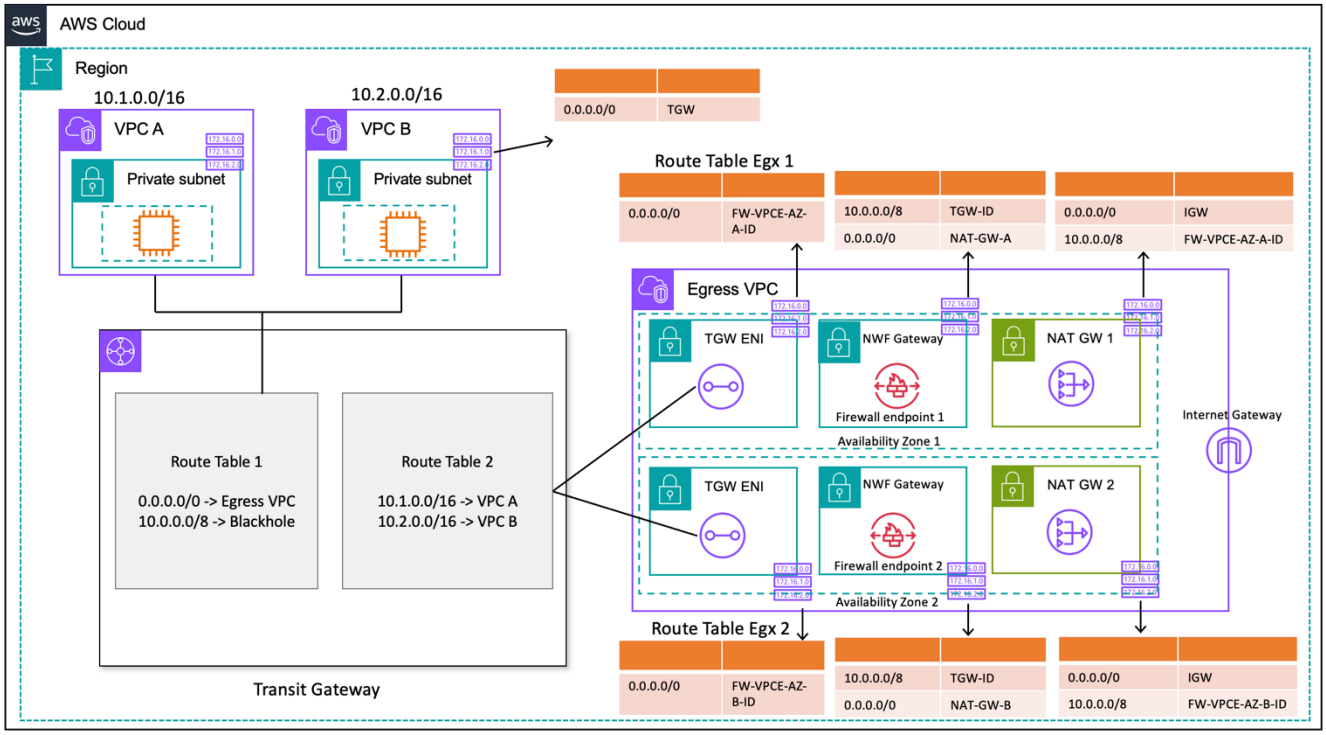
Un singolo NAT gateway può supportare fino a 55.000 connessioni simultanee per indirizzo IP assegnato a ciascuna destinazione unica. È possibile richiedere un aggiustamento della quota per consentire fino a otto indirizzi IP assegnati, consentendo 440.000 connessioni simultanee a un unico IP e porta di destinazione. NATil gateway fornisce 5 Gbps di larghezza di banda e si ridimensiona automaticamente fino a 100 Gbps. Transit Gateway generalmente non funge da load balancer e non distribuisce il traffico in modo uniforme tra i NAT gateway nelle diverse zone di disponibilità. Il traffico attraverso il Transit Gateway rimarrà all'interno di una zona di disponibilità, se possibile. Se l'EC2istanza Amazon che avvia il traffico si trova nella zona di disponibilità 1, il traffico uscirà dall'interfaccia di rete elastica Transit Gateway nella stessa zona di disponibilità 1 in uscita VPC e fluirà verso l'hop successivo in base alla tabella di routing di sottorete in cui risiede l'elastic network interface. Per un elenco completo delle regole, consulta i NATgateway nella documentazione di Amazon Virtual Private Cloud.

Per ulteriori informazioni, consulta il post di blog Creazione di un singolo punto di uscita Internet da più VPCs Using AWS Transit Gateway.

Utilizzo del NAT gateway con AWS Network Firewall per l'uscita centralizzata IPv4

Se desideri ispezionare e filtrare il traffico in uscita, puoi incorporare AWS Network Firewall con NAT gateway nella tua architettura di uscita centralizzata. AWS Network Firewall è un servizio gestito che semplifica l'implementazione delle protezioni di rete essenziali per tutti i tuoi. VPCs Fornisce il controllo e la visibilità dell'intero traffico di rete di livello 3-7. VPC È possibile filtrare URL /domain name, IP address e il traffico in uscita basato sul contenuto per bloccare possibili perdite di dati, contribuire a soddisfare i requisiti di conformità e bloccare le comunicazioni malware note. AWS Network Firewall supporta migliaia di regole in grado di filtrare il traffico di rete destinato a noti indirizzi IP o nomi di dominio non validi. Puoi anche utilizzare IPS le regole di Suricata come parte del AWS Network Firewall servizio importando set di regole open source o creando regole personalizzate per l'Intrusion Prevention System () utilizzando la sintassi delle regole Suricata. IPS AWS Network Firewall consente inoltre di importare regole compatibili fornite dai partner. AWS

Nell'architettura di uscita centralizzata con ispezione, l' AWS Network Firewall endpoint è un obiettivo predefinito della tabella di routing nella tabella di routing della sottorete transit gateway attachments per l'uscita. VPC Il traffico tra spoke VPCs e Internet viene ispezionato utilizzando AWS Network Firewall quanto illustrato nel diagramma seguente.



Uscita centralizzata con gateway (progettazione della tabella di AWS Network Firewall percorsoNAT)

Per un modello di implementazione centralizzato con Transit Gateway, AWS consiglia di implementare gli AWS Network Firewall endpoint in più zone di disponibilità. Dovrebbe esserci un endpoint firewall in ogni zona di disponibilità in cui il cliente esegue i carichi di lavoro, come illustrato nel diagramma precedente. Come procedura ottimale, la sottorete firewall non deve contenere altro traffico perché non AWS Network Firewall è in grado di ispezionare il traffico proveniente da fonti o destinazioni all'interno di una sottorete firewall.

Analogamente alla configurazione precedente, VPC gli allegati Spoke sono associati alla Route Table 1 (RT1) e vengono propagati alla Route Table 2 (). RT2 Viene aggiunta esplicitamente una rotta Blackhole per impedire ai due VPCs di comunicare tra loro.

Continua a utilizzare un percorso predefinito per indirizzare tutto il traffico in RT1 uscita. VPC Transit Gateway inoltrerà tutti i flussi di traffico verso una delle due zone di disponibilità in uscitaVPC. Una volta che il traffico raggiunge uno dei Transit Gateway ENIs in uscitaVPC, si segue un percorso predefinito che inoltrerà il traffico a uno degli AWS Network Firewall endpoint nella rispettiva zona di disponibilità. AWS Network Firewall esaminerà quindi il traffico in base alle regole impostate prima di inoltrarlo al NAT gateway utilizzando un percorso predefinito.

Questo caso non richiede la modalità appliance Transit Gateway, perché non si invia traffico tra gli allegati.

> **Note**
>
> AWS Network Firewall non esegue la traduzione degli indirizzi di rete per voi, questa funzione verrebbe gestita dal NAT gateway dopo l'ispezione del traffico tramite. AWS Network Firewall Il routing in ingresso non è necessario in questo caso, poiché il traffico di ritorno verrà inoltrato a quello predefinito. NATGW IPs

Poiché si utilizza un Transit Gateway, qui possiamo posizionare il firewall prima del NAT gateway. In questo modello, il firewall può vedere l'IP di origine dietro il Transit Gateway.

Se lo facessi in un'unica soluzioneVPC, possiamo utilizzare i miglioramenti del VPC routing che consentono di ispezionare il traffico tra le sottoreti della stessa. VPC Per i dettagli, consulta il post sul blog Deployment models for AWS Network Firewall with routing enhancements. VPC

Scalabilità

AWS Network Firewall può aumentare o ridurre automaticamente la capacità del firewall in base al carico di traffico per mantenere prestazioni stabili e prevedibili e ridurre al minimo i costi. AWS

Network Firewall è progettato per supportare decine di migliaia di regole firewall e può scalare fino a 100 Gbps di velocità effettiva per zona di disponibilità.

Considerazioni chiave

- Ogni endpoint firewall è in grado di gestire circa 100 Gbps di traffico. Se hai bisogno di un burst più elevato o di un throughput sostenuto, contatta l'assistenza. AWS
- Se scegli di creare un NAT gateway nel tuo AWS account insieme a Network Firewall, non verranno addebitati i costi di elaborazione standard del NAT gateway e di utilizzo all'ora in one-to-one base all'elaborazione per GB e alle ore di utilizzo addebitate per il firewall.
- Puoi anche prendere in considerazione l'utilizzo di endpoint firewall distribuiti AWS Firewall Manager senza Transit Gateway.
- Verifica le regole del firewall prima di trasferirle in produzione, in modo simile a una lista di controllo degli accessi alla rete, poiché l'ordine è importante.
- Per un'ispezione più approfondita sono necessarie regole avanzate in Suricata. Il firewall di rete supporta l'ispezione crittografata del traffico in ingresso e in uscita.
- La variabile del gruppo di `HOME_NET` regole definiva l'intervallo IP di origine idoneo per l'elaborazione nel motore Stateful. Utilizzando un approccio centralizzato, è necessario aggiungere tutti gli altri VPC CIDRs allegati al Transit Gateway per renderli idonei all'elaborazione. Consulta la documentazione di Network Firewall per maggiori dettagli sulla variabile del gruppo di `HOME_NET` regole.
- Prendi in considerazione la possibilità di implementare Transit Gateway e l'uscita VPC in un account Network Services separato per separare l'accesso in base alla delega di compiti; ad esempio, solo gli amministratori di rete possono accedere all'account Network Services.
- Per semplificare l'implementazione e la gestione di questo modello AWS Network Firewall , può essere utilizzato. AWS Firewall Manager Firewall Manager consente di amministrare centralmente i diversi firewall applicando automaticamente la protezione creata nella posizione centralizzata a più account. Firewall Manager supporta modelli di distribuzione distribuiti e centralizzati per Network Firewall. Per ulteriori informazioni, consulta il post del blog How to deploy AWS Network Firewall by using. AWS Firewall Manager

Utilizzo del NAT gateway e del Gateway Load Balancer con EC2 istanze Amazon per l'uscita centralizzata IPv4

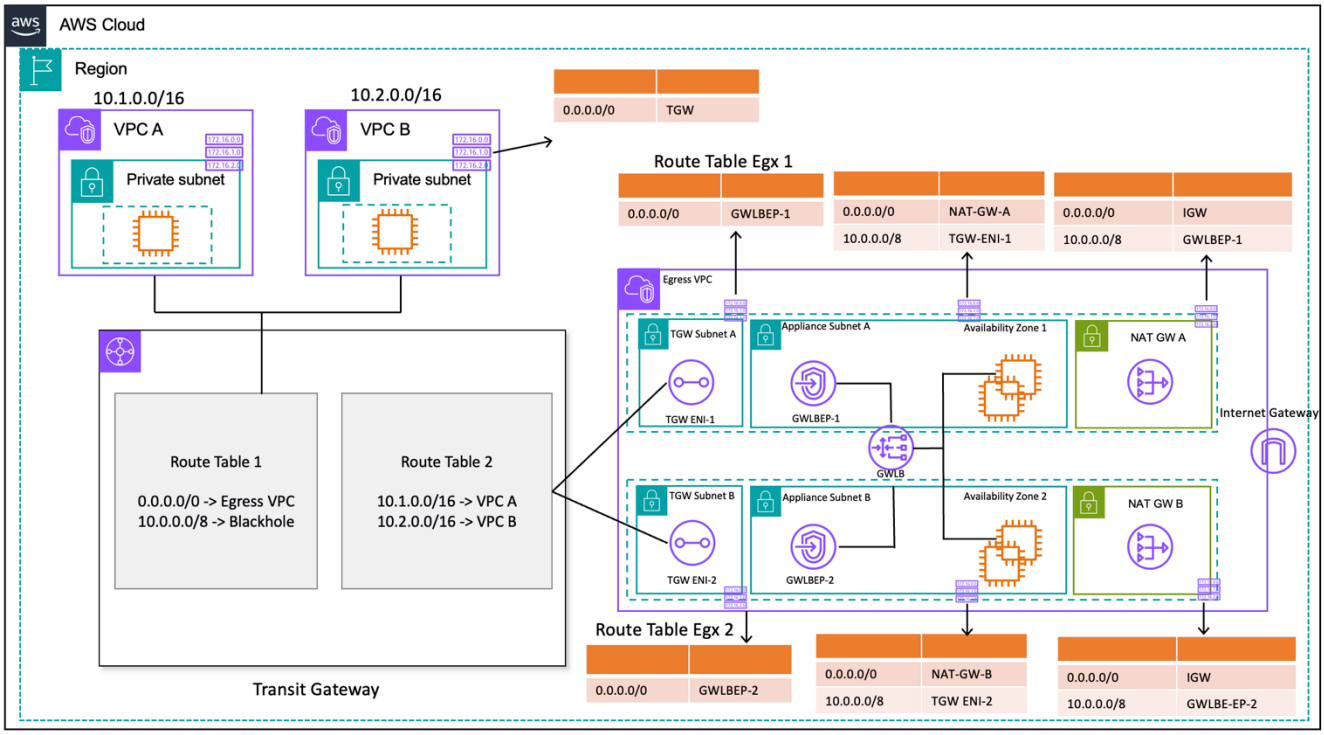
L'utilizzo di un'appliance virtuale basata su software (su AmazonEC2) da Marketplace AWS e AWS Partner Network come punto di uscita è simile alla configurazione del NAT gateway. Questa opzione può essere utilizzata se si desidera utilizzare il sistema di prevenzione e rilevamento delle intrusioni (IPS/IDS) avanzato di livello 7 e le funzionalità di ispezione approfondita dei pacchetti offerte dai vari fornitori.

Nella figura seguente, oltre al NAT gateway, si distribuiscono appliance virtuali utilizzando EC2 istanze dietro un Gateway Load GWLB Balancer (). In questa configurazioneGWLB, Gateway Load Balancer Endpoint (GWLBE), le appliance e i NAT gateway virtuali vengono distribuiti in un sistema centralizzato VPC collegato al Transit Gateway tramite allegato. VPC Gli spoke VPCs sono inoltre collegati al Transit Gateway tramite un VPC Attachment. Poiché GWLBEs sono una destinazione instradabile, puoi indirizzare il traffico che si sposta da e verso il Transit Gateway verso la flotta di appliance virtuali configurate come destinazioni dietro aGWLB. GWLBagisce come un bump-in-the-wire e trasmette in modo trasparente tutto il traffico di livello 3 attraverso dispositivi virtuali di terze parti e quindi è invisibile alla fonte e alla destinazione del traffico. Pertanto, questa architettura consente di ispezionare centralmente tutto il traffico in uscita che attraversa Transit Gateway.

Per ulteriori informazioni su come il traffico fluisce dalle applicazioni su Internet e viceversa attraverso questa configurazione, consulta Architettura di ispezione centralizzata con AWS Gateway Load AWS Transit Gateway Balancer e. VPCs

È possibile abilitare la modalità appliance su Transit Gateway per mantenere la simmetria del flusso attraverso le appliance virtuali. Ciò significa che il traffico bidirezionale viene instradato attraverso lo stesso dispositivo e la zona di disponibilità per tutta la durata del flusso. Questa impostazione è particolarmente importante per i firewall stateful che eseguono un'ispezione approfondita dei pacchetti. L'attivazione della modalità appliance elimina la necessità di soluzioni alternative complesse, come la traduzione degli indirizzi di rete di origine (SNAT), per forzare il ritorno del traffico all'appliance corretta per mantenere la simmetria. Per ulteriori informazioni, consulta le best practice per l'implementazione di Gateway Load Balancer.

È anche possibile implementare gli GWLB endpoint in modo distribuito senza Transit Gateway per consentire l'ispezione in uscita. Scopri di più su questo modello architettonico nel post del blog Introducing AWS Gateway Load Balancer: Supported architecture patterns.



Uscita centralizzata con Gateway Load Balancer EC2 e istanza (progettazione della tabella di percorso)

Elevata disponibilità

AWSconsiglia di implementare Gateway Load Balancer e appliance virtuali in più zone di disponibilità per una maggiore disponibilità.

Gateway Load Balancer può eseguire controlli di integrità per rilevare i guasti delle appliance virtuali. In caso di malfunzionamento dell'appliance, GWLB reindirizza i nuovi flussi verso dispositivi funzionanti. I flussi esistenti vanno sempre allo stesso obiettivo indipendentemente dallo stato di salute dell'obiettivo. Ciò consente di svuotare la connessione e di evitare errori nei controlli di integrità dovuti a CPU picchi sugli elettrodomestici. Per ulteriori dettagli, fare riferimento alla sezione 4: Comprendere gli scenari di errore di appliance e Availability Zone nel post del blog Best practice for deploying Gateway Load Balancer. Gateway Load Balancer può utilizzare gruppi con scalabilità automatica come obiettivi. Questo vantaggio elimina l'oneroso compito di gestire la disponibilità e la scalabilità delle flotte di appliance.

Vantaggi

Gli endpoint Gateway Load Balancer e Gateway Load Balancer sono alimentati AWS PrivateLink da, che consente lo scambio di traffico VPC attraverso i confini in modo sicuro senza la necessità di attraversare la rete Internet pubblica.

Gateway Load Balancer è un servizio gestito che elimina il carico indifferenziato di gestione, implementazione e scalabilità delle appliance di sicurezza virtuali, in modo che tu possa concentrarti sulle cose che contano. Gateway Load Balancer può esporre lo stack di firewall come servizio endpoint a cui i clienti possono abbonarsi utilizzando il. Marketplace AWS Si chiama Firewall as a Service (FWaaS); introduce una distribuzione semplificata ed elimina la necessità di ECMP affidarsi BGP e distribuire il traffico su più istanze AmazonEC2.

Considerazioni chiave

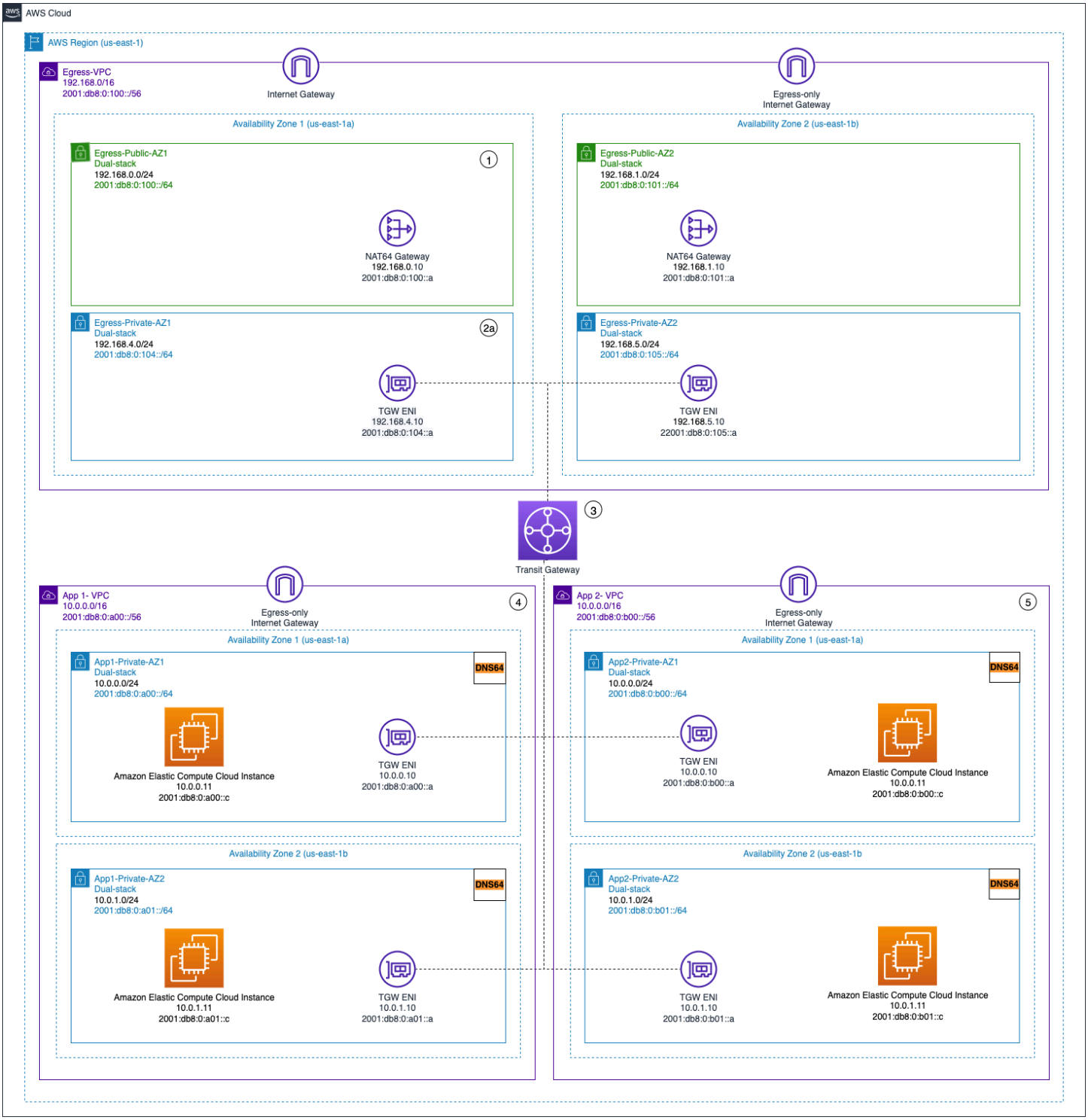
- Le apparecchiature devono supportare il protocollo di incapsulamento Geneve con cui integrarsi. GWLB
- Alcuni dispositivi di terze parti possono supportare SNAT e sovrapporre il routing (modalità a due bracci), eliminando così la necessità di creare gateway per risparmiare sui costi. NAT Tuttavia, consulta un AWS partner di tua scelta prima di utilizzare questa modalità, poiché dipende dal supporto e dall'implementazione del fornitore.
- Prendi nota del timeout di GWLBinattività. Ciò può causare timeout di connessione per i client. È possibile regolare i timeout a livello di client, server, firewall e sistema operativo per evitare che ciò si verifichi. Per ulteriori informazioni, consultate la Sezione 1: Ottimizzazione dei valori TCP keep-alive o timeout per supportare TCP flussi di lunga durata nel post del blog Best practice for deploying Gateway Load Balancer.
- GWLBEsono alimentati da, pertanto verranno applicati dei AWS PrivateLink costi. AWS PrivateLink Puoi saperne di più nella pagina AWS PrivateLink dei prezzi. Se si utilizza il modello centralizzato con Transit Gateway, saranno applicabili i costi di elaborazione dei TGW dati.
- Prendi in considerazione la possibilità di implementare Transit Gateway e l'uscita VPC in un account Network Services separato per separare l'accesso in base alla delega di compiti, ad esempio solo gli amministratori di rete possono accedere all'account di servizi di rete.

Uscita centralizzata per IPv6

Per supportare l'IPv6uscita in implementazioni dual stack con uscita centralizzataIPv4, è necessario scegliere uno dei due modelli seguenti:

- IPv4Uscita IPv6 centralizzata con uscita decentralizzata
- Uscita centralizzata e uscita centralizzata IPv4 IPv6

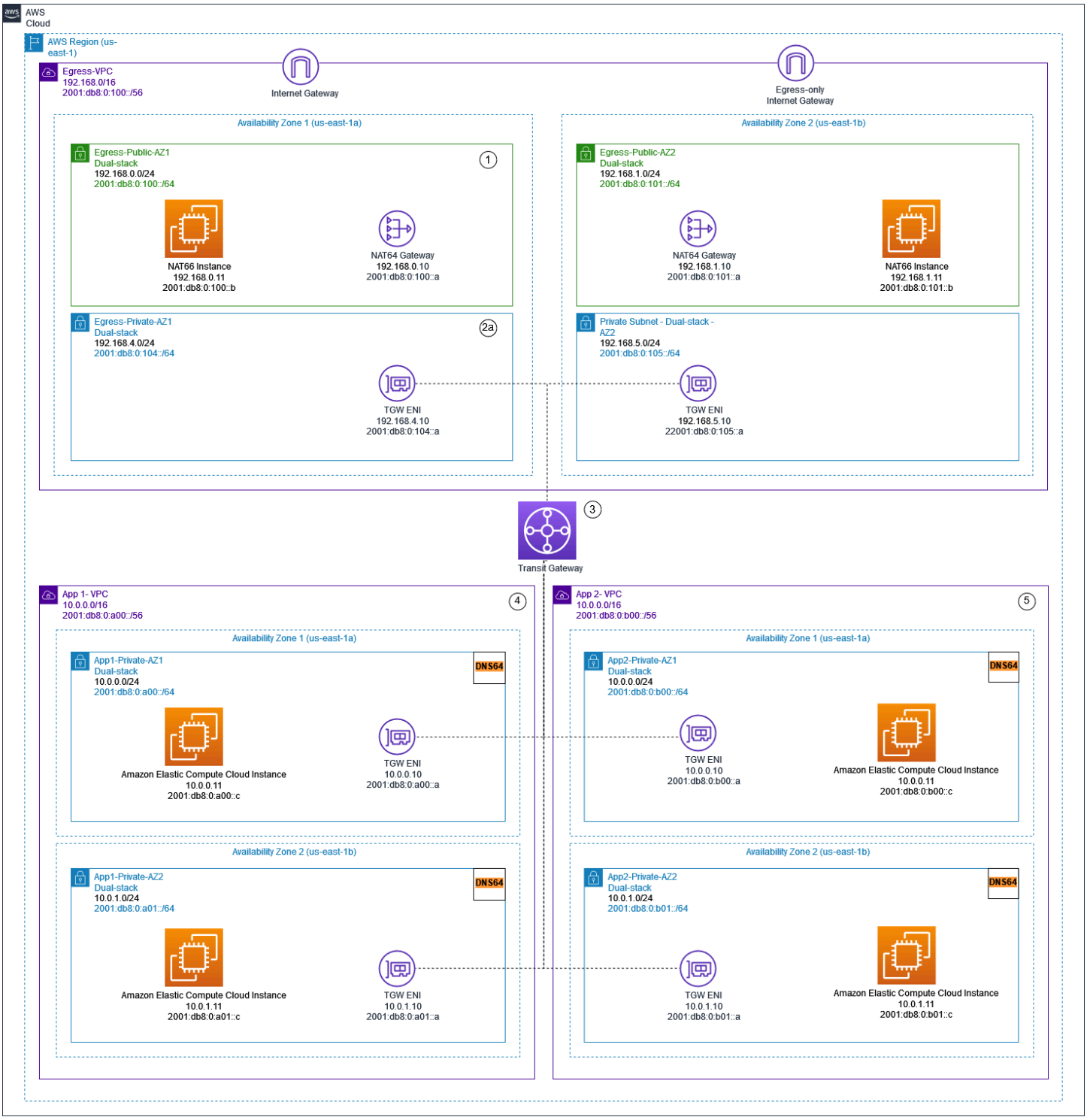
Nel primo schema, illustrato nel diagramma seguente, i gateway Internet di sola uscita vengono distribuiti in ogni raggio. VPC I gateway Internet solo in uscita sono gateway a scalabilità orizzontale, ridondanti e ad alta disponibilità che consentono la comunicazione in uscita da istanze interne al sistema. IPv6 VPC Impediscono a Internet di avviare connessioni con le tue istanze. IPv6 I gateway Internet solo in uscita sono gratuiti. In questo modello di implementazione, il IPv6 traffico esce dai gateway Internet solo in uscita di ciascuno di essi VPC e IPv4 il traffico fluisce attraverso i gateway centralizzati implementati. NAT



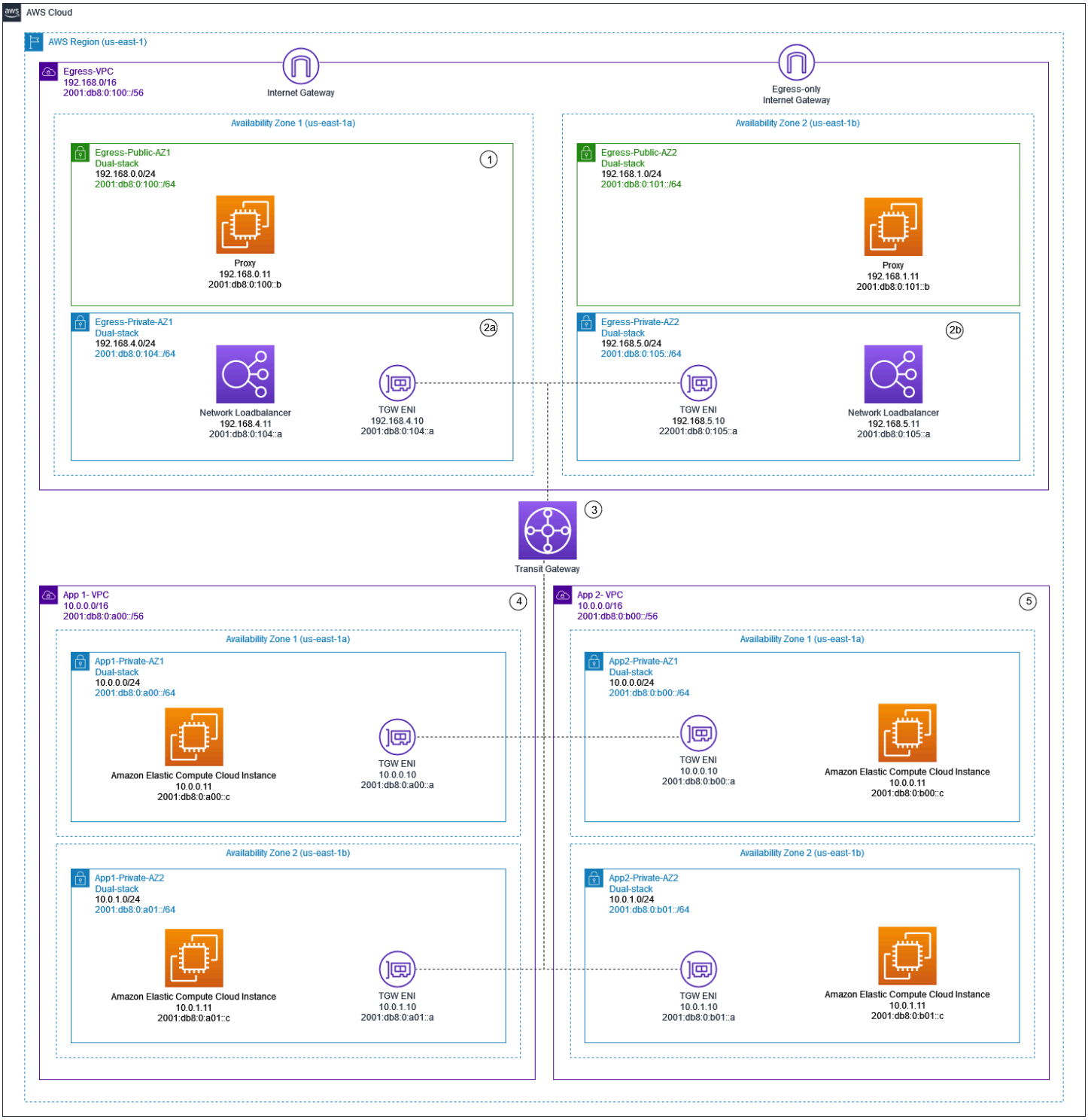
Uscita centralizzata e uscita decentralizzata solo in uscita IPV4 IPv6

Nel secondo schema, illustrato nei diagrammi seguenti, il IPv6 traffico in uscita dalle istanze viene inviato a un sistema centralizzato. VPC Ciò può essere ottenuto utilizzando IPv6 -to- IPv6 Network Prefix Translation (NPTv6) con NAT66 istanze e NAT gateway o utilizzando Proxy Instances e

Network Load Balancer. Questo schema è applicabile se è richiesta un'ispezione centralizzata del traffico in uscita e non può essere eseguita in ogni raggio. VPC



Uscita centralizzata tramite gateway e istanze IPv6 NAT NAT66



Centralizzato IPv4 e in IPv6 uscita tramite istanze proxy e Network Load Balancer

Il AWSwhite paper IPv6 descrive i modelli di uscita centralizzati. IPv6 I modelli IPv6 di uscita sono discussi più dettagliatamente nel blog Traffico Internet in uscita centralizzato per il dual stack IPv4 e IPv6VPCs, insieme a considerazioni speciali, soluzioni di esempio e diagrammi.

Sicurezza di rete centralizzata per il traffico da VPC a VPC e da locale a VPC

Potrebbero esserci scenari in cui un cliente desidera implementare un firewall/IPS/ID di livello 3-7 all'interno del proprio ambiente multi-account per ispezionare i flussi di traffico tra VPC (traffico est-ovest) o tra un data center locale e un VPC (traffico nord-sud). Ciò può essere ottenuto in diversi modi, a seconda del caso d'uso e dei requisiti. Ad esempio, è possibile incorporare Gateway Load Balancer, Network Firewall, Transit VPC o utilizzare architetture centralizzate con Transit Gateway. Questi scenari sono descritti nella sezione seguente.

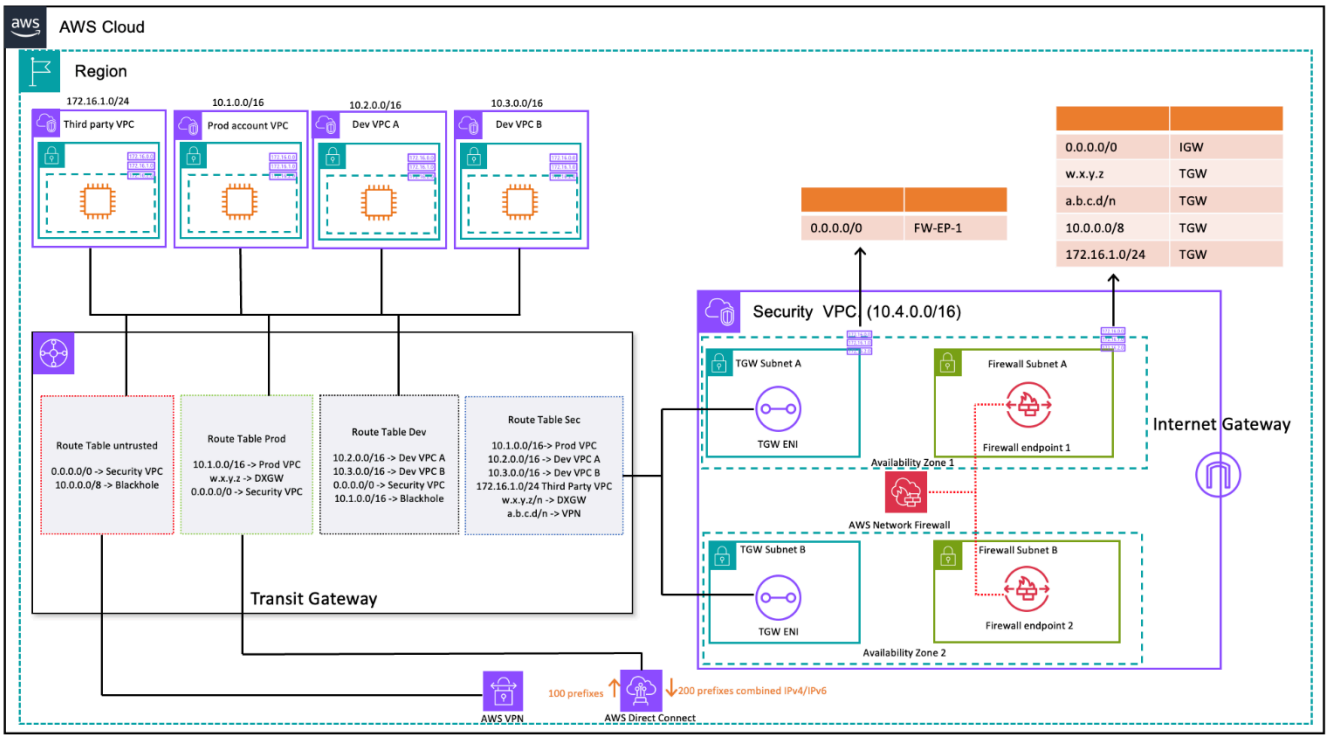
Considerazioni sull'utilizzo di un modello centralizzato di ispezione della sicurezza della rete

Per ridurre i costi, dovresti essere selettivo in merito al traffico che passa attraverso il tuo AWS Network Firewall o il Gateway Load Balancer. Un modo per procedere consiste nel definire le zone di sicurezza e ispezionare il traffico tra zone non attendibili. Un'area non attendibile può essere un sito remoto gestito da una terza parte, un VPC di un fornitore che non controlli o non ti fidi o un VPC sandbox/dev, che ha regole di sicurezza più rilassate rispetto al resto dell'ambiente. In questo esempio sono presenti quattro zone:

- Zona non attendibile: si tratta di qualsiasi traffico proveniente dalla «VPN verso un sito remoto non affidabile» o dal VPC del fornitore terzo.
- Zona di produzione (Prod): contiene il traffico proveniente dal VPC di produzione e dal DC del cliente locale.
- Zona di sviluppo (Dev): contiene il traffico proveniente dai due VPC di sviluppo.
- Zona di sicurezza (Sec): contiene i nostri componenti firewall Network Firewall o Gateway Load Balancer.

Questa configurazione ha quattro zone di sicurezza, ma potresti averne di più. È possibile utilizzare più tabelle di percorsi e percorsi blackhole per ottenere un isolamento di sicurezza e un flusso di traffico ottimale. La scelta del giusto set di zone dipende dalla strategia generale di progettazione della Landing Zone (struttura dell'account, progettazione del VPC). È possibile disporre di zone per consentire l'isolamento tra unità aziendali (BU), applicazioni, ambienti e così via.

Se desideri ispezionare e filtrare il traffico da VPC a VPC, il traffico interzona e il traffico VPC on-premise, puoi incorporare Transit Gateway nella tua architettura centralizzata. AWS Network Firewall Utilizzando il modello di, è possibile ottenere un modello di implementazione centralizzato. hub-and-spoke AWS Transit Gateway AWS Network Firewall Viene distribuito in un VPC di sicurezza separato. Un VPC di sicurezza separato offre un approccio semplificato e centrale alla gestione delle ispezioni. Tale architettura VPC offre visibilità IP di AWS Network Firewall origine e destinazione. Vengono preservati sia gli IP di origine che quelli di destinazione. Questo VPC di sicurezza è composto da due sottoreti in ciascuna zona di disponibilità, dove una sottorete è dedicata agli AWS Transit Gateway allegati e l'altra è dedicata all'endpoint del firewall. Le sottoreti in questo VPC devono contenere solo endpoint AWS Network Firewall perché Network Firewall non può ispezionare il traffico nelle stesse sottoreti degli endpoint. Quando si utilizza Network Firewall per ispezionare centralmente il traffico, è possibile eseguire un'ispezione approfondita dei pacchetti (DPI) sul traffico in ingresso. Il modello DPI viene approfondito nella sezione Centralized Inbound Inspection di questo paper.



Ispezione del traffico da VPC a VPC e da locale a VPC tramite Transit Gateway e (progettazione della tabella di percorso) AWS Network Firewall

Nell'architettura centralizzata con ispezione, le sottoreti Transit Gateway richiedono una tabella di routing VPC separata per garantire che il traffico venga inoltrato all'endpoint del firewall all'interno della stessa zona di disponibilità. Per il traffico di ritorno, viene configurata una singola tabella di routing VPC contenente una route predefinita verso il Transit Gateway. Il traffico viene riportato

AWS Transit Gateway nella stessa zona di disponibilità dopo essere stato ispezionato da. AWS Network Firewall Ciò è possibile grazie alla funzionalità di modalità appliance del Transit Gateway. La funzionalità in modalità appliance del Transit Gateway consente inoltre di disporre di funzionalità AWS Network Firewall di ispezione del traffico con stato all'interno del VPC di sicurezza.

Con la modalità appliance abilitata su un gateway di transito, seleziona un'unica interfaccia di rete utilizzando l'algoritmo flow hash per l'intera durata della connessione. Il gateway di transito utilizza la stessa interfaccia di rete per il traffico di ritorno. In questo modo, il traffico bidirezionale viene instradato simmetricamente: viene instradato attraverso la stessa zona di disponibilità nell'allegato VPC per tutta la durata del flusso. Per ulteriori informazioni sulla modalità appliance, consulta le appliance Stateful e la modalità appliance nella documentazione di Amazon VPC.

Per le diverse opzioni di implementazione di Security VPC with AWS Network Firewall e Transit Gateway, consulta il post sul blog Deployment models for AWS Network Firewall.

Utilizzo di Gateway Load Balancer con Transit Gateway per la sicurezza di rete centralizzata

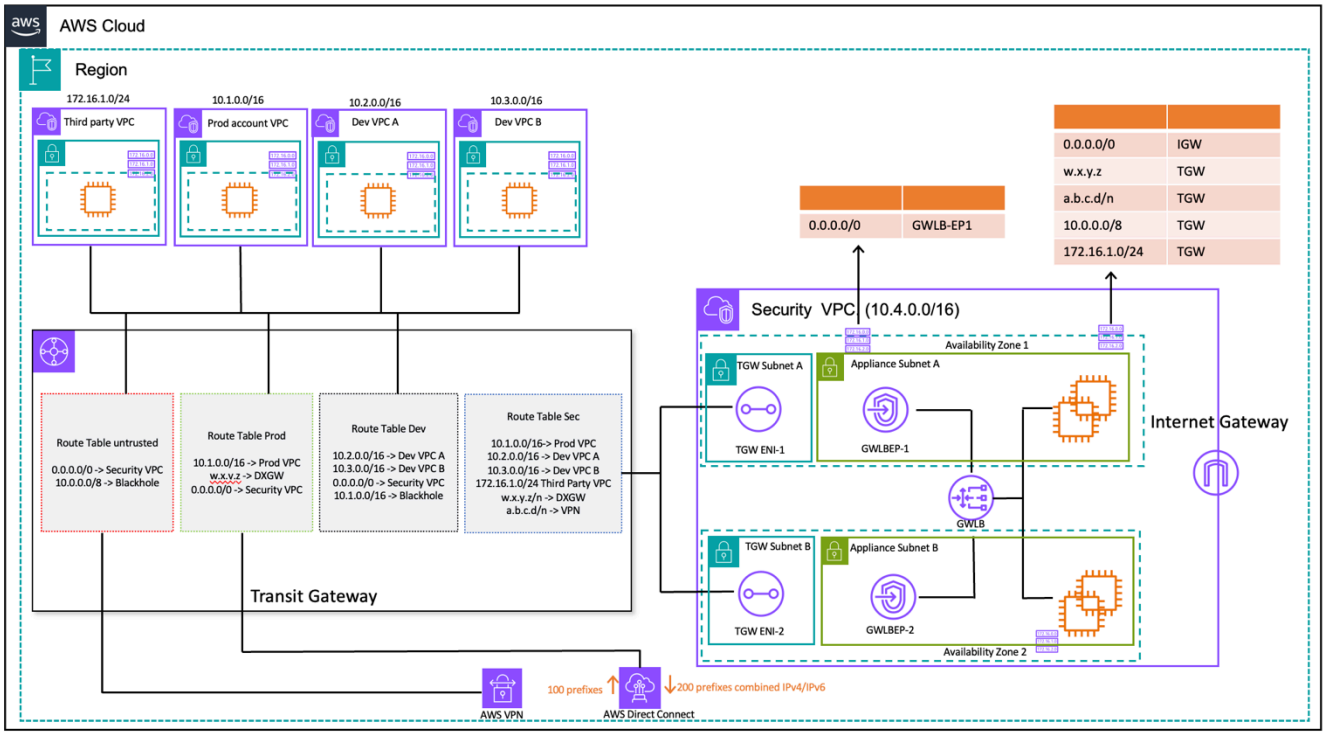
Spesso i clienti desiderano incorporare dispositivi virtuali per gestire il filtraggio del traffico e fornire funzionalità di ispezione della sicurezza. In questi casi d'uso, possono integrare Gateway Load Balancer, appliance virtuali e Transit Gateway per implementare un'architettura centralizzata per l'ispezione del traffico da VPC a VPC e VPC. to-on-premises

Gateway Load Balancer viene distribuito in un VPC di sicurezza separato insieme alle appliance virtuali. Le appliance virtuali che controlleranno il traffico sono configurate come obiettivi dietro il Gateway Load Balancer. Poiché gli endpoint Gateway Load Balancer sono un target instradabile, i clienti possono instradare il traffico che si sposta da e verso Transit Gateway verso la flotta di appliance virtuali. Per garantire la simmetria del flusso, la modalità appliance è abilitata sul Transit Gateway.

Ogni VPC a spoke ha una tabella di routing associata al Transit Gateway, che ha la route predefinita verso l'allegato Security VPC come hop successivo.

Il Security VPC centralizzato è costituito da sottoreti di appliance in ciascuna zona di disponibilità, che dispongono degli endpoint Gateway Load Balancer e delle appliance virtuali. Dispone inoltre di sottoreti per gli allegati Transit Gateway in ogni zona di disponibilità, come illustrato nella figura seguente.

Per ulteriori informazioni sull'ispezione di sicurezza centralizzata con Gateway Load Balancer e Transit Gateway, consulta l'architettura di ispezione centralizzata con AWS Gateway Load Balancer e il post del blog. AWS Transit Gateway



on-premises-toIspezione del traffico da VPC a VPC e -VPC utilizzando Transit Gateway e AWS Gateway Load Balancer (progettazione della tabella di percorso)

Considerazioni chiave per AWS Network FirewallAWS Gateway Load Balancer

- La modalità appliance deve essere abilitata sul Transit Gateway quando si esegue l'ispezione est-ovest.
- È possibile implementare lo stesso modello per l'ispezione del traffico verso altri utenti Regioni AWS utilizzando il peering interregionale AWS Transit Gateway.
- Per impostazione predefinita, ogni Gateway Load Balancer distribuito in una zona di disponibilità distribuisce il traffico tra le destinazioni registrate solo all'interno della stessa zona di disponibilità. Questa è chiamata affinità della zona di disponibilità. Se abiliti il bilanciamento del carico tra zone, Gateway Load Balancer distribuisce il traffico su tutti i target registrati e integri in tutte le zone di disponibilità abilitate. Se tutte le destinazioni in tutte le zone di disponibilità non sono integre, il Gateway Load Balancer non si apre. Per ulteriori dettagli, fare riferimento alla sezione 4:

Informazioni sugli scenari di errore di appliance e Availability Zone nel post del blog Best practice for deploying Gateway Load Balancer.

- Per l'implementazione in più regioni, si AWS consiglia di configurare VPC di ispezione separati nelle rispettive regioni locali per evitare dipendenze tra regioni e ridurre i costi di trasferimento dei dati associati. È necessario ispezionare il traffico nella regione locale anziché centralizzare l'ispezione in un'altra regione.
- Il costo di esecuzione di una coppia aggiuntiva ad alta disponibilità (HA) basata su EC2 in implementazioni multiregionali può aumentare. Per ulteriori informazioni, consulta il post di blog sulle migliori pratiche per la distribuzione di Gateway Load Balancer.

AWS Network Firewall rispetto a Gateway Load Balancer

Tabella 2: AWS Network Firewall confronto tra Gateway Load Balancer

Criteri	AWS Network Firewall	Gateway Load Balancer
Caso d'uso	Firewall di rete Stateful, gestito, con funzionalità di servizio di rilevamento e prevenzione delle intrusioni compatibile con Suricata.	Servizio gestito che semplifica l'implementazione, la scalabilità e la gestione di dispositivi virtuali di terze parti
Complessità	AWS servizio gestito. AWS gestisce la scalabilità e la disponibilità del servizio.	Servizio gestito da AWS. AWS gestirà la scalabilità e la disponibilità del servizio Gateway Load Balancer. Il cliente è responsabile della gestione della scalabilità e della disponibilità delle appliance virtuali alla base di Gateway Load Balancer.
Scala	AWS Network Firewall gli endpoint sono alimentati da AWS PrivateLink. Network Firewall supporta fino a 100	Gli endpoint Gateway Load Balancer supportano una larghezza di banda massima fino a 100 Gbps per endpoint

Criteri	AWS Network Firewall	Gateway Load Balancer
	Gbps di traffico di rete per endpoint firewall.	
Costo	AWS Network Firewall costo dell'endpoint + costi di elaborazione dei dati	Gateway Load Balancer + Endpoint Gateway Load Balancer + appliance virtuali + costi di elaborazione dati

Ispezione centralizzata in entrata

Le applicazioni connesse a Internet, per loro natura, hanno una superficie di attacco più ampia e sono esposte a categorie di minacce che la maggior parte degli altri tipi di applicazioni non deve affrontare. Avere la protezione necessaria dagli attacchi contro questi tipi di applicazioni e ridurre al minimo la superficie di impatto sono elementi fondamentali di qualsiasi strategia di sicurezza.

Quando distribuisci le applicazioni nella tua Landing Zone, gli utenti accederanno a molte app tramite la rete Internet pubblica (ad esempio, tramite un Content Delivery Network (CDN) o un'applicazione Web rivolta al pubblico) tramite un sistema di bilanciamento del carico pubblico, un gateway API o direttamente tramite un gateway Internet. In questo caso puoi proteggere i tuoi carichi di lavoro e le tue applicazioni utilizzando AWS Web Application Firewall (AWS WAF) per Inbound Application Inspection o, in alternativa, IDS/IPS Inbound Inspection utilizzando Gateway Load Balancer o. AWS Network Firewall

Man mano che continui a distribuire applicazioni nella tua Landing Zone, potresti dover ispezionare il traffico Internet in entrata. È possibile raggiungere questo obiettivo in diversi modi, utilizzando architetture di ispezione distribuite, centralizzate o combinate utilizzando Gateway Load Balancer che esegue dispositivi firewall di terze parti o AWS Network Firewall con funzionalità DPI e IDS/IPS avanzate tramite l'uso di regole Suricata open source. Questa sezione tratta sia del Gateway Load Balancer che di una distribuzione centralizzata, che utilizza la AWS Transit Gateway funzione di hub centrale per il routing del traffico. AWS Network Firewall

AWS WAF e AWS Firewall Manager per ispezionare il traffico in entrata da Internet

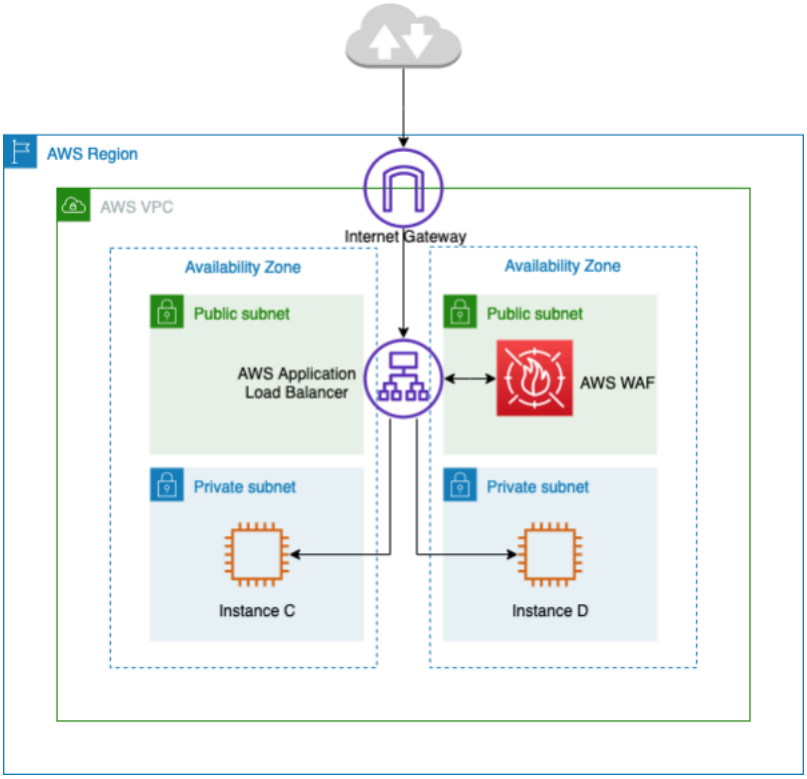
AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web o le API da exploit e bot Web comuni che possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive. AWS WAF consente di controllare il modo in cui il traffico raggiunge le applicazioni, consentendovi di creare regole di sicurezza che controllano il traffico dei bot e bloccano i modelli di attacco più comuni, come l'iniezione SQL o il cross-site scripting (XSS). Puoi anche personalizzare le regole che filtrano modelli di traffico specifici.

Puoi implementarlo AWS WAF su Amazon CloudFront come parte della tua soluzione CDN, l'Application Load Balancer che fronteggia i tuoi server Web, Amazon API Gateway per le tue API REST o AWS AppSync per le tue API GraphQL.

Una volta implementata AWS WAF, puoi creare le tue regole di filtro del traffico utilizzando il generatore di regole visive, il codice in JSON, le regole gestite gestite da AWS oppure puoi abbonarti alle regole di terze parti di. Marketplace AWS Queste regole possono filtrare il traffico indesiderato valutando il traffico rispetto ai modelli specificati. Puoi inoltre utilizzare Amazon CloudWatch per monitorare le metriche e la registrazione del traffico in entrata.

Per una gestione centralizzata di tutti i tuoi account e applicazioni AWS Organizations, puoi usare. AWS Firewall Manager AWS Firewall Manager è un servizio di gestione della sicurezza che consente di configurare e gestire centralmente le regole del firewall. Man mano che vengono create nuove applicazioni, AWS Firewall Manager è facile rendere conformi nuove applicazioni e risorse applicando un insieme comune di regole di sicurezza.

In questo modo AWS Firewall Manager, puoi implementare facilmente AWS WAF le regole per i tuoi Application Load Balancer, le istanze API Gateway e le distribuzioni Amazon. CloudFront AWS Firewall Manager si integra con Regole gestite da AWS for AWS WAF, che ti offre un modo semplice per distribuire regole preconfigurate e curate sulle tue applicazioni. AWS WAF Per ulteriori informazioni sulla gestione centralizzata AWS WAF con AWS Firewall Manager, consulta Gestione centralizzata AWS WAF (API v2) e su larga scala con. Regole gestite da AWS AWS Firewall Manager



Ispezione centralizzata del traffico in entrata utilizzando AWS WAF

Nell'architettura precedente, le applicazioni vengono eseguite su istanze Amazon EC2 in più zone di disponibilità nelle sottoreti private. C'è un Application Load Balancer (ALB) rivolto al pubblico distribuito davanti alle istanze Amazon EC2, che bilancia il carico delle richieste tra diversi target. AWS WAF È associato all'ALB.

Vantaggi

- Con AWS WAF Bot Control, ottieni visibilità e controllo sul traffico di bot comune e pervasivo verso le tue applicazioni.
- Con Managed Rules for AWS WAF, puoi iniziare rapidamente e proteggere la tua applicazione web o le tue API dalle minacce comuni. Puoi scegliere tra molti tipi di regole, ad esempio quelle che risolvono problemi come i 10 principali rischi per la sicurezza dell'Open Web Application Security Project (OWASP), le minacce specifiche per i sistemi di gestione dei contenuti (CMS) come Joomla WordPress o persino le emergenti Common Vulnerabilities and Exposures (CVE). Le regole gestite vengono aggiornate automaticamente man mano che emergono nuovi problemi, in modo da poter dedicare più tempo alla creazione di applicazioni.
- AWS WAF è un servizio gestito e non è necessario alcun dispositivo per l'ispezione in questa architettura. Inoltre, fornisce log quasi in tempo reale tramite Amazon Data Firehose. AWS WAF offre una visibilità quasi in tempo reale del tuo traffico web, che puoi utilizzare per creare nuove regole o avvisi in Amazon. CloudWatch

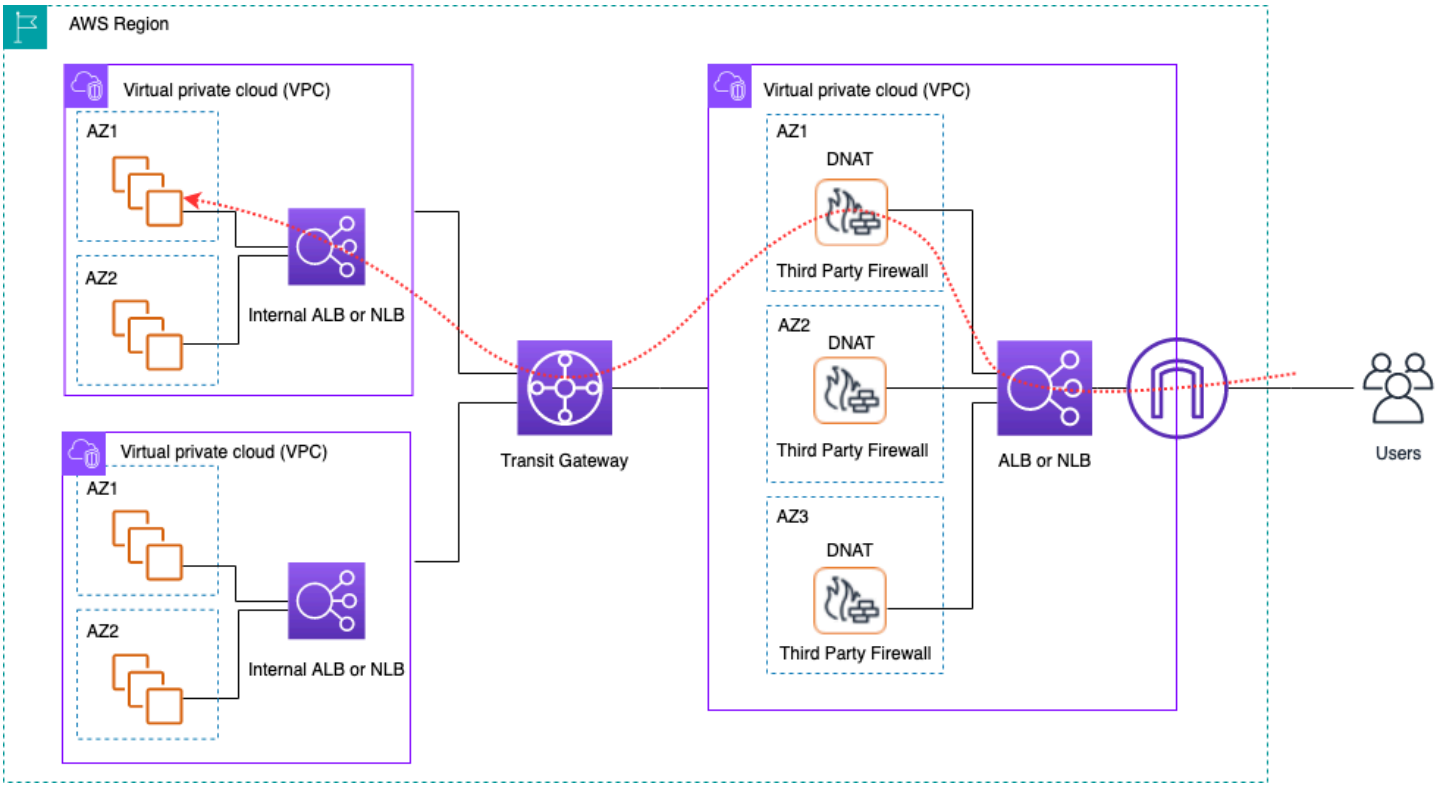
Considerazioni chiave

- Questa architettura è la più adatta per l'ispezione delle intestazioni HTTP e le ispezioni distribuite, poiché AWS WAF è integrata su un API Gateway per ALB, distribuzione e CloudFront API. AWS WAF non registra il corpo della richiesta.
- Il traffico diretto a un secondo set di ALB (se presente) potrebbe non essere ispezionato dalla stessa AWS WAF istanza, perché verrebbe effettuata una nuova richiesta al secondo set di ALB.

Ispezione centralizzata in entrata con dispositivi di terze parti

In questo modello di progettazione architettonica, distribuisci appliance firewall di terze parti su Amazon EC2 su più zone di disponibilità dietro un Elastic Load Balancer (ELB) come un Application/Network Load Balancer in un VPC di ispezione separato.

L'Inspection VPC e gli altri VPC Spoke sono collegati tra loro tramite un Transit Gateway come allegati VPC. Le applicazioni in Spoke VPC sono frontend da un ELB interno che può essere ALB o NLB a seconda del tipo di applicazione. I client tramite Internet si connettono al DNS dell'ELB esterno nel VPC di ispezione che indirizza il traffico verso uno dei dispositivi Firewall. Il Firewall ispeziona il traffico e quindi lo indirizza verso Spoke VPC tramite Transit Gateway utilizzando il DNS dell'ELB interno, come illustrato nella figura seguente. Per ulteriori informazioni sull'ispezione di sicurezza in entrata con appliance di terze parti, consulta il post del blog Come integrare le appliance firewall di terze parti in un ambiente AWS.



Ispezione centralizzata del traffico in ingresso mediante dispositivi di terze parti ed ELB

Vantaggi

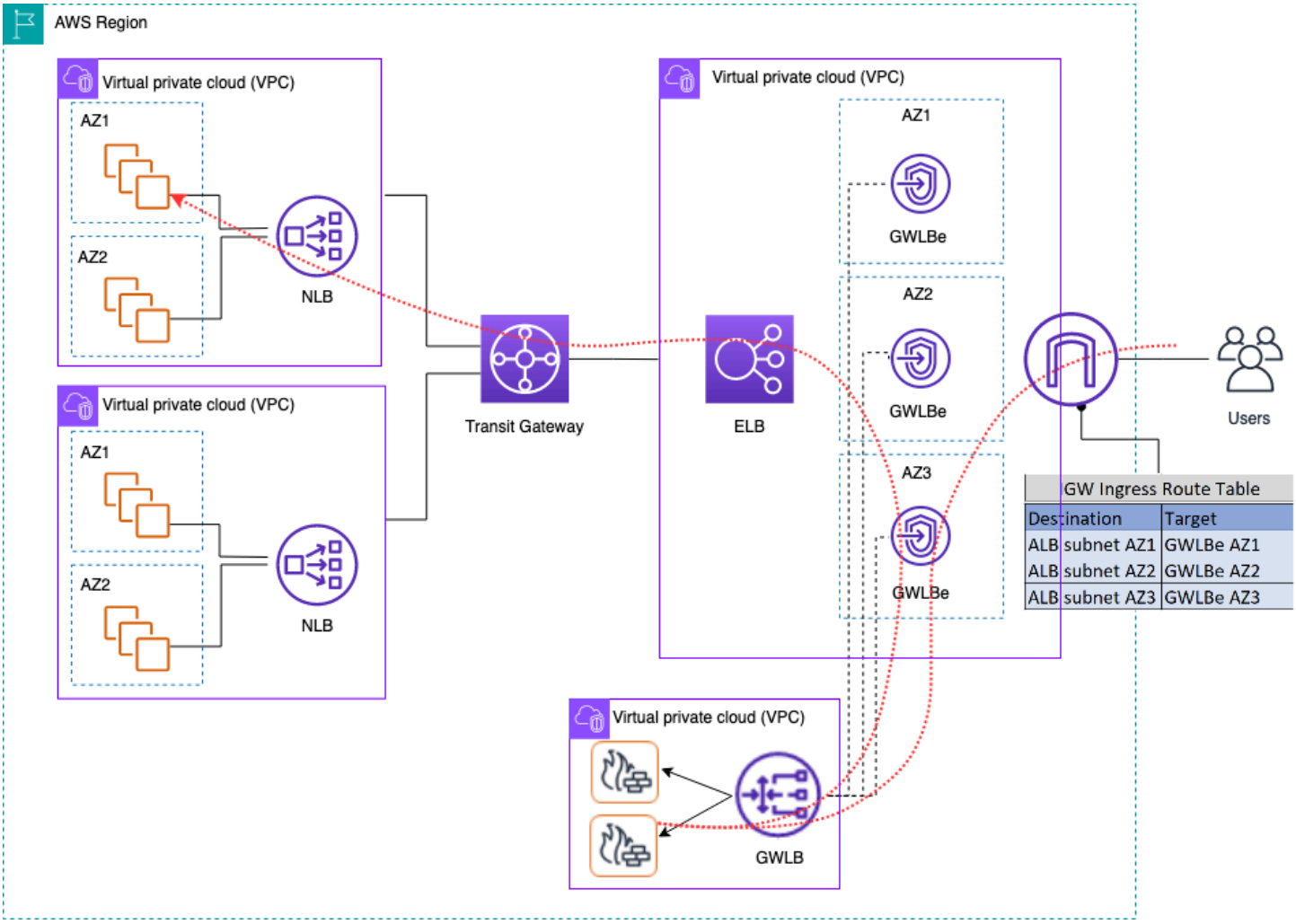
- Questa architettura può supportare qualsiasi tipo di applicazione per l'ispezione e le funzionalità di ispezione avanzate offerte tramite dispositivi firewall di terze parti.
- Questo modello supporta il routing basato su DNS dalle appliance firewall agli Spoke VPC, il che consente alle applicazioni in Spoke VPC di scalare indipendentemente grazie a un ELB.
- È possibile utilizzare Auto Scaling con ELB per scalare le appliance firewall nel VPC di Inspection.

Considerazioni chiave

- È necessario implementare più dispositivi firewall nelle zone di disponibilità per un'elevata disponibilità.
- Il firewall deve essere configurato ed eseguito con Source NAT per mantenere la simmetria del flusso, il che significa che l'indirizzo IP del client non sarà visibile all'applicazione.
- Prendi in considerazione l'implementazione di Transit Gateway e Inspection VPC nell'account Network Services.
- Costi aggiuntivi di licenza/supporto per firewall di fornitori terzi. I costi di Amazon EC2 dipendono dal tipo di istanza.

Ispezione del traffico in entrata da Internet utilizzando dispositivi firewall con Gateway Load Balancer

I clienti utilizzano firewall di nuova generazione (NGFW) e sistemi di prevenzione delle intrusioni (IPS) di terze parti come parte della loro strategia di difesa approfondita. Tradizionalmente si tratta spesso di hardware o software/dispositivi virtuali dedicati. È possibile utilizzare Gateway Load Balancer per scalare queste appliance virtuali orizzontalmente per ispezionare il traffico da e verso il VPC, come illustrato nella figura seguente.



Ispezione centralizzata del traffico in ingresso tramite dispositivi firewall con Gateway Load Balancer

Nell'architettura precedente, gli endpoint Gateway Load Balancer vengono distribuiti in ciascuna zona di disponibilità in un VPC edge separato. I firewall di nuova generazione, i sistemi di prevenzione delle intrusioni ecc. vengono implementati dietro il Gateway Load Balancer nel VPC centralizzato dell'appliance. Questo VPC dell'appliance può trovarsi nello stesso account AWS dei VPC spoke o in un account AWS diverso. Le appliance virtuali possono essere configurate per utilizzare i gruppi Auto Scaling e vengono registrate automaticamente con Gateway Load Balancer, consentendo la scalabilità automatica del livello di sicurezza.

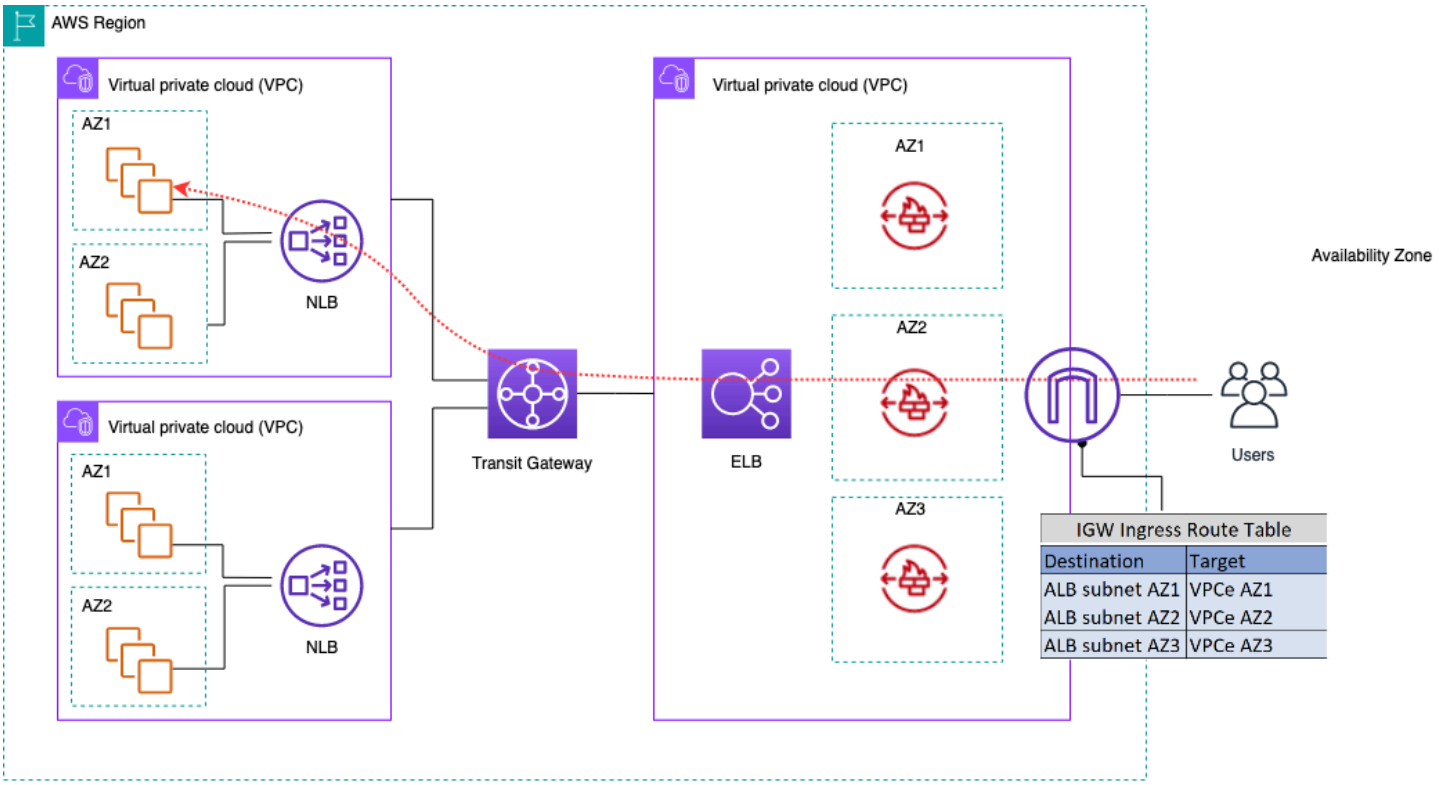
Queste appliance virtuali possono essere gestite accedendo alle relative interfacce di gestione tramite un Internet Gateway (IGW) o utilizzando una configurazione bastion host nel VPC dell'appliance.

Utilizzando la funzionalità di routing in ingresso VPC, la tabella edge route viene aggiornata per instradare il traffico in entrata da Internet alle appliance firewall dotate di Gateway Load Balancer. Il

traffico ispezionato viene instradato tramite gli endpoint Gateway Load Balancer verso l'istanza VPC di destinazione. Per informazioni dettagliate sui vari modi di utilizzare AWS Gateway Load Balancer: Supported architecture patterns, consulta il post sul blog Introducing Gateway Load Balancer: Supported architecture patterns.

Utilizzo di AWS Network Firewall per l'ingresso centralizzato

In questa architettura, il traffico in ingresso viene ispezionato AWS Network Firewall prima di raggiungere il resto dei VPC. In questa configurazione, il traffico viene suddiviso tra tutti gli endpoint firewall distribuiti nell'Edge VPC. Si distribuisce una sottorete pubblica tra l'endpoint del firewall e la sottorete Transit Gateway. Puoi utilizzare un ALB o un NLB, che contengono destinazioni IP nei tuoi VPC spoke mentre gestisci l'Auto Scaling per i target sottostanti.

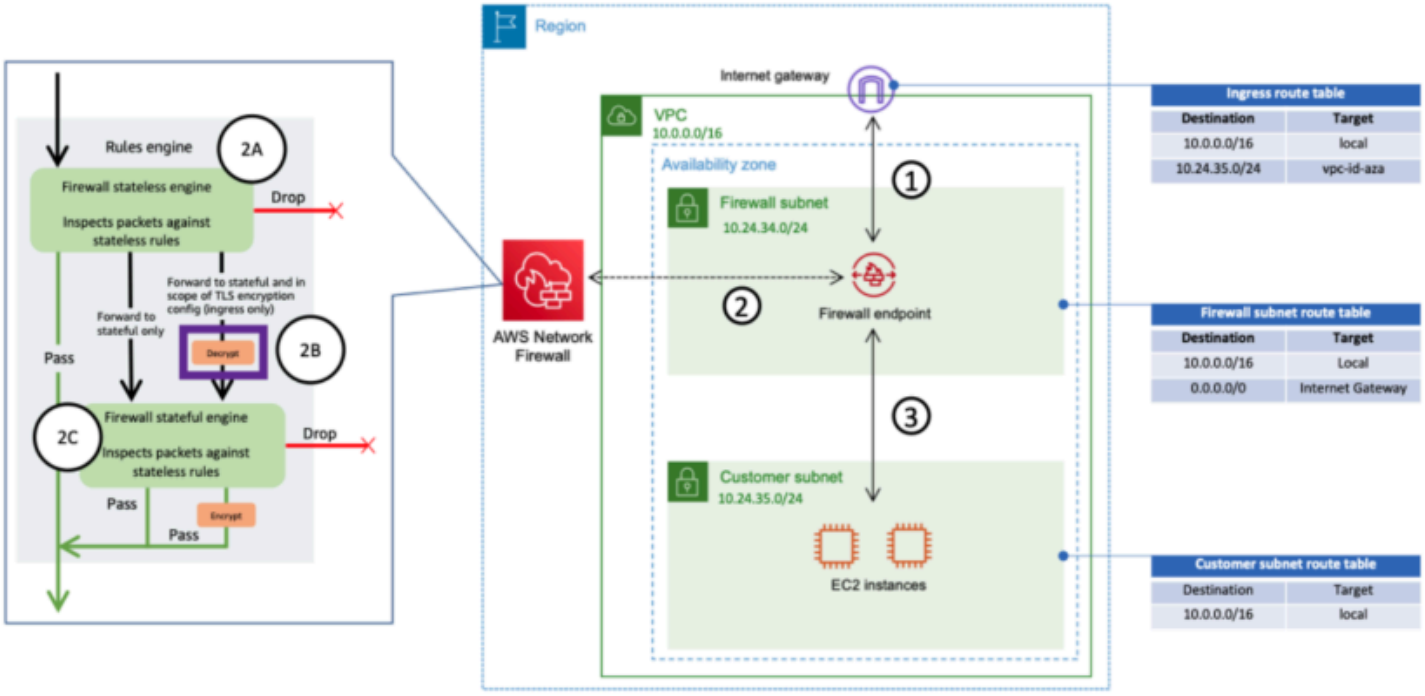


Ispezione del traffico in ingresso con AWS Network Firewall

Per semplificare l'implementazione e la gestione AWS Network Firewall di questo modello, AWS Firewall Manager può essere utilizzato. Firewall Manager consente di amministrare centralmente i diversi firewall applicando automaticamente la protezione creata nella posizione centralizzata a più account. Firewall Manager supporta modelli di distribuzione distribuiti e centralizzati per Network Firewall. Il post del blog How to deploy AWS Network Firewall by using AWS Firewall Manager fornisce maggiori dettagli sul modello.

Deep Packet Inspection (DPI) con AWS Network Firewall

Network Firewall può eseguire un'ispezione approfondita dei pacchetti (DPI) sul traffico in ingresso. Utilizzando un certificato Transport Layer Security (TLS) archiviato in AWS Certificate Manager (ACM), Network Firewall può decrittografare i pacchetti, eseguire DPI e ricrittografare i pacchetti. Esistono alcune considerazioni sulla configurazione di DPI con un firewall di rete. Innanzitutto, un certificato TLS affidabile deve essere archiviato in ACM. In secondo luogo, le regole del Network Firewall devono essere configurate per inviare correttamente i pacchetti per la decrittografia e la ricrittografia. Per ulteriori dettagli, consulta il post del blog Configurazione dell'ispezione TLS per il traffico crittografato. AWS Network Firewall



Ispezione del traffico in ingresso tramite Network Firewall con DPI

Considerazioni chiave per un'architettura di AWS Network Firewall ingresso centralizzata

- Elastic Load Balancing in Edge VPC può avere solo indirizzi IP come tipi di destinazione, non un nome host. Nella figura precedente, gli obiettivi sono gli IP privati del Network Load Balancer nei VPC spoke. L'utilizzo di target IP dietro l'ELB nel VPC edge comporta la perdita dell'Auto Scaling.
- Prendi in considerazione l'idea di utilizzarlo AWS Firewall Manager come unico pannello di controllo per gli endpoint del firewall.

- Questo modello di implementazione utilizza l'ispezione del traffico non appena entra nel VPC edge, quindi ha il potenziale per ridurre il costo complessivo dell'architettura di ispezione.

DNS

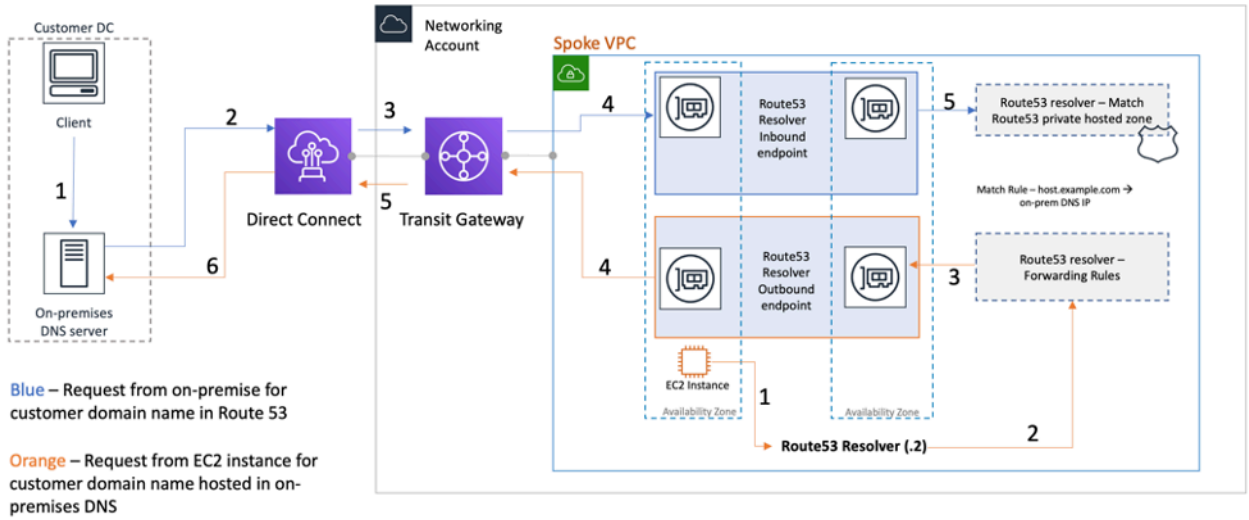
Quando avvii un'istanza in un VPC, escluso il VPC predefinito, AWS fornisce all'istanza un nome host DNS privato (e potenzialmente un nome host DNS pubblico) a seconda degli attributi DNS specificati per il VPC e se l'istanza ha un indirizzo IPv4 pubblico. Quando l'`enableDnsSupport`attributo è impostato su`true`, si ottiene una risoluzione DNS all'interno del VPC da Route 53 Resolver (offset IP +2 rispetto al VPC CIDR). Per impostazione predefinita, Route 53 Resolver risponde alle query DNS per i nomi di dominio VPC, come i nomi di dominio per le istanze EC2 o i sistemi di bilanciamento del carico Elastic Load Balancing. Con il peering VPC, gli host in un VPC possono risolvere i nomi di host DNS pubblici in indirizzi IP privati per le istanze in VPC peerizzati, a condizione che l'opzione per farlo sia abilitata. Lo stesso vale per i VPC connessi tramite. AWS Transit Gateway Per ulteriori informazioni, consulta Enabling DNS Resolution Support for a VPC peering Connection.

Se desideri mappare le tue istanze su un nome di dominio personalizzato, puoi utilizzare Amazon Route 53 per creare un record di mappatura DNS-IP personalizzato. Una zona ospitata di Amazon Route 53 è un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini. Le zone ospitate pubbliche contengono informazioni DNS risolvibili sulla rete Internet pubblica, mentre le zone ospitate private sono un'implementazione specifica che presenta informazioni solo ai VPC collegati alla specifica zona ospitata privata. In una configurazione di Landing Zone in cui hai più VPC o account, puoi associare una singola zona ospitata privata a più VPC tra account AWS e tra regioni (fattibile solo con SDK/CLI/API). Gli host finali nei VPC utilizzano il rispettivo IP Route 53 Resolver (+2 offset il VPC CIDR) come server dei nomi per le query DNS. Il Route 53 Resolver in VPC accetta query DNS solo da risorse all'interno di un VPC.

DNS ibrido

Il DNS è un componente fondamentale di qualsiasi infrastruttura, ibrida o meno, in quanto fornisce la risoluzione dal nome host all'indirizzo IP su cui si basano le applicazioni. I clienti che implementano ambienti ibridi di solito dispongono già di un sistema di risoluzione DNS e desiderano una soluzione DNS che funzioni in tandem con il sistema attuale. Il resolver Route 53 nativo (+2 offset del VPC CIDR di base) non è raggiungibile dalle reti locali tramite VPN o. AWS Direct Connect Pertanto, quando integri il DNS per i VPC in una regione AWS con il DNS per la tua rete, hai bisogno di un endpoint in entrata Route 53 Resolver (per le query DNS che stai inoltrando ai tuoi VPC) e un endpoint in uscita Route 53 Resolver (per le query che stai inoltrando dai tuoi VPC alla tua rete).

Come illustrato nella figura seguente, puoi configurare gli endpoint Resolver in uscita per inoltrare le query ricevute dalle istanze Amazon EC2 nei tuoi VPC ai server DNS della tua rete. Per inoltrare query selezionate, da un VPC a una rete locale, crea regole Route 53 Resolver che specificano i nomi di dominio per le query DNS che desideri inoltrare (ad esempio example.com) e gli indirizzi IP dei resolver DNS sulla tua rete a cui desideri inoltrare le query. Per le query in entrata dalle reti locali alle zone ospitate di Route 53, i server DNS sulla rete possono inoltrare le query agli endpoint Resolver in entrata in un VPC specifico.



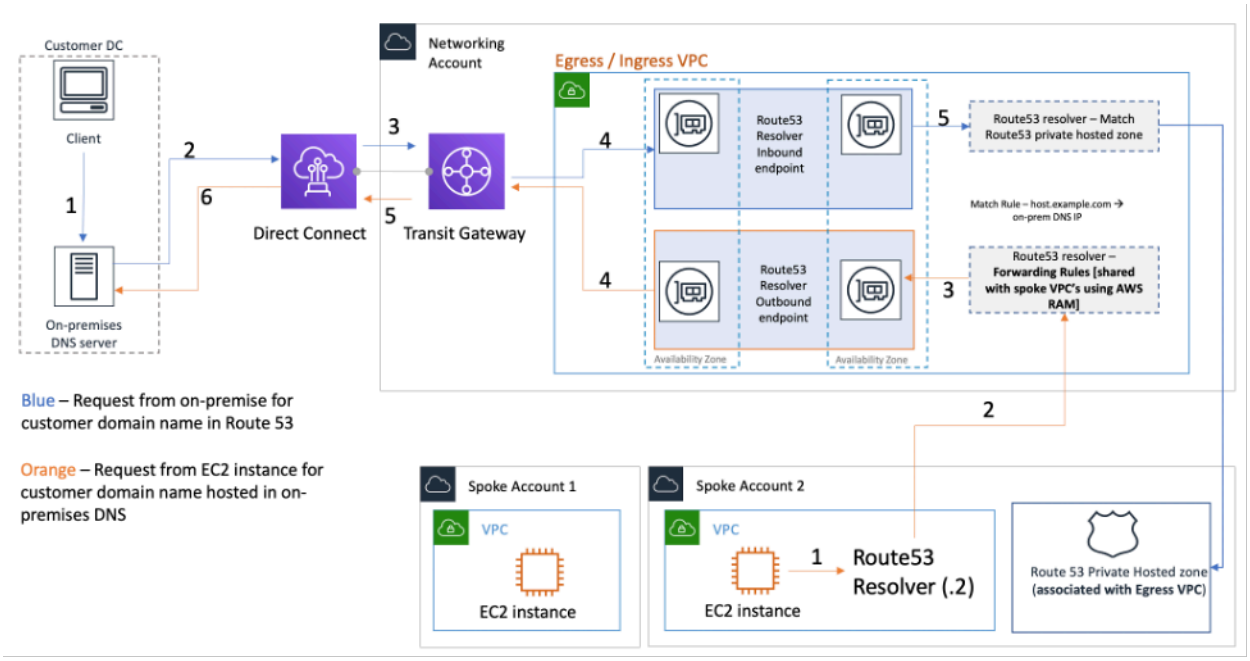
Risoluzione DNS ibrida con Route 53 Resolver

Ciò consente ai resolver DNS locali di risolvere facilmente i nomi di dominio per le risorse AWS, come le istanze o i record di Amazon EC2 in una zona ospitata privata Route 53 associata a quel VPC. Inoltre, gli endpoint Route 53 Resolver possono gestire fino a circa 10.000 query al secondo per ENI, quindi possono essere scalati facilmente fino a volumi di query DNS molto più grandi. Per ulteriori dettagli, consulta le Best practice for Resolver nella documentazione di Amazon Route 53.

Non è consigliabile creare endpoint Route 53 Resolver in ogni VPC della Landing Zone. Centralizzali in un VPC di uscita centrale (nell'account dei servizi di rete). Questo approccio consente una migliore gestibilità mantenendo bassi i costi (viene addebitata una tariffa oraria per ogni endpoint resolver in entrata/uscita creato). Condividete l'endpoint centralizzato in entrata e in uscita con il resto della Landing Zone.

- Risoluzione in uscita: utilizza l'account Network Services per scrivere regole di resolver (in base alle quali le query DNS verranno inoltrate ai server DNS locali). Utilizzando Resource Access Manager (RAM), condividi queste regole di Route 53 Resolver con più account (e associale ai VPC negli account). Le istanze EC2 in VPC spoke possono inviare query DNS a Route 53 Resolver e Route 53 Resolver Service inoltrerà queste query al server DNS locale tramite gli endpoint Route

53 Resolver in uscita nel VPC in uscita. Non è necessario collegare i VPC in modalità peer spoke al VPC in uscita o collegarli tramite Transit Gateway. Non utilizzate l'IP dell'endpoint resolver in uscita come DNS primario nei VPC spoke. I VPC Spoke devono utilizzare Route 53 Resolver (per compensare il CIDR del VPC) nel proprio VPC.



Centralizzazione degli endpoint Route 53 Resolver nel VPC in ingresso/uscita

- Risoluzione DNS in entrata: crea endpoint in ingresso Route 53 Resolver in un VPC centralizzato e associa tutte le zone ospitate private nella tua Landing Zone a questo VPC centralizzato. Per ulteriori informazioni, consulta Associare più VPC a una zona ospitata privata. Più zone private ospitate (PHZ) associate a un VPC non possono sovrapporsi. Come illustrato nella figura precedente, questa associazione di PHZ con il VPC centralizzato consentirà ai server locali di risolvere il DNS per qualsiasi ingresso in qualsiasi zona ospitata privata (associata al VPC centrale) utilizzando l'endpoint in ingresso nel VPC centralizzato. Per ulteriori informazioni sulle configurazioni DNS ibride, consulta Gestione DNS centralizzata del cloud ibrido con Amazon Route 53 e AWS Transit Gateway e opzioni DNS di cloud ibrido per Amazon VPC.

Firewall DNS Route 53

Amazon Route 53 Resolver DNS Firewall aiuta a filtrare e regolare il traffico DNS in uscita per i tuoi VPC. Uno degli usi principali del firewall DNS consiste nell'impedire l'esfiltrazione dei dati

definendo elenchi di nomi di dominio consentiti che consentono alle risorse del tuo VPC di effettuare richieste DNS in uscita solo per i siti considerati affidabili dall'organizzazione. Offre inoltre ai clienti la possibilità di creare elenchi di blocco per i domini con cui non vogliono che le risorse all'interno di un VPC comunichino tramite DNS. Amazon Route 53 Resolver Il firewall DNS presenta le seguenti funzionalità:

I clienti possono creare regole per definire la modalità di risposta alle query DNS. Le azioni che possono essere definite per i nomi di dominio includonoNODATA, OVERRIDE e. NXDOMAIN

I clienti possono creare avvisi sia per le liste consentite che per le liste di rifiuto per monitorare l'attività delle regole. Ciò può rivelarsi utile quando i clienti desiderano testare la regola prima di passare alla produzione.

Per ulteriori informazioni, consulta il post del blog How to Get Started with Amazon Route 53 Resolver DNS Firewall for Amazon VPC.

Accesso centralizzato agli endpoint VPC privati

Un VPC endpoint consente di connettersi privatamente ai AWS servizi supportati senza richiedere un gateway Internet o un NAT dispositivo, una connessione o una VPN connessione. VPC AWS Direct Connect Pertanto, il tuo non VPC è esposto alla rete Internet pubblica. Le istanze presenti non VPC richiedono indirizzi IP pubblici per comunicare con gli endpoint di AWS servizio con questo endpoint di interfaccia. Il traffico tra l'utente VPC e gli altri servizi non esce dalla spina dorsale della AWS rete. VPCgli endpoint sono dispositivi virtuali. Sono componenti ridondanti, scalabili orizzontalmente e ad alta disponibilità. VPC Attualmente è possibile fornire due tipi di endpoint: endpoint di interfaccia (con tecnologia) ed endpoint gateway. AWS PrivateLink Gli endpoint gateway possono essere utilizzati per accedere ai servizi Amazon S3 e Amazon DynamoDB in modo privato. L'utilizzo di endpoint gateway non comporta costi supplementari. Vengono applicati i costi standard per il trasferimento dei dati e l'utilizzo delle risorse.

Endpoint VPC di interfaccia

Un endpoint di interfaccia è costituito da una o più interfacce di rete elastiche con un indirizzo IP privato che funge da punto di ingresso per il traffico destinato a un servizio supportato. AWS Quando si effettua il provisioning di un endpoint di interfaccia, viene addebitato un costo per ogni ora di funzionamento dell'endpoint, oltre ai costi di elaborazione dei dati. Per impostazione predefinita, si crea un endpoint di interfaccia in ogni dispositivo VPC da cui si desidera accedere al servizio. AWS Ciò può essere proibitivo in termini di costi e difficile da gestire nella configurazione della Landing Zone, in cui un cliente desidera interagire con uno specifico servizio su più piattaformeAWS. VPCs Per evitare ciò, puoi ospitare gli endpoint dell'interfaccia in modo centralizzato. VPC Tutti gli spoke VPCs utilizzeranno questi endpoint centralizzati tramite Transit Gateway.

Quando crei un VPC endpoint per un AWS servizio, puoi abilitarlo come privato. DNS Se abilitata, l'impostazione crea una zona ospitata privata Route 53 AWS gestita (PHZ), che consente la risoluzione dell'endpoint del AWS servizio pubblico sull'IP privato dell'endpoint di interfaccia.
Il managed funziona PHZ solo all'interno dell'endpoint VPC con l'interfaccia. Nella nostra configurazione, quando vogliamo che Spoke VPCs sia in grado di risolvere un VPC endpoint DNS ospitato in un ambiente centralizzatoVPC, il managed PHZ non funzionerà. Per ovviare a questo problema, disabilita l'opzione che crea automaticamente l'interfaccia privata DNS quando viene creato un endpoint di interfaccia. Successivamente, crea manualmente una zona ospitata privata Route 53 corrispondente al nome dell'endpoint del servizio e aggiungi un record Alias con il nome completo dell'endpoint che punti all' Servizio AWS endpoint dell'interfaccia.

1. Accedi a Route 53 e accedi a Route AWS Management Console 53.
2. Seleziona la zona ospitata privata e vai a Crea record.
3. Compila il campo Nome del record, seleziona Tipo di record come A e abilita l'alias.

   Tieni presente che alcuni servizi, come Docker e OCI client endpoints (**`dkr.ecr`**), richiedono l'uso di un alias jolly (**`*`**) per il Record Name.
4. Nella sezione Indirizza il traffico verso, seleziona il servizio a cui inviare il traffico e seleziona la regione dall'elenco a discesa.
5. Seleziona la politica di routing appropriata e attiva l'opzione Valuta lo stato dell'obiettivo.

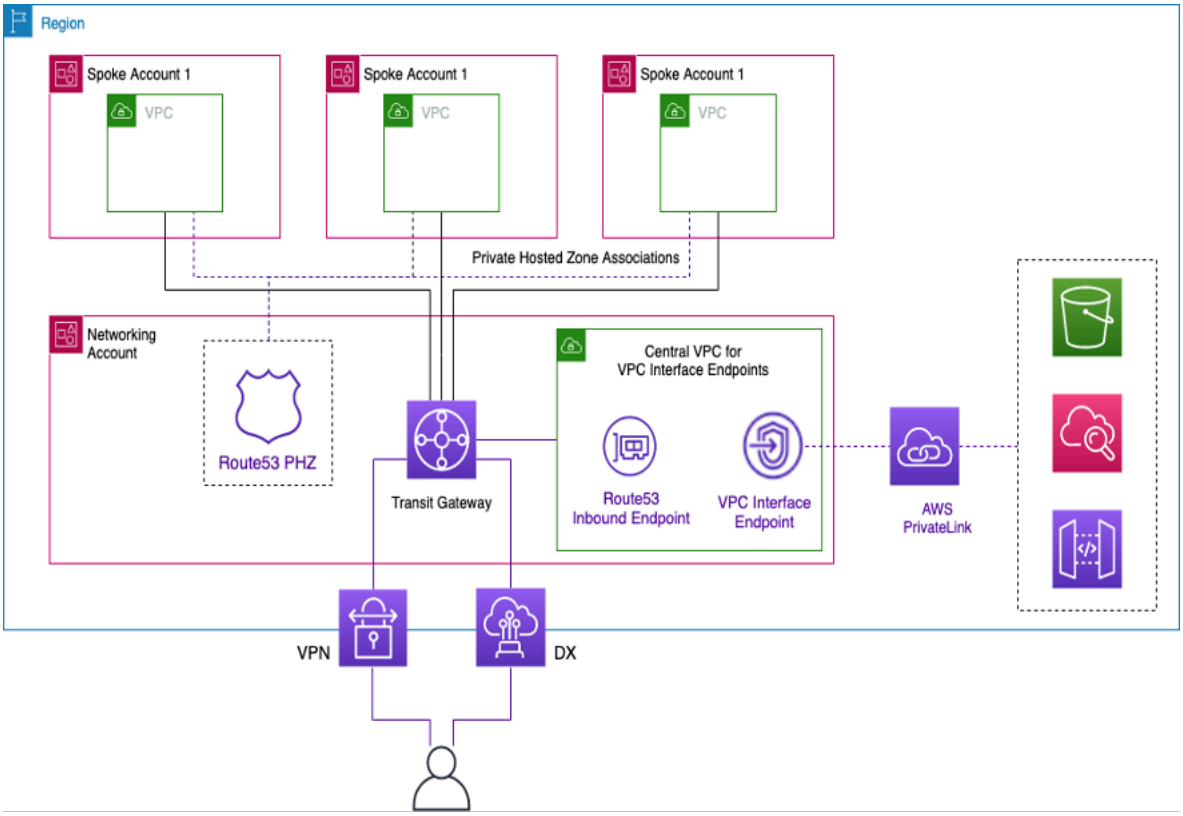
Associate questa zona ospitata privata ad altre all'VPCsinterno della Landing Zone. Questa configurazione consente a Spoke di VPCs risolvere i nomi degli endpoint a servizio completo per interfacciare gli endpoint in modo centralizzato. VPC

> **Note**
>
> Per accedere alla zona ospitata privata condivisa, gli host nello spoke VPCs devono utilizzare il proprio IP Route 53 Resolver. VPC Gli endpoint dell'interfaccia sono accessibili anche dalle reti locali tramite VPN Direct Connect. Utilizza le regole di inoltro condizionale per inviare tutto il DNS traffico relativo ai nomi degli endpoint a servizio completo agli endpoint in entrata di Route 53 Resolver, che risolveranno le richieste in base alla zona ospitata privata. DNS

Nella figura seguente, Transit Gateway abilita il flusso del traffico dagli spoke VPCs agli endpoint dell'interfaccia centralizzata. Crea gli VPC endpoint e la relativa zona ospitata privata in Network Services Account e condividili con gli account spoke VPCs in the spoke. Per maggiori dettagli sulla condivisione delle informazioni sugli endpoint con altriVPCs, consulta il post di blog Integrating AWS Transit Gateway with e AWS PrivateLink Amazon Route 53 Resolver.

> **Note**
>
> Un approccio distribuito agli VPC endpoint, vale a dire un endpoint per, VPC consente di applicare politiche con privilegi minimi sugli endpoint. VPC Con un approccio centralizzato, applicherai e gestirai le policy per tutti gli VPC accessi su un unico endpoint. Con l'aumento del numero diVPCs, potrebbe aumentare la complessità legata al mantenimento del privilegio minimo con un unico documento di policy. Un unico documento politico si traduce anche in un

raggio d'azione più ampio. Le dimensioni del documento di policy sono inoltre limitate (20.480 caratteri).



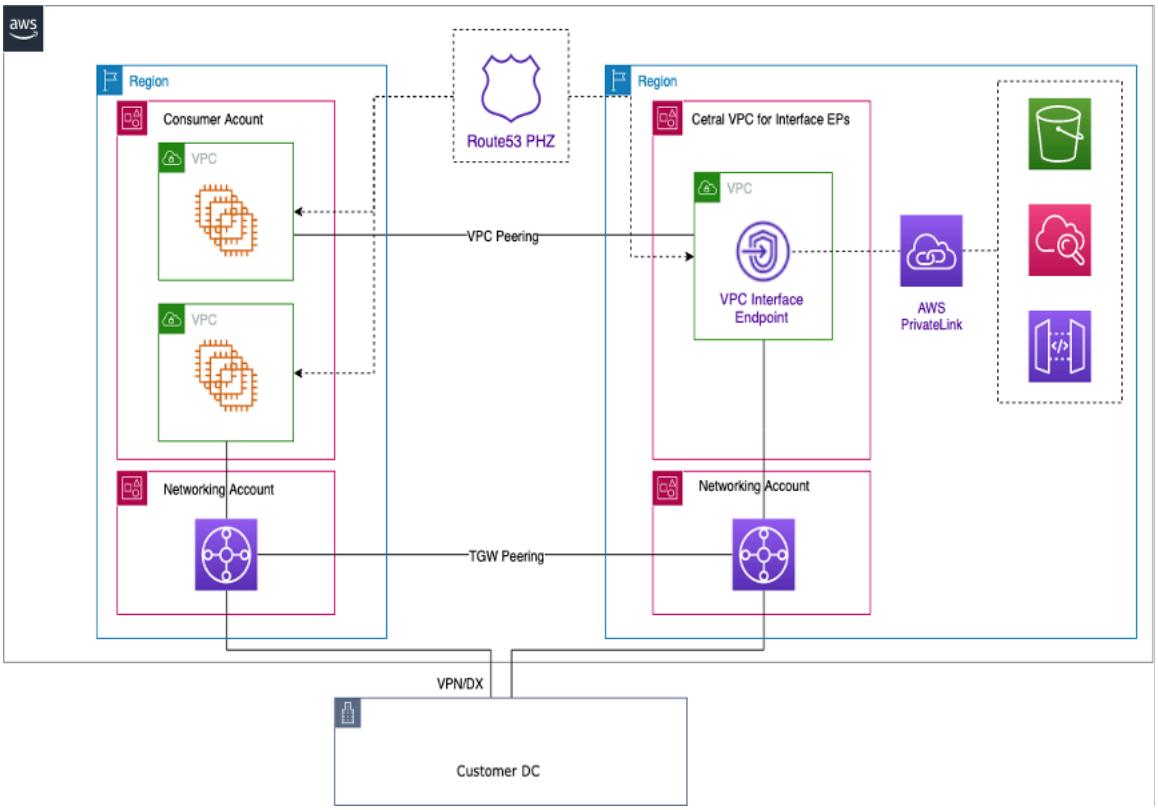
Centralizzazione VPC degli endpoint dell'interfaccia

Accesso agli endpoint interregionali

Se desideri VPCs configurazioni multiple in diverse regioni che condividono un VPC endpoint comune, usa unPHZ, come indicato in precedenza. Entrambi VPCs in ciascuna regione verranno PHZ associati all'alias dell'endpoint. Per instradare il traffico tra le due regioni VPCs in un'architettura multiregionale, i gateway di transito di ciascuna regione devono essere collegati tra loro. Per ulteriori informazioni, consulta questo blog: Utilizzo delle zone ospitate private Route 53 per architetture multiregionali tra account.

VPCsda diverse regioni possono essere instradate l'una verso l'altra utilizzando Transit Gateway o Peering. VPC Utilizza la seguente documentazione per il peering dei Transit Gateway: Transit Gateway Peering Attachments.

In questo esempio, l'EC2istanza Amazon nella VPC `us-west-1` regione utilizzerà il PHZ per ottenere l'indirizzo IP privato dell'endpoint nella `us-west-2` regione e indirizzare il traffico verso la `us-west-2` regione VPC tramite il peering o VPC il peering Transit Gateway. Utilizzando questa architettura, il traffico rimane all'interno della AWS rete, permettendo all'EC2istanza di accedere in modo sicuro `us-west-1` al VPC servizio `us-west-2` senza passare da Internet.



VPCEndpoint multiregionali

> **Note**
>
> I costi per il trasferimento di dati tra regioni si applicano quando si accede agli endpoint tra regioni diverse.

Facendo riferimento alla figura precedente, un servizio endpoint viene creato in una VPC regione. `us-west-2` Questo servizio endpoint fornisce l'accesso a un AWS servizio in quella regione. Affinché le istanze in un'altra regione (ad esempio`us-east-1`) possano accedere all'endpoint nella `us-west-2` regione, è necessario creare un record di indirizzo in PHZ con un alias per l'endpoint desiderato. VPC

Innanzitutto, assicurati che VPCs in ogni regione siano associati a quello che hai creato. PHZ

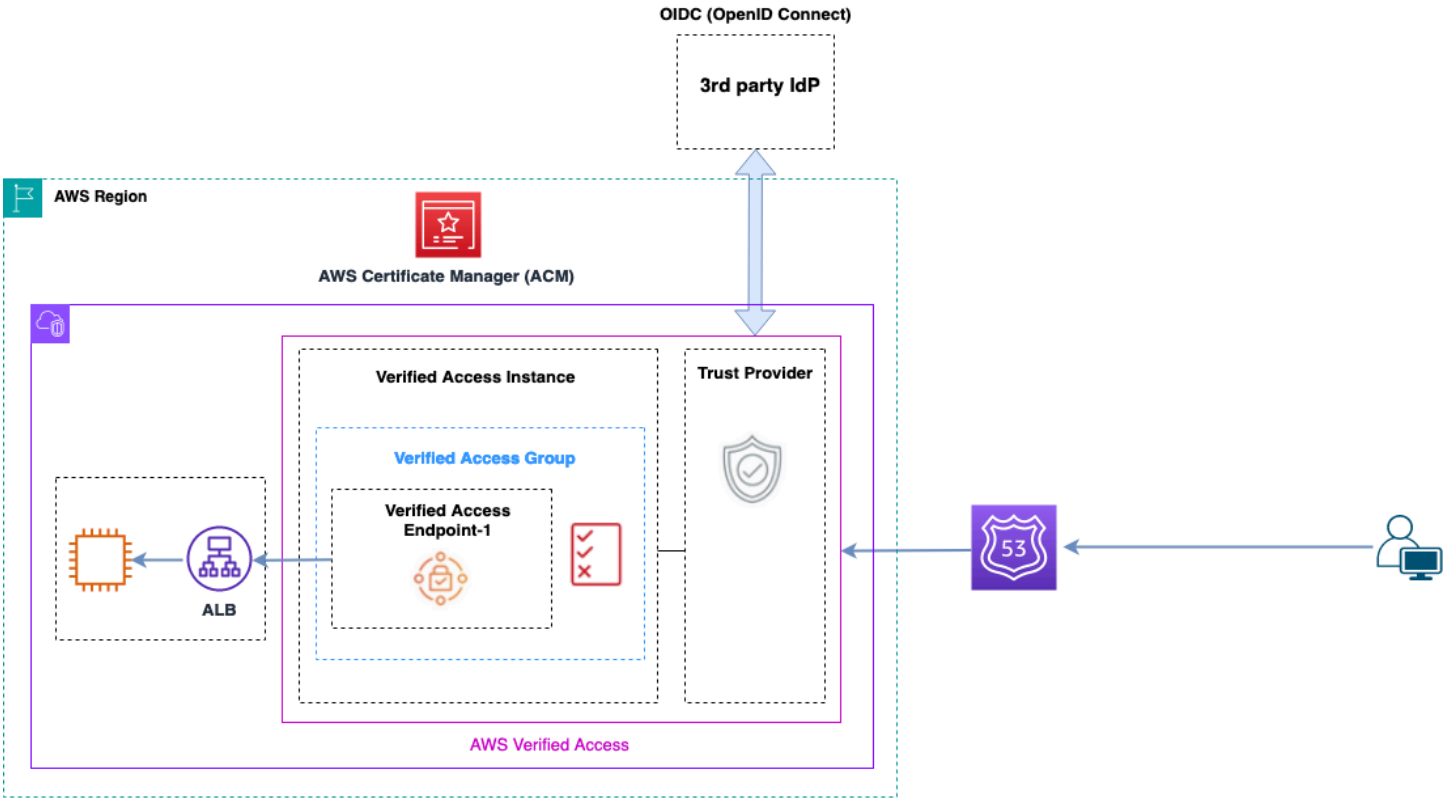
Quando si implementa un endpoint in più zone di disponibilità, l'indirizzo IP dell'endpoint restituito proviene da DNS una qualsiasi delle sottoreti della zona di disponibilità allocata.

Quando richiami l'endpoint, usa il nome di dominio completo () che si trova in. FQDN PHZ

Accesso verificato da AWS

Accesso verificato da AWS offre un accesso sicuro alle applicazioni nella rete privata senza unVPN. Valuta le richieste in tempo reale come identità, dispositivo e posizione. Questo servizio garantisce l'accesso in base a politiche per le applicazioni e la connessione degli utenti migliorando la sicurezza dell'organizzazione. Verified Access fornisce l'accesso alle applicazioni private fungendo da proxy inverso con riconoscimento dell'identità. L'identità dell'utente e lo stato del dispositivo, se applicabile, vengono eseguiti prima di instradare il traffico verso l'applicazione.

Il diagramma seguente fornisce una panoramica di alto livello dell'accesso verificato. Gli utenti inviano richieste di accesso a un'applicazione. Verified Access valuta la richiesta in base alla politica di accesso del gruppo e a qualsiasi politica degli endpoint specifica dell'applicazione. Se l'accesso è consentito, la richiesta viene inviata all'applicazione tramite l'endpoint.



Panoramica dell'accesso verificato

I componenti principali di un' Accesso verificato da AWS architettura sono:

- Istanze di accesso verificato: un'istanza valuta le richieste delle applicazioni e concede l'accesso solo quando sono soddisfatti i requisiti di sicurezza.
- Endpoint ad accesso verificato: ogni endpoint rappresenta un'applicazione. Un endpoint può essere un'interfaccia di NLB reteALB.
- Gruppo Verified Access: una raccolta di endpoint Verified Access. Ti consigliamo di raggruppare gli endpoint per applicazioni con requisiti di sicurezza simili per semplificare l'amministrazione delle policy.
- Criteri di accesso: un insieme di regole definite dall'utente che determinano se consentire o negare l'accesso a un'applicazione.
- Fornitori di fiducia: Verified Access è un servizio che facilita la gestione delle identità degli utenti e degli stati di sicurezza dei dispositivi. È compatibile sia con i provider di fiducia che con quelli di terze parti AWS e richiede che almeno un provider fiduciario sia collegato a ciascuna istanza di Verified Access. Ciascuna di queste istanze può includere un singolo provider di trust di identità e più provider di fiducia per dispositivi.
- Dati attendibili: i dati di sicurezza che il fornitore di servizi fiduciari invia a Verified Access, come l'indirizzo e-mail di un utente o il gruppo a cui appartiene, vengono valutati in base alle politiche di accesso dell'utente ogni volta che viene ricevuta una richiesta di candidatura.

Maggiori dettagli sono disponibili nei post del blog Verified Access.

Conclusioni

Man mano che si ridimensiona l'utilizzo AWS e si distribuiscono le applicazioni nella AWS Landing Zone, il numero di VPC e componenti di rete aumenta. Questo white paper spiega come gestire questa infrastruttura in crescita garantendo scalabilità, alta disponibilità e sicurezza mantenendo bassi i costi. Prendere le giuste decisioni di progettazione quando si utilizzano servizi come Transit Gateway, Shared VPC, endpoint AWS Direct Connect VPC, Gateway Load Balancer, AWS Network Firewall Amazon Route 53 e appliance software di terze parti diventa fondamentale. È importante comprendere le considerazioni chiave di ogni approccio, partire dalla base dei requisiti e analizzare l'opzione o la combinazione di opzioni più adatta alle proprie esigenze.

Collaboratori

Le seguenti persone hanno contribuito a questo documento:

- Sohaib Tahir, architetto di soluzioni, Amazon Web Services
- Shirin Bhambhani, architetto di soluzioni, Amazon Web Services
- Kunal Pansari, architetto di soluzioni, Amazon Web Services
- Eric Vasquez, architetto di soluzioni, Amazon Web Services
- Tushar Jagdale, architetto di soluzioni, Amazon Web Services
- Ameer Shariff, architetto di soluzioni, Amazon Web Services
- Glenn Davis, architetto di soluzioni, Amazon Web Services
- Nick Kniveton, architetto di soluzioni, Amazon Web Services
- Sidhartha Chauhan, Architetto principale delle soluzioni, Amazon Web Services

Cronologia dei documenti

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed RSS.

Modifica	Descrizione	Data
Aggiornamento importante	Aggiornamenti in tutto il white paper per le modifiche a CloudWAN, Amazon VPC Lattice, ENA Express, connettività AWS Direct Connect ibrida, Sitelink, Deep Packet Inspection e. Accesso verificato da AWS	17 aprile 2024
Aggiornamento secondario	Diagrammi aggiornati per essere più coerenti, opzioni di connettività DX aggiornate per includere una VPN IP privata e numerose modifiche minori.	6 luglio 2023
Aggiornamento secondario	AWS Control Tower Informazioni aggiornate, con nuovi limiti di throughput per vari servizi, diagramma del gateway NAT aggiornato, sezione di sicurezza aggiornata per l'uscita centralizzata.	4 aprile 2023
Aggiornamento secondario	Sezione aggiunta: accesso agli endpoint interregionali.	19 luglio 2022
Aggiornamento importante	Sezione Transit Gateway aggiornata con Transit Gateway Connect, sezione Transit VPC aggiornata; AWS Direct Connect sezione	22 febbraio 2022

	aggiornata con MacSec e consigli sulla resilienza; sezione aggiornata. AWS PrivateLink Aggiunta la tabella di confronto tra VPC peering e Transit VPC e Transit Gateway; aggiunta una sezione di ispezione centraliz zata in entrata; sicurezza di rete centralizzata aggiornata per VPC-to-VPC e da VPC-on-premise a VPC e uscita centralizzata verso Internet con modelli di progettazione Gateway Load Balancer; aggiunte sezioni gateway NAT privato e firewall DNS AWS Network Firewall Amazon Route 53.	
Aggiornamento secondario	Sezione di peering Transit Gateway vs VPC aggiornata	2 aprile 2021
Whitepaper aggiornato	Testo corretto in modo che corrisponda alle opzioni illustrate nella Figura 7	10 giugno 2020
Pubblicazione iniziale	Whitepaper pubblicato.	15 novembre 2019

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi fornitori, licenziatari o affiliate. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.